CONTENT

Chapter 1 Commands for Basic Switch

1.1 Basic Switch Configuration

1.1.1 Basic Configuration

1.1.1.1 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 and 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, the user can login as long as a authentication method is passed. AAA function and RADIUS server should be configured before the RADIUS authentication 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 Telnet and ssh login method to RADIUS authentication method.

Switch(config)# authentication line vty login radius

Relative Command: aaa enable, radius-server authentication host, tacacs-server authentication host, tacacs-server key

1.1.1.2 banner

Command: banner motd <LINE>
no banner motd

Function: This command is used to configure the information displayed when the login

authentication of a telnet or console user is successful, the no command configures that the information is not displayed when the authentication is successful.

Parameters: <*LINE*>: The information displayed when the authentication is successful, length limit from 1 to 100 characters.

Default: Do not show the information when the authentication is successful.

Command mode: Global mode.

Example:

Switch(config)#banner motd Welcome

1.1.1.3 boot img

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

Function**:** Configure the first and second img files used in the next boot of the switch.

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

1. The file path comprises of three parts: device prefix used as the root directory (flash:/), sub-directory, and the file name. No space is allowed in each part or between two parts.

2. The suffix of all file names should be .img.

3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.

Command Mode: Admin Mode.

Default: The factory original configuration only specifies the first booting IMG file, it is nos.img file in the FLASH, without the second booting IMG file.

Usage Guide**:** The first and second img files can only use **.img** files stored in switch.

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

Switch#boot img flash:/nos.img backup

1.1.1.4 boot startup-config

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

Function: Configure the CFG file used in the next booting of the switch.

Parameters: The NULL keyword means to use the factory original configuration as the next booting configuration. Setting the CFG file used in the next booting as NULL equals to implementing set default and write commands. ***<file-url>*** is the full path of CFG file used in the next booting. The format of which is as follows:

1. The file path comprises of three parts: device prefix used as the root directory (flash:/), sub-directory, and the file name. No space is allowed in each part or between two parts.

***2.* The** suffix of all file names should be .cfg.

3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.

Command Mode: Admin Mode.

Default Settings: None.

Usage Guide: Configure the CFG file used in the next booting can only use .cfg files stored in the switch.

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

Switch# boot startup-config flash:/ startup.cfg

1.1.1.5 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 2006.1.1 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

Relative Command: show clock

1.1.1.6 config

Command: config [terminal]

Function: Enter Global Mode from Admin Mode.

Parameter: [terminal] indicates terminal configuration.

Command mode: Admin Mode

Example:

Switch#config

1.1.1.7 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.

1.1.1.8 disable

Command: disable

Function: Disable admin mode.

Parameter: None.

Default: None.

Command mode: Admin Mode.

Usage Guide: None.

Example:

Switch#disable

Switch>

1.1.1.9 enable

Command: enable [<*1-15*>]

Function: Use **enable** command to enter Admin Mode from User Mode, or change the privilege level of the users.

Command mode: User Mode/ Admin Mode.

Default: None.

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. When the user's privilege is changed from the low level to the high level, it needs to authenticate the password of the corresponding level, or else it will not authenticate the password. Set the Admin user password under Global Mode with "**enable password**" command.

Example:

Switch>enable

Switch#

1.1.1.10 enable password

Command: enable password [level <*1-15*>] [0 | 7] <*password*>

no enable password [level <*1-15*>]

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

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

Parameter: level <*1-15*> is used to specify the privilege level, the default level is 15. **<*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: Configure the command for general users to enter the admin mode by rule as test.
Switch(config)#enable password 0 test

1.1.1.11 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#

1.1.1.12 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 0~59.
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

1.1.1.13 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#

1.1.1.14 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
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 a
command argument (e.g. 'show ?') and describes each possible
argument.
2. Partial help is provided when an abbreviated argument is entered
and you want to know what arguments match the input
(e.g. 'show ve?'.)

1.1.1.15 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 64 characters are allowed.

Command mode: Global Mode

Default: The default prompt is relative 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)#

1.1.1.16 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 64 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

1.1.1.17 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 command deletes this mapping relationship.

Parameter: *<hostname>* is the name of the host, containing max 64 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

1.1.1.18 ip http server

Command: ip http server

no ip http server

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

Default: Enable.

Command mode: Global mode

Usage guide: Web configuration is for supplying an interface configured with HTTP for the user, which is straight and visual, easy to understand.

Example: Enable Web Server function and enable Web configurations.

Switch(config)#ip http server

1.1.1.19 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.

1.1.1.20 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

1.1.1.21 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 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: 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

1.1.1.22 privilege

Command: privilege mode level <*1-15*> LINE

no privilege mode level <*1-15*> LINE

Function: Configure the level for the specified command, the no command restores the original level of the command.

Parameters: mode: register mode of the command, 'Tab' or '?' is able to show all register modes

<*1-15*> is the level, its range between 1 and 15

LINE: the command needs to be configured, it supports the command

abbreviation

Command Mode: Global mode

Usage Guide: This function cannot change the command itself. LINE must be the whole command format, the command with the abbreviation format must be analyzed successfully. For half-baked command, false command about writing and command that abbreviation cannot be analyzed successfully, the configuration is failure. For changing the command line with the parameter, it should fill in the parameter which is able to be selected discretionarily according to the required format. However, level of the no command is able to be set optionally and it does not affect the result. When using no command, LINE must be the configured command line. If the command line with the parameter, the parameter must be matched with the configured command. (After configure the privilege of enable command, please add command **authencation line console login local** and configure corresponding privilege username password to ensure users can enter privilege mode again. If console link in usual user mode after complete configuration through other login way, please input exit or quit again, it will prompt user to input user name password to enter privilege mode.)

Example: Change the level of **show ip route** command to level 5.

Switch(config)#privilege exec level 5 show ip route

Change the level of **peer A.B.C.D** command to level 6.

Switch(config)#privilege router-msdp level 6 peer 1.2.3.4

Restore the original level for **show ip route** command.

Switch(config)#no privilege exec level 5 show ip route

Restore the original level for **peer A.B.C.D** command.

Switch(config)#no privilege router-msdp level 6 peer 1.2.3.4

1.1.1.23 privilege mode level <1-15> all

Command: privilege mode level <1-15> all

no privilege mode level all

Function: Configure the level for all commands, the no command restores the original level of all commands.

Parameters: mode: register mode of the command, 'Tab' or '?' is able to show all register modes

<*1-15*> is the level, its range between 1 and 15

Command Mode: Global mode

Usage Guide: This function cannot change the privilege of enable、end、exit or help command, the command of privilege mode level <1-15> LINE can be used to change them individually if necessary.

Example: Change the level of all commands on config mode to level 15.

Switch(config)#privilege config level 15 all

Restore the original level for all commands on config mode.

Switch(config)#no privilege config level all

1.1.1.24 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.

1.1.1.25 rps-power monitor

Command: rps-power monitor {on | off}

Function: Device power status monitoring switch.

Command mode: Global Mode.

Default: Rps-power monitor off by system default

Usage Guide: The **rps-power monitor on** command to enable device power monitoring, monitor power status changes, and switch between DC and AC power supplies, and record logs; Run the **rps-power monitor off** command to cancel the monitoring and no logs for power status change.

Attention: Some devices not support.

Example: Enable device power monitoring

Switch(config)#rps-power monitor on

1.1.1.26 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, ip ftp 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

1.1.1.27 service password valid-time

Command: service password valid-time *<0-90>*

no service password valid-time

Function: Set the user password validity, The "**no service password valid-time**" command cancels the user password validity configuration.

Command mode: Configuration mode.

Default: No user password valid time by system default.

Usage guide: Set the validity period of the user password. When the user password is created, the creation time of the current password will be recorded, and the system will prompt to change

the password after the expiration date. Valid time '0' means that the password is always valid.

Example: Set a password valid for 7 days

Switch(config)# service user password valid-time 7

1.1.1.28 login-fail retry-times

Command: login-fail retry-times *<retry-times>* lock-time *<lock-time>*

no login-fail

Function: Sets the maximum number of failed login attempts. The "**no login-fail**" command cancels the maximum failed login attempts configuration.

Parameter: ***<retry-times>*:**Maximum number of failed login attempts, in times, ranging from 0-10.

***<lock-time>*:**The amount of time, in minutes, that an account is locked after reaching the number of failures, ranging from 1-120 minutes.

Default: No login-fail retry-times by system default. Accounts are locked for 120 minutes after reaching the number of failures by system default.

Command mode: Global Mode

Usage guide: Set the maximum number of failed login attempts.When this command is set, the user will be locked out after the set number of failed login attempts. Only after the configured lock time is over, can the user log in normally with the account. Setting the maximum number of failed login attempts to 0 means that the number of failed login attempts is not checked.

Example: The maximum number of failed login attempts is set to 3 and the lock time is 30 minutes

Switch(config)# login-fail retry-times 3 lock-time 30

1.1.1.29 show locked user

Command: show locked user

Function: Show the locked user information.

Command mode: Admin and configuration mode.

Usage Guide: Used to display the locked user name, the locked time, and the remaining locked time

Example: Show the current locked user.

Switch(config)#show locked user

Global login-fail retry times 3, lock time 30 minutes

Username	Lock Time(sec)	Remain Time(sec)
User1	1800	100
User2	1800	50

1.1.1.30 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

1.1.1.31 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

1.1.1.32 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

1.1.1.33 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

1.1.1.34 set boot password

Command: set boot password

no set boot password

Function: Configure the password of entering the bootrom. The no command cancels the password.

Parameters: New password is the password configured by user; Confirm password is the password confirmed by user.

Default: None.

Command mode: Global Mode.

Usage Guide: Under the img mode, configure the password of entering the bootrom mode next time; under the global mode, input this command and the password according to the prompt and confirm it, then successfully to configure. Notice: the characters length of the password is from 3 to 32.

Example:

switch(config)#set boot password

New password :*****

Confirm password :*****

Set password success!

1.1.1.35 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.

1.1.1.36 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

1.1.1.37 show cpu usage

Command: show cpu usage [<slotno>]

Function: Show CPU usage rate.

Command mode: Admin and configuration mode.

Usage Guide: Check the current usage of CPU resource by **show cpu usage** command. Only **the *chassis switch*** uses **slotno** parameter which is used to show the CPU usage rate of the card on specified slot, if there is no parameter, the default is current card.

Example: Show the current usage rate of CPU.

Switch#show cpu usage

Last 5 second CPU IDLE: 87%

Last 30 second CPU IDLE: 89%

Last 5 minute CPU IDLE: 89%

From running CPU IDLE: 89%

1.1.1.38 show cpu utilization

Command: show cpu utilization

Function: Show the current CPU utilization rate.

Parameter: None.

Default: None.

Command mode: Admin mode.

Usage Guide: This command is used to show CPU utilization rate in the past 5 seconds, 30 seconds and 5 minutes.

Example: Show CPU utilization rate.

Switch#show cpu utilization

Last 5 second CPU USAGE: 9%

Last 30 second CPU USAGE: 11%

Last 5 minute CPU USAGE: 11%

From running CPU USAGE: 11%

1.1.1.39 show memory usage

Command: show memory usage [<slotno>]

Function: Show memory usage rate.

Command mode: Admin and configuration mode.

Usage Guide: Check the current usage of memory resource by **show memory usage** command. Only **the *chassis switch*** uses **slotno** parameter which is used to show the memory usage rate of card on the specified slot, if there is no parameter, the default is current card.

Example: Show the current usage rate of the memory.

Switch#show memory usage

The memory total 128 MB, free 58914872 bytes, usage is 56.10%

1.1.1.40 show privilege

Command: show privilege

Function: Show privilege of the current users.

Parameter: None.

Command Mode: All configuration modes

Example: Show privilege of the current user.

Switch(Config)#show privilege

Current privilege level is 15

1.1.1.41 show privilege mode LINE

Command: show privilege mode LINE

Function: Show the level of the specified command.

Parameters: mode: register mode of the command, 'Tab' or '?' is able to show all register modes

LINE: the command needs to be configured, it supports the command abbreviation

Command Mode: Admin and configuration mode

Usage Guide: LINE must be the whole command format, the abbreviation format is used to the command which can be analyzed successfully. For half-baked command, false command about writing and command that abbreviation cannot be analyzed successfully, the level of them cannot be shown.

Example: Show the level of **privilege** command.

Switch(config)#show privilege exec show ip route

The command : show ip route

Privilege is : 15

1.1.1.42 show tcam usage

This command is not supported by the switch.

1.1.1.43 show temperature

This command is not supported by the switch.

1.1.1.44 show tech-support

Command: show tech-support [no-more]

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.

Parameter: no-more: Display the operational information and the task status of the switch directly, do not connect the user by “more”.

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

1.1.1.45 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 of the switch, it includes the hardware version and the software version information.

Example:

Switch#show version.

1.1.1.46 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 username, its range should not exceed 32 characters. **<*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 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted (Use 32 bits password encrypted by MD5).

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
4a7d1ed414474e4033ac29ccb8653d9b (The password is 32 bits password encrypted by MD5)
Switch(config)# username user2 password 0 user2
Switch(config)# authentication line console login local

1.1.1.47 web-auth privilege <1-15>

Command: web-auth privilege <1-15>
no web-auth privilege

Function: Configure the level of logging in the switch by web.

Parameter: <1-15>: Appoint the level of logging in the switch by web and the range is from 1 to 15.

Command Mode: Global Mode.

Default: 15.

Usage Guide: After configured the level of logging in the switch by web, only the user with the level that is equal to or higher than it can login in the switch by web.

Example: Configure the level of logging in the switch by web as 10.

Switch(config)# web-auth privilege 10

1.1.1.48 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.

1.1.1.49 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 specified configuration file, 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.

1.1.1.50 write running-config

Command: write running-config [<*startup-config-file-name*>]

Function: Save the current running config as .cfg file to Flash Memory.

Parameters: <*startup-config-file-name*> is the full path of the cfg file. The format of which is as follows:

1. The file path comprises of two parts: device prefix used as the root directory (flash:/) and the file name. No space is allowed in each part or between two parts.

2. The suffix of all file names should be .cfg.

3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.

Command Mode: Admin Mode.

Usage Guide: Config file saved by Flash Memory can be used for startup file.

Example: Save the current running config as .cfg file with name of 123.

Switch#write running-config 123.cfg

1.1.2 Telnet

1.1.2.1 aaa authorization config-commands

Command: aaa authorization config-commands

no aaa authorization config-commands

Function: Enable command authorization function for the login user with VTY (login with Telnet and SSH). The no command disables this function. Only enabling this command and configuring command authorization manner, it will request to authorize when executing some command.

Default: Disable.

Command Mode: Global Mode.

Usage Guide: Only after configuring this command and configuring command authorization manner and authorization selection priority of login user with VTY, it can be authorized when configuring command with corresponding command level for login user with VTY.

Example: Enable VTY command authorization function.

Switch(config)# aaa authorization config-commands

1.1.2.2 accounting exec

Command: accounting line {console | vty} exec {start-stop | stop-only | none} method1 [method2…]

no accounting line {console | vty} exec

Function: Configure the list of the accounting method for the login user with VTY (login with Telnet and SSH) and Console. The no command restores the default accounting method.

Parameters: line selects the accounting line, including **console**, **vty** (telnet and ssh); **start-stop** sends the accounting start or the accounting stop when the user is logging or exit the login; **stop-only** sends the accounting stop when the user exits the login only; **none** does not send the accounting start or the accounting stop; **method** is the list of the accounting method, it only supports **tacacs** keyword; **tacacs** uses the remote TACACS+ server to count.

Default: There is no accounting.

Command Mode: Global Mode.

Usage Guide: console and **vty** login method are able to set the corresponding accounting method respectively, the accounting method only supports TACACS+ method currently.

Example: Configure the login accounting with the telnet method.

Switch(config)#accounting line vty exec start-stop tacacs

1.1.2.3 accounting command

Command: accounting line {console | vty} command <*1-15*> {start-stop | stop-only | none} method1 [method2…]

no accounting line {console | vty} command <*1-15*>

Function: Configure the list of the command accounting method with VTY (login with Telnet and SSH) and Console. The no command restores the default accounting method.

Parameters: line selects the accounting line, including **console**, **vty** (telnet and ssh); **command <*1-15*>** is the level of the accounting command; **start-stop** sends the accounting start or the accounting stop when the user is logging or exit the login; **stop-only** sends the accounting stop when the user exits the login only; **none** does not send the accounting start or the accounting stop; **method** is the list of the accounting method, it only supports **tacacs** keyword; **tacacs** uses the remote TACACS+ server to count.

Default: There is no accounting method.

Command Mode: Global Mode.

Usage Guide: console and **vty** login method are able to set the corresponding command accounting method respectively, the accounting method only supports TACACS+ method currently. Only the stop information of the accounting is recorded, whether command accounting configures start-stop method or stop-only method.

Example: Configure the command accounting with the telnet method.

Switch(config)#authorization line vty command 15 start-stop tacacs

1.1.2.4 authentication enable

Command: authentication enable method1 [method2…]

no authentication enable

Function: Configure the list of the enable authentication method. The no command restores the default authentication method.

Parameters: method is the list of the authentication method, it must be among **local**, **tacacs** and **radius** keywords; **local** uses the local database to authenticate; **tacacs** uses the remote TACACS+ authentication server to authenticate; **radius** uses the remote RADIUS authentication server to authenticate.

Default: The local authentication is enable command by default.

Command Mode: Global Mode.

Usage Guide: The enable authentication method can be any one or combination of Local, RADIUS and 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 corresponding 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.

Example: Configure the enable authentication method to be tacacs and local.

Switch(config)#authentication enable tacacs local

1.1.2.5 authentication ip access-class

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

no authentication ip access-class

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

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

1.1.2.6 authentication ipv6 access-class

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

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 and 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 in

1.1.2.7 authentication line login

Command: authentication line {console | vty | web} login method1 [method2…]

no authentication line {console | vty | web} login

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

Parameters: line selects the login line, including **console**, **vty** (telnet and ssh) and **web**; **method** is the list of the authentication method, it must be among **local**, **tacacs** and **radius** keywords; **local** uses the local database to authenticate; **tacacs** uses the remote TACACS+ authentication server to authenticate; **radius** uses the remote RADIUS authentication server to authenticate.

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 and 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 corresponding 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 telnet and ssh login with the remote RADIUS authentication.

Switch(config)#authentication line vty login radius

Relative Command: aaa enable，radius-server authentication host，tacacs-server authentication host， tacacs-server key

1.1.2.8 authentication securityip

Command: authentication securityip <*ip-addr*>

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

1.1.2.9 authentication securityipv6

Command: authentication securityipv6 *<ipv6-addr>*

no authentication securityipv6 *<ipv6-addr>*

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

Parameters: *<ipv6-addr>* is the security IPv6 address which can login the switch.

Default: No security 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 security IPv6 address is not configured. After the security IPv6 address is configured, only clients with security IPv6 addresses are able to login the switch. Up to 32 security IPv6 addresses can be configured in the switch.

Example: Configure the security IPv6 address is 2001:da8:123:1::1.

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

1.1.2.10 authorization

Command: authorization line {console | vty | web} exec method [method…]

no authorization line {console | vty | web} exec

Function: Configure the list of the authorization method for the login user with VTY (login with Telnet and SSH), Web and Console. The no command restores the default authorization method.

Parameters: line selects the authorization line, including **console**, **vty** (telnet and ssh) and **web**; **method** is the list of the authorization method, it must be among **local**, **tacacs** and **radius** keywords; **local** uses the local database to authorize; **tacacs** uses the remote TACACS+ server to authorize; **radius** uses the remote RADIUS server to authorize.

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 corresponding 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 authorization method to RADIUS.

Switch(config)#authorization line vty exec radius

1.1.2.11 authorization line vty command

Command: authorization line vty command <1-15> {local | radius | tacacs} (none|)

no authorization line vty command <1-15>

Function: Configure command authorization manner and authorization selection priority of login user with VTY (login with Telnet and SSH). The no command recovers to be default manner.

Default: The authorization manner is not configured as default.

Command Mode: Global Mode.

Usage Guide: Configure the authorization manner when VTY login user configures command, the manners include any combination of Local, RADIUS and TACACS, the manner of none is just as the last manner. When using combination authorization manners, the priority of the front authorization manner is the highest and the others are in descending order; if the authorization with high priority passed, it is successful to configure command and the back authorization manner will be ignored. Notice: as long as one authorization manner receives a clear response of the corresponding agreement. Whether it is received or refused, the next authorization manner will not be attempted. If the clear response is not received, try the next manner. When using RADIUS authorization, AAA function must be enabled and configure RADIUS server. when using TACACS authorization, TACACS server must be configured. None is the manner of escaping and it only can be the last manner. This manner returns to passed authorization directly and it is successful to configure the command.

Example: Configure level 1 command authorization manner of telnet login user as TACACS.

Switch(config)#authorization line vty command 1 tacacs

1.1.2.12 clear line vty <0-31>

Command: clear line vty <0-31>

Function: Delete the logged user information on the appointed line, force user to get down the line who logs in through telnet or ssh.

Command mode: Admin Mode.

Usage guide: After inputting this command, there is need to judge for this command, "Confirm[Y/N]: ", when inputting "Y" or "y", run to delete; when inputting "？ ", do not run to delete, print the notice information only. When inputting other characters, do not run to delete.

1.1.2.13 crypto key clear rsa

Command: crypto key clear rsa
Function: Clear the secret key of ssh.
Command mode: Admin Mode.

1.1.2.14 terminal length

Command: terminal length <0-512>
terminal no length
Function: Set length of characters displayed in each screen on terminal; the "**terminal no length**" cancels the screen switching operation and display content once in all.
Parameter: Length of characters displayed in each screen, ranging between 0-512 (0 refers to non-stop display).
Command mode: Admin Mode.
Default: Default Length is 25.
Usage guide: Set length 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. Default length is 25.
Example: Configure length of characters in each display to 20.
Switch#terminal length 20

1.1.2.15 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

1.1.2.16 telnet

Command: telnet [vrf <*vrf-name*>] {<*ip-addr*> | <*ipv6-addr*> | host <*hostname*>} [<*port*>]
Function: Login on the remote host by Telnet

Parameter: ***<vrf-name>*** is the specific VRF name; ***<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 64 characters; ***<port>*** is the port number, ranging between 0 and 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:***
router>

1.1.2.17 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

1.1.2.18 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

1.1.2.19 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

Usage Guide: None.

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

Example: Set the time for retrying SSH authentication to 5.

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

1.1.2.20 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

1.1.2.21 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

1.1.2.22 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

1.1.2.23 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.

Usage Guide: This command is used to set SSH authentication timeout, the default timeout is 180 seconds.

Example: Set SSH authentication timeout to 240 seconds.

Switch(config)#ssh-server timeout 240

1.1.2.24 show crypto key

Command: show crypto key

Function: Show the secret key of ssh.

Command mode: Admin Mode.

1.1.2.25 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

1.1.2.26 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

1.1.2.27 show users

Command: show users

Function: Show the user information who logs in through telnet or ssh. It includes line number, user name and user IP.

Command mode: Admin Mode.

Usage Guide: When inputting this command, show the user information who logs in through telnet or ssh. It includes line number, user name and user IP. Because 16 telnet users and 16 ssh users are supported at most currently, vty0-15 are used for telnet, and 16-31 are used for ssh.

Example:

Switch#show users

Line	User	Location
vty 16	a	192.168.1.1
vty 0	admin	192.168.1.2
vty 17	mab	192.168.1.13
vty 1	test	192.168.1.40

1.1.2.28 who

Command: who

Function: Show the current login users with vty.

Parameter: None.

Command Mode: All configuration modes

Example: Show the current login users with vty.

Switch#who

Telnet user a login from 192.168.1.20

1.1.3 Configuring Switch IP

1.1.3.1 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)#

1.1.3.2 interface ethernet 0

This command is not supported by the switch.

1.1.3.3 ip address

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

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

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

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

Default: No IP address is configured upon switch shipment.

Command mode: VLAN Interface Mode

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

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

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip address 10.1.128.1 255.255.255.0

Switch(Config-if-Vlan1)#exit

Switch(config)#

Relative Command: ip bootp-client enable, ip dhcp-client enable

1.1.3.4 ipv6 address

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

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

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

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

Command Mode: Interface Configuration Mode.

Default: None.

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

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

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

1.1.3.5 ip bootp-client enable

Command: ip bootp-client enable

no ip bootp-client enable

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

Default: BootP client function is disabled by default.

Command mode: VLAN Interface Mode

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

Example: Get IP address through BootP.

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip bootp-client enable

Switch (Config-if-Vlan1)#exit

Switch(config)#

Relative command: ip address, ip dhcp-client enable

1.1.3.6 ip dhcp-client enable

Command: ip dhcp-client enable

no ip dhcp-client enable

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

Default: the DHCP client function is disabled by default.

Command mode: VLAN Interface Mode

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

Example: Getting an IP address through DHCP.

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip dhcp-client enable

Switch(Config-if-Vlan1)#exit

Switch(config)#

1.1.3.7 ip dhcp-client upgrade enable

Command: ip dhcp-client upgrade enable

no ip dhcp-client upgrade enable

Function: Enables the switch to realize the automatic upgrade function of img / cfg file through DHCP option66 and option 67; the no operation of this command is to close the function of automatic upgrade of img / cfg file through DHCP option66 and option 67.

Default: The automatic upgrade function of DHCP client is disabled by default.

Command mode: VLAN Interface Mode.

Usage Guide: Enables the switch to realize the automatic upgrade function of img / cfg file through DHCP option66 and option 67.

Example: Enables DHCP automatic upgrade function.

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip dhcp-client enable

Switch(Config-if-Vlan1)#ip dhcp-client upgrade enable

Switch(Config-if-Vlan1)#exit

Switch(config)#

Relative command: ip dhcp-client enable

1.1.3.8 ip dhcp-client upgrade begin

Command: ip dhcp-client upgrade begin

Function: Starts up the switch to realize the automatic upgrade function of img / cfg file through

DHCP option66 and option 67.

Default: The automatic upgrade function of DHCP client is closed by default.

Command mode: VLAN Interface Mode.

Usage Guide: Starts up the switch to realize the automatic upgrade function of img / cfg file through DHCP option66 and option 67.

Example: Starts up DHCP automatic upgrade function.

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

Relative command: ip dhcp-client enable, ip dhcp-client upgrade enable

1.1.4 SNMP

1.1.4.1 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

1.1.4.2 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

1.1.4.3 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 enabled by default.

Example:

Enable RMON.

Switch(config)#rmon enable

Disable RMON.

Switch(config)#no rmon enable

1.1.4.4 show private-mib oid

Command: show private-mib oid

Function: Show the original oid of the private mib.

Command mode: Admin and configuration mode.

Usage Guide: Check the beginning oid of the private mib by **show private-mib oid** command.

Example: Show the original oid of the private mib.

Switch#show private-mib oid

Private MIB OID:1.3.6.1.4.1.6339

1.1.4.5 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.

1.1.4.6 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

1.1.4.7 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

1.1.4.8 show snmp mib

Command: show snmp mib

Function: Display all MIB supported by the switch.

Command Mode: Admin and Configuration Mode.

1.1.4.9 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

1.1.4.10 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

1.1.4.11 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

1.1.4.12 snmp-server community

Command: snmp-server community {ro | rw} {0 | 7} *<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 command deletes the configured community string.

Parameter: ***<string>*** is the configured community string. If key option is set as 0, the specified community string is not encrypted, if key option is set as 7, the specified community string is encrypted;

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 rw 0 private

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

Switch(config)#snmp-server community ro 0 public

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

Switch(config)# snmp-server community ro 0 private

Delete community string “private”.

Switch(config)#no snmp-server community 0 private

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

Switch(config)#snmp-server community ro 0 public read pviewr

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

Switch(config)#snmp-server community rw 0 private read pviewr write pvieww

1.1.4.13 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

1.1.4.14 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: Forbid to send Trap message.

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

1.1.4.15 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

1.1.4.16 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

Delete group

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

1.1.4.17 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>*** is IP address of NMS management station which receives Trap message.

<host-ipv6-addr> is IPv6 address of NMS management 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 to configure IPv4 or IPv6 addresses of SNMP management station that receive Trap message at the same time, but IPv4 and IPv6 addresses of v1 and v2c version 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 an IPv6 address to receive Trap.

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

1.1.4.18 snmp-server packet delay

Command: snmp-server packet delay (0|10|20)

no snmp-server packet delay

Function: The delayed time of snmp receiving packets.

parameters: (0|10|20) is the delayed time and the unit is ms.

Command Mode: Global Mode.

Default: 10ms.

Usage Guide: The snmp function must be enabled before use this function.

Example: Configure the delayed time of snmp receiving packets as 20 ms.

Switch(config)#snmp-server packet delay 20

1.1.4.19 snmp-server securityip

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

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

Function: Configure security IPv4 or IPv6 address allowed to access NMS management station; the no command deletes security IPv4 or IPv6 address configured.

Command Mode: Global Mode.

Parameter: <ipv4-address> is NMS security IPv4 address, dotted decimal notation.

<ipv6-address> is NMS security IPv6 address, colon hexadecimal.

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 20 in all.

Example:

Configure security IP address of NMS management station.

Switch(config)#snmp-server securityip 1.1.1.5

Delete security IPv6 address.

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

1.1.4.20 snmp-server securityip

Command: snmp-server securityip {enable | disable}

Function: Enable/disable the security IP address authentication on NMS management station.

Command Mode: Global Mode

Default: Enable the security IP address authentication function.

Example:

Disable the security IP address authentication function.

Switch(config)#snmp-server securityip disable

1.1.4.21 snmp-server trap-source

Command: snmp-server trap-source {<ipv4-address> | <ipv6-address>}

no snmp-server trap-source {<ipv4-address> | <ipv6-address>}

Function: Set the source IPv4 or IPv6 address which is used to send trap packet, the no command deletes the configuration.

Parameter: <ipv4-address>: IPv4 address is used to send trap packet in dotted decimal notation

<ipv6-address>: IPv6 address is used to send trap packet in colon hexadecimal.

Command Mode: Global Mode.

Usage Guide: If there is no configuration, select the source address according to the interface address sent by actual trap packet, when configure the IP address, adopt the configured source address as the source address of trap packet.

Example:

Set the IP address which is used to send trap packet.

Switch(config)#snmp-server trap-source 1.1.1.5

Delete the configured source address which is used to send IPv6 trap packet.

Switch(config)#no snmp-server trap-source 2001::1

1.1.4.22 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

Delete an User

Switch (config)#no snmp-server user tester

1.1.4.23 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

1.1.4.24 switchport updown notification enable

Command: [no] switchport updown notification enable

Function: Enable/disable the function of sending the trap message to the port of UP/DOWN event.

Default: Send the trap message to the port of IP/DOWN event as default.

Command Mode: Port Mode.

Usage Guide: This command can control to send the trap message when the port happens the UP/DOWN event or not. As default, send the trap message to all the ports of UP/DOWN event after enabled snmp trap.

Example: Disable the function of sending the trap message to the port 1/0/1 of the UP/DOWN event.

Switch(config)#in e 1/0/1

Switch(config-if-ethernet1/0/1)#no switchport updown notification enable

Switch(config-if-ethernet1/0/1)#show running-config current-mode

!

Interface Ethernet1/0/1

no switchport updown notification enable

1.1.5 Switch Upgrade

1.1.5.1 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	It means the reboot configuration files when using copy running-config startup-config command
nos.img	System files
boot.rom	System startup files
stacking/nos.img	As destination address, execute system files upgrade for Slave in stacking mode
stacking/nos.rom	As destination address, execute system startup files upgrade for Slave in stacking mode

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

1.1.5.2 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 a 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	It means the reboot configuration files when using copy running-config startup-config command
nos.img	System files
boot.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

1.1.5.3 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.

1.1.5.4 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

1.1.5.5 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

1.1.5.6 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, its range should not exceed 32 characters; **<*password*>** is the password of the FTP link, if input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted.

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)#

1.1.5.7 show ftp

Command: show ftp

Function: Display the parameter settings for the FTP server.

Command mode: Admin and Configuration Mode.

Default: Do not display.

Example:

Switch#show ftp

Timeout : 600

Displayed information	Description
Timeout	Timeout time.

1.1.5.8 show tftp

Command: show tftp

Function: Display the parameter settings for the TFTP server.

Default: Do not display.

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.

1.1.5.9 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: Disable TFTP Server.
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

1.1.5.10 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: Retransmit 5 times.
Command mode: Global Mode
Example: Modify the retransmission to 10 times.
Switch#config
Switch(config)#tftp-server retransmission-number 10

1.1.5.11 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

1.1.5.12 show archive running-config

Command：show archive running-config

Function： Display all settings information for the configuration archive.

Parameters： None.

Default： None.

Command mode： Admin and Configuration Mode.

Usage Guide： Directly enter the show archive running-configuration command to display all settings information for the configuration archive.

Example： Display all settings information for the configuration archive.

switch1#show archive running-config

Current Period: 1 Hours(Default Value: 24 Hours)

Current Maximum: 30 Files(Default Value: 30 Files)

Current ServerType: TFTP, ServerIp: 1.1.1.254, Filename: ab.cfg

Previous Upload Time: %Nov 08 09:22:19 2019 , Status: Successfull, Filename: ab3.cfg

1.1.5.13 archive running-config

Command：archive running-config {location WORD | maximum<1-100> |period<1-3600> }

no archive running-config

Function： After executing this command, the system will automatically archive the configuration file to the specified path; The no operation of this command will cancel this function.

Parameters：location WORD： The server path to which the configuration archive files are located,file path example ftp: //user: password@s erverIp/filename or tftp: //serverIp/ filename.

maximum<1-100>： Maximum number of files,the valid range is 1-100,the default value is 30.

period<1-3600>： Time interval for archive,the valid range is 1-3600 hours,the default value is 24 hours.

Default： None.

Command mode： Global Configuration Mode.

Usage Guide： Use this command to specify the file path, maximum number of files, and backup interval for the configuration archive.

Example： Archive the configuration file of the switch.

switch1(config)#archive running-config location tftp://172.17.100.42/1314.cfg

Begin to send file, please wait...

File transfer complete.

%Feb 27 04:42:54 2012 Sending running-config to TFTP server 172.17.100.42 13141.cfg Successfull!

Modification interval and maximum number of files:

switch1(config)#archive running-config maximum 10

Begin to send file, please wait...

File transfer complete.

%Feb 27 07:30:01 2012 Sending running-config to TFTP server 172.17.100.42 13141.cfg

Successfull!
switch1(config)#archive running-config period 1
Begin to send file, please wait...
File transfer complete.
%Feb 27 07:30:07 2012 Sending running-config to TFTP server 172.17.100.42 13141.cfg Successfull!

1.1.6 Boot Configuration

1.1.6.1 baudrate

Command: baudrate *<value>*
Function: This command is used to configure the baud rate of the switch.
Parameters: ***<value>*** is the baud rate, the baud rate the switch supported currently are 9600,14400,19200,38400,57600,115200.
Default: 9600.
Command Mode: Boot Mode.
Usage Guide: This command is used to configure the appropriate baud rate when transmitting the files under the xmodem mode. The baud rate of the switch must be the same as the baud rate of the serial port software in PC.
Example: Configure the baud rate of the switch as 115200 when transmitting the files under the xmodem mode.
[Boot]: baudrate 115200

1.1.6.2 boot img

Command: boot img *<img-file-url>* {primary | backup}
Function: Configure the first and second starting of img files of the switch.
Parameters: primary means to configure the first starting of IMG file, **backup** means to configure the second starting of IMG file, ***<img-file-url>*** is the full path of the booting IMG file.
Command mode: Boot mode.
Default: There is only the first booting IMG file which is nos.img file in the FLASH, the second booting IMG file is free.
Usage Guide: Configure the first and second starting of img files of the switch through this command. If the first booting img file failed, the system will start the second automatically. The format of the img full path is as follows:
1. The file path comprises of two parts: device prefix used as the root directory (flash:/) and the file name. No space is allowed in each part or between those two parts.
2. The suffix of all file names must be .img.
3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.
Example: Configure the first starting of img files of the switch as flash:/nos.img.

[Boot]: boot img flash:/nos.img primary

1.1.6.3 boot startup-config

Command: boot startup-config *<file-url>*

Function: Configure the CFG file used in the next booting of the switch.

Parameters: *<file-url>* is the full path of CFG file used in the next booting.

Command Mode: Boot Mode.

Default: Null as default.

Usage Guide: Configure the CFG file used in the next booting of the switch through this command. The file name must include the suffix of .cfg. The format of the full path is as follows:

1. The file path comprises of two parts: device prefix used as the root directory (flash:/) and the file name. No space is allowed in each part or between those two parts.

2. The suffix of all file names must be .cfg.

3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.

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

[Boot]: boot startup-config flash:/ startup-config

1.1.6.4 clearconfig

Command: clearconfig

Function: Recover bootrom parameters to be the default.

Parameters: None.

Command Mode: Boot Mode.

Default Settings: None.

Usage Guide: Recover bootrom parameters to be the default through this command.

Example: Recover bootrom parameters to be the default.

[Boot]: clearconfig

Network interface configure OK.

Boot config set Ok.

1.1.6.5 Copy

This command is not supported by the switch.

1.1.6.6 Delete

This command is not supported by the switch.

1.1.6.7 dir

Command: dir

Function: Display the files list and property in the current switch.

Default: None.

Command mode: Boot Mode.

Usage guide: Input this command will display the name and size of the file.

Example: View the files list and property in the current switch. Notice: the rom file will not be shown.

```
[[Boot]: dir
   1461094      nos.img.ecc
     91393      mantest.img.ecc
  41559526      nos.img
   2599038      mantest.img
      1547      startup.cfg

5 file(s), 0 dir(s)

Total size:64483328 bytes , used size:45851648 bytes, free size:18631680 bytes
```

1.1.6.8 help

Command: h

help

Function: Show the commands and the function explanation which are supported by the current bootRom.

Default: None

Parameters: None.

Command Mode: Boot Mode.

Usage Guide: View the explanation of the commonly used commands.

Example: Print the explanation of the commonly used commands.

```
[Boot]: help
baudrate                - set the baudrate
boot                    - select the active bootimg image file or startup-config file
clearconfig             - set default bootrom configurations
copy <src> <dst>        - copy a file
delete <filename>       - delete a file
dir                     - display the contents of the current directory
h                       - print help list
help                    - print help list
load <filename>         - load system image(binary format)
nobootpassword          - no bootpassword for setup
ping <x.x.x.x>          - ping test
reboot                  - reboot system
saveconfig              - save bootrom configurations
```

setbootpassword - set boot password
setconfig - set bootrom configurations
show - show machine info
showconfig - show bootrom configurations
write <filename> - write file to flash; file gotten by 'load'
xmodem - load file by xmodem

1.1.6.9 load

Command: load*<filename>*
Function: Download files through the TFTP.
Parameters: *<filename>* is the name of file to be downloaded.
Command Mode: Boot Mode.
Usage Guide: Download files through the TFTP by inputting the load + filename command.
Example: Download boot.img file.
[Boot]:load boot.img

1.1.6.10 nobootpassword

Command: nobootpassword
Function: Clear the password which is used to enter into the boot.
Parameter: None.
Default: None.
Command mode: Boot Mode.
Usage Guide: Clear password which is used to enter into the boot through this command.
Example: Clear password which is used to enter into the boot.
[Boot]: nobootpassword
clear password ok

1.1.6.11 ping

Command: ping *<x.x.x.x>*
Function: Test the network connection.
Parameters: *< x.x.x.x >* is the ip address to ping and it is the ip address of the pc generally.
Command Mode: Boot Mode.
Default: None.
Usage Guide: This command is used to test the network connection. It is like the ping command of PC, but there is no optional parameters and it can only ping the PC from the switch.
Examples: Test the network connection of 192.168.0.1.
[Boot]:ping 192.168.0.1

1.1.6.12 reboot

Command: reboot

Function: Reboot the switch.

Parameters: None

Default: none

Command mode: Boot Mode

Usage Guide: Reboot the switch in warm mode

Example: Reboot the switch.

[Boot]:reboot

1.1.6.13 saveconfig

Command: saveconfig

Function: Save the configuration of bootrom.

Parameters: None.

Default: None.

Command mode: Boot Mode.

Usage Guide: Save the configuration of bootrom through this command.

Example: Save the configuration of bootrom.

[Boot]: saveconfig

change boot params is OK

1.1.6.14 setbootpassword

Command: setbootpassword

Function: Set the password which is used to enter into the boot.

Parameters: None.

Default: There is no password which is used to enter into the boot as default.

Command mode: Boot Mode.

Usage Guide: Set password which is used to enter into the boot. The length of the password cannot be less than 3 and larger than 32.

Example: Set the password which is used to enter into the boot.

[Boot]: setbootpassword

Password:******

Confirm Password:******

Password has been set successfully!

1.1.6.15 setconfig

Command: setconfig

Function: Set the configuration parameters of bootrom.

Parameters: None.

Default: The Host IP is 10.1.1.1 and the Server IP is 10.1.1.2 as default.

Command mode: Boot Mode.

Usage Guide: Set the configuration parameters of bootrom through this command. The two parameters which are used to configure the Host IP and Server IP only support TFTP protocol currently.

Example: Set the configuration parameters of bootrom.

[Boot]: setconfig

Host IP Address: [10.1.1.1] 192.168.1.1

Server IP Address: [10.1.1.2] 192.168.1.2

1.1.6.16 show

Command: show [board|config|boot-files|partition]

Function: Show the configuration of the corresponding switch.

Parameters: board is the parameter information of switch, such as type, mac, sn and etc. **config** is the configuration parameter of the current bootrom; **boot-files** is the configuration parameter of first /second img files and cfg files; **partition** is the partition of flash.

Default: None.

Command mode: Boot Mode.

Usage Guide: show board is used to show the parameters information of switch, such as type, mac, sn and etc. **Show config** is used to show the configuration parameter of bootrom; **show boot-files** is used to show the configuration parameter of first /second img files and cfg files; **show partition** is used to show the partition of flash.

Example: Show the configuration of first img files.

[Boot]: show boot-files

The primary img file : flash:/1.img

The backup img file : flash:/nos.img

1.1.6.17 showconfig

Command: showconfig

Function: Show the configuration parameter of bootrom, this command is the same as **show config** command.

Parameters: None.

Default: None.

Command mode: Boot Mode.

Usage Guide: Show the user configuration of bootrom.

Example: Show the configuration parameter of bootrom.

[Boot]: showconfig

Host IP Address: 192.168.1.1

Server IP Address: 192.168.1.2

1.1.6.18 write

Command: write *<filename>*

Function: Write the file which was downloaded before into the memory such as flash.

Parameters: *<filename>* is the name of the file which will be written into the memory.

Default: None.

Command mode: Boot Mode.

Usage Guide: Write the file which was downloaded before into the flash or bootrom.

Example: Write the boot.room file in the flash and name it as boot.room.

[Boot]:write boot.room

1.1.6.19 xmodem

Command: xmodem

Function: The command is used to transmit the files through the Xmodem protocol under the bootrom.

Parameters: None.

Default: None.

Command mode: Boot Mode.

Usage Guide: In order to improve the transmission rate, the higher baud rate is suggested (baudrate command). After this command was enabled, the switch will enter into the xmodem reception status. In this time, the PC should run the xmodem transmission through the software which supports the xmodem. (realtek only supports download, not support upload)

Example: Make switch enter into the Xmodem mode.

[Boot]: xmodem

Ready for binary (xmodem) download to 0x04400000 at 9600 bps...

1.2 File System

1.2.1 cd

Command: cd <*directory*>

Function: Change the working directory for the storage device.

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

Command Mode: Admin Mode.

Default Settings: The default working directory is Flash.

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

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

Switch#cd flash:

Switch#pwd
flash:/
Switch#

1.2.2 copy

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

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

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

1. The prefix of the source file URL should be in one of the following forms:

- starting with “flash:/”
- “ftp://username:pass@server-ip/file-name”
- “tftp://server-ip/file-name”

2. The prefix of the destination file URL should be in one of the following forms:

- starting with “flash:/”
- “ftp://username:pass@server-ip/file-name”
- “tftp://server-ip/file-name”

Command Mode: Admin Mode.

Default Settings: None.

Usage Guide:

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

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

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

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

Example: Copy the file “flash:/nos.img” and store it as “flash/ 6.1.11.0.img”.

Switch#copy flash:/nos.img flash:/nos-6.1.11.0.img
Copy flash:/nos.img to flash:/nos-6.1.11.0.img? [Y:N] y
Copyed file flash:/nos.img to flash:/nos-6.1.11.0.img.

1.2.3 delete

Command: delete <*file-url*>

Function: Delete the designate file on the storage device.

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

Command Mode: Admin Mode.
Default Settings: None.
Usage Guide: The designated file will be deleted after implementing this command.
Example: Delete file flash:/nos.img.
Switch#delete flash:/nos5.img
Delete file flash:/nos5.img?[Y:N]y
Deleted file flash:/nos.img.

1.2.4 dir

Command: dir [WORD]
Function: Display the information of the designated directory on the storage device.
Parameters: <WORD> is the name of the shown directory. There may be the following formats: directory name, slot-xx#directory name, flash:/directory name, cf:/directory name.
Command Mode: Admin Configuration Mode.
Default Settings: No <WORD> means to display information of the current working directory.
Usage Guide: Implementing this command will display information of files and sub-directories in the designated directory.
Note: This command does not support a recursive display of all sub-directories.
Example: Display information of the directory “flash:/”.
Switch#dir flash:/
nos.img 2,449,496 1980-01-01 00:01:06 ----
startup-config 2,064 1980-01-01 00:30:12 ----
Total 7, 932, 928 byte(s) in 4 file(s)， free 4, 966, 400 byte(s)
Switch#

1.2.5 Format

This command is not supported by the switch.

1.2.6 mkdir

This command is not supported by the switch.

1.2.7 mount

This command is not supported by the switch.

1.2.8 pwd

Command: pwd
Function: Display the current working directory.
Parameters: None.

Command Mode: Admin Mode.

Default Settings: The default directory is flash.

Example: Display the current working directory.

Switch#pwd

flash:/

Switch#

1.2.9 rename

Command: rename <*source-file-url*> <*new-filename* >

Function: Rename a designated file on the switch.

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

Command Mode: Admin Mode.

Default Settings: None.

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

Example: Change the name of file "nos.img" in the current working directory to "nos-6.1.11.0.img".

Switch# rename nos5.img nos-6.1.11.0.img

Rename flash:/nos5.img to flash:/nos-6.1.11.0.img ok!

1.2.10 rmdir

This command is not supported by the switch.

1.2.11 unmount

This command is not supported by the switch.

1.2.12 md5sum

Command: md5sum <*file-url*>

Function: calculate the md5 value of the specified file on the storage device.

Parameters: ***<file-url>*** is the full path of the file to be calculated.

Command Mode: Admin Mode.

Default Settings: None.

Usage Guide: The designated file will be calculated after implementing this command.

Example: calculate file flash:/nos.img。

Switch#md5sum flash:/nos.img

MD5 : 84e4353531c71afda206f8ab7834c132

calculate file on SM flash:/nos.img
Switch#md5sum slot-2#nos.img
MD5 : 84e4353531c71afda206f8ab7834c132

1.3 Cluster

1.3.1 clear cluster nodes

Command: clear cluster nodes [nodes-sn <*candidate-sn-list*> | mac-address <*mac-addr*>]
Function: Clear the nodes in the candidate list found by the commander switch.
Parameters: candidate-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 read, 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

1.3.2 cluster auto-add

Command: cluster auto-add
no cluster auto-add
Function: When this command is executed in the commander switch, the newly discovered candidate switches will be added to the cluster as a member switch automatically; the "**no cluster auto-add**" command disables this function.
Command mode: Global Mode
Default: This function is disabled by default. That means that the candidate switches are not automatically added to the cluster.
Usage Guide: After enabling this command on a commander switch, candidate switches will be automatically added as members.
Example: Enable the auto adding function in the commander switch.
Switch(config)#cluster auto-add

1.3.3 cluster commander

Command: cluster commander [*<cluster-name>*]

no cluster commander

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

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

Command mode: Global Mode

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

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

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

Switch(config)#cluster commander switch

1.3.4 cluster ip-pool

Command: cluster ip-pool *<commander-ip>*

no cluster ip-pool

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

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

Command mode: Global Mode

Default: The default address pool is 10.254.254.1.

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

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

Switch(config)#cluster ip-pool 10.254.254.10

1.3.5 cluster keepalive interval

Command: cluster keepalive interval *<second>*

no cluster keepalive interval

Function: Configure the interval of keepalive messages within the cluster.

Parameters: ***<second>:*** keepalive 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

1.3.6 cluster keepalive loss-count

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

no cluster keepalive loss-count

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

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

Default: The default value is 3.

Command Mode: Global Configuration Mode

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

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

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

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

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

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

Switch(config)#cluster keepalive loss-count 5

1.3.7 cluster member

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

***<member-id>*]}**

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

Function: On a commander switch, manually add candidate switches into the cluster created by it. The no command deletes the specified member switch to change it as candidate.

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

1.3.8 cluster member auto-to-user

Command: cluster member auto-to-user

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

Parameter: None.

Default: None.

Command Mode: Global Mode.

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

Example: change automatically added members to manually added ones.

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

1.3.9 cluster reset member

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

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

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

Default: Boot all member switches.

Command mode: Admin Mode.

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

Example: In the commander switch, reset the member switch 1.

Switch#cluster reset member 1

1.3.10 cluster run

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

no cluster run

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

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

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

Command mode: Global Mode

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

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

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

Example: Disable cluster function in the local switch.

Switch (config)#no cluster run

1.3.11 cluster update member

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

Function: Remotely upgrade member switches from the commander switch.

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

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

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

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

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

when src-url is a TFTP address, its form will be: tftp://<ipadress>/<filename>，in which

<ipadress>is the IP address of the TFTP server <filename> is the name of the file to be downloaded via.

Special keywords used in filename:

Keywords	source or destination address
startup-config	start the configuration file
nos.img	system file

Command mode: Admin Mode

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

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

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

1.3.12 debug cluster

Command: debug cluster {statemachine | application | tcp}

no debug cluster {statemachine | application | tcp}

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

Parameters: statemachine: print debugging when the switch status changes.

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

tcp: the TCP connection between the commander and the member.

Default: None.

Command Mode: Admin Mode.

Usage Guide: None.

Example: Enable the debug status changed on the switch.

Swtich#debug cluster statemachine

1.3.13 debug cluster packets

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

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

Function: Enable the debug; the no command disables the debug.

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 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 of receiving DP messages.

Switch#debug cluster packets DP receive

1.3.14 show cluster

Command: show cluster

Function: Display cluster information of the switch.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: None.

Example: Execute this command on different switches.

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

Switch#show cluster

Status: Enabled

Cluster VLAN: 1

Role: commander

IP pool: 10.254.254.1

Cluster name: MIS_zebra

Keepalive interval: 30

Keepalive loss-count: 3

Auto add: Disabled

Number of Members: 0

Number of Candidates: 3

----in a member ----------

Switch#show cluster

Status: Enabled

Cluster VLAN: 1

Role: Member

Commander Ip Address: 10.254.254.1

Internal Ip Address: 10.254.254.2

Commamder Mac Address: 00-12-cf-39-1d-90

---- a candidate ----------

Switch#show cluster

Status: Enabled

Cluster VLAN: 1

Role: Candidate

---- disabled ----------

Switch#show cluster

Status: Disabled

1.3.15 show cluster members

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

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

Parameters: member-id: member id of the switch.

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

Default: No parameters means to display information of all member switches.

Command Mode: Admin and Configuration Mode.

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

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

Switch#show cluster members

Switch#show cluster members id 1

1.3.16 show cluster candidates

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

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

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

mac-address： mac address of the candidate switch

Default: No parameters means to display information of all member switches.

Command Mode: Admin and Configuration Mode.

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

Example: Display configuration information of all cluster candidate switches.

Switch#show cluster candidates

Cluster Candidates:

SN Mac Description Hostname

--- ----------------- ----------------------- -----------------------

xxx xx-xx-xx-xx-xx-xx xxxxxxxxxxxxxxxxxxxxxx24 xxxxxxxxxxxxxxxxxxxxxx24

1 00-01-02-03-04-06 ES3528M

2 01-01-02-03-04-05 ES3528M MIS_zebra

1.3.17 show cluster topology

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

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

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

node-sn-list：the switch node sn.

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

No parameters means to display all topology information.

Command Mode: Admin and Configuration Mode.

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

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

Switch#show cluster topology

Role: commander(CM);Member(M);Candidate(CA);Other commander(OC);Other member(OM)

LV SN Description Hostname Role MAC_ADDRESS Upstream Upstream leaf

local-port remote-port node

== ========== ========== == ========== ========== ========== =

x xxx xxxxxxxxxx12 xxxxxxxxxx12 xx xx-xx-xx-xx-xx-xx xxxxxxxxxx12 xxxxxxxxxx12 x

1 1 ES4626H LAB_SWITCH_1 CM 01-02-03-04-05-01 -root- -root- -

2 ES4626H LAB_SWITCH_2 M 01-02-03-04-05-02 eth 1/0/1 eth 1/0/2 N

3 ES4626H LAB_SWITCH_3 CA 01-02-03-04-05-03 eth 1/0/1 eth 1/0/3 Y

4 ES4626H LAB_SWITCH_4 CA 01-02-03-04-05-04 eth 1/0/1 eth 1/0/4 Y

.....

2 2 ES4626H LAB_SWITCH_2 M 01-02-03-04-05-02 eth 1/0/1 eth 1/0/2 -

5 ES3528M LAB_SWITCH_1 OC 01-02-03-04-05-13 eth 1/0/1 eth 1/0/2 Y

6 ES3528M LAB_SWITCH_1 OM 01-02-03-04-05-14 eth 1/0/1 eth 1/0/3 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 ES4626H          LAB_SWITCH_2 M    01-02-03-04-05-02 eth 1/0/1       eth 1/0/2        -
     5  ES3528M           LAB_SWITCH_1  OC  01-02-03-04-05-13  eth  1/0/1       eth  1/0/2
Y
     6  ES3528M           LAB_SWITCH_1  OM  01-02-03-04-05-14  eth  1/0/1       eth  1/0/3
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: ES4626H
Hostname     : LAB_SWITCH_2
Upstream local-port: eth 1/0/1
Upstream node: 01-02-03-04-05-01
Upstream remote-port:eth 1/0/2
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: ES4626H
Hostname     : LAB_SWITCH_2
Upstream local-port: eth 1/0/1
Upstream node: 01-02-03-04-05-01
Upstream remote-port: eth 1/0/2
Upstream speed: 100full
```

1.3.18 rcommand commander

Command: rcommand commander

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

Parameter: None.

Default: None.

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

1.3.19 rcommand member

Command: rcommand member *<mem-id>*
Function: In the commander switch, this command is used to remotely manage the member switches in the cluster.
Parameter: ***<mem-id>*** commander the member id allocated by commander to each member, whose range is 1～128.
Default: None.
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 member-id 1.
Switch#rcommand member 1

Chapter 2 Commands for Layer 2 services

2.1 Port Configuration

2.1.1 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 kbps 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 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. If the actual bandwidth is not a integral multiple of chip bandwidth granularity, it will be modified automatically. For example, a chip bandwidth granularity is 64K, but the input bandwidth is 50, the bandwidth will be modified as 64K.

Bandwidth control is similar to broadcast suppression. There is granularity limitation for the chip; the switch support 16Kbps granularities. If the <Kbits> that user input is not the integer times of 16, the system will adjust to the integer times of 16 automatically and print the true limit value to user.

Example: Set the bandwidth limit of 1/0/1-8 port is 40000K.

Switch(config)#interface ethernet 1/0/1-8

Switch(Config-If-Port-Range)#bandwidth control 40000 both

2.1.2 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 port1/0/1.
Switch#clear counters interface ethernet 1/0/1

2.1.3 description

Command: description *<string>*
no description
Function: Set name for specified port; the no command cancels this configuration.
Parameter: ***<string>*** is a character string, which should not exceeds 200 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 1/0/1-2 ports which is used by financial department, engineering as the name of 1/0/9 ports which belongs to the engineering department, while the name of 1/0/12 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 description of 1/0/1-2 port as financial.
Switch(config)#interface ethernet 1/0/1-2
Switch(Config-If-Port-Range)#description financial

2.1.4 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 ports 1/0/1-8.

Switch(config)#interface ethernet 1/0/1-8

Switch(Config-If-Port-Range)#flow control

2.1.5 hardware profile module <1-4> 4×10G

This command is not supported by the switch.

2.1.6 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 ports1/0/1，1/0/4-5，1/0/8。

Switch(config)#interface ethernet 1/0/1;1/0/4-5;1/0/8

Switch(Config-If-Port-Range)#

2.1.7 interface mode

This command is not supported by the switch.

2.1.8 loopback

Command: loopback

no loopback

Function: Enables the loopback test function in an Ethernet port; the no 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 1/0/1-8.

Switch(config)#interface ethernet 1/0/1-8

Switch(Config-If-Port-Range)#loopback

2.1.9 media-type

This command is not supported by the switch.

2.1.10 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. To change the negotiation mode, speed and duplex mode of 1000Base-TX port, use speed-duplex command instead.
Example: Port 21 of Switch1 is connected to port 21 of Switch2, the following will disable the negotiation for both ports.
Switch1(config)#interface ethernet1/0/21
Switch1(Config-If-Ethernet1/0/21)#negotiation off
Switch2(config)#interface ethernet1/0/21
Switch2(Config-If-Ethernet1/0/21)#negotiation off

2.1.11 port-rate-statistics interval

Command: port-rate-statistics interval <interval-value>
Function: Set the interval of port-rate-statistics, ranging from 5 to 600.
Parameter: interval-value: The interval of port-rate-statistics, unit is second, ranging from 5 to 600 with the configuration step of 5.
Default: Only port-rate-statistics of 5 seconds and 5 minutes are displayed.
Command Mode: Global Mode
Usage Guide: None.
Example: Count the interval of port-rate-statistics as 20 seconds.
Switch(config)#port-rate-statistics interval 20

2.1.12 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.
Parameter: 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.

Notice: 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

2.1.13 port-status query interval

This command is not supported by the switch.

2.1.14 rate-violation

Command: rate-violation [broadcast | multicast | unicast | all] <200-2000000>

no rate-violation

Function: Set the max packet reception rate of a port. Any packet which violate the packet reception rate to process the control operation (currently shutdown and block operations are supported) of rate-violation. The no command will disable the rate-violation function of a port.

The rate-violation means the port received the packet rate (the number of the received packets per second), it can distinguish the packet type, such as broadcast packet, multicast packet, unicast packet.

Parameters: broadcast: broadcast packet

multicast: multicast packet

unicast: unicast packet

all: all packets

<200-2000000>: the number of packets allowed to pass per second.

Command Mode: Port Mode

Default: There is no limit for the packet reception rate.

Usage Guide: This command is mainly used to detect the abnormal port flow. For example, when there are a large number of broadcast packets caused by a loopback, which affect the processing of other tasks, the port will be shut down or block to ensure the normal processing of the switch. This command needs to associate with rate-violation control command.

Example: Set the rate-violation of port 1/0/8-10 (GB ports) as 10000pps, it will be shutdown after rate-violation 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 1/0/8-10

Switch(Config-Port-Range)#rate-violation unicast 10000

Switch(Config-Port-Range)#rate-violation control shutdown recovery 1200

2.1.15 rate-violation control

Command: rate-violation control [shutdown recovery <0-86400> | block]

no rate-violation control

Function: Set the control operation after the rate-violation of a port, shutdown (it needs to configure the recovery time of a port after shutdown) and block operations are supported presently. The no operation will disable the rate-violation control operation of a port.

Parameters: shutdown: A port is shutdown after rate-violation.

block: A port is block after rate-violation, this parameter and MSTP, EAPS(MRPP), Loopback Detection, ULPP are mutually exclusive. If other modules set STP state, this function can not be set to block mode.

<0-86400>: The interval of recovery after shutdown, the unit is s.

recovery: After a period of time the port can recover Shutdown to UP again. <0-86400> 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 expires. The default timeout is 300s, while 0 means the recovery will never happen.

Command Mode: Port Mode

Default: There is no control operation for rate-violation.

Usage Guide: This command is mainly used to the control operation after rate-violation. shutdown or block operation can ensure the normal processing to other tasks of the switch. This command needs to associate with rate-violation [broadcast|multicast|unicast|all] <200-2000000> command.

Example: After set the rate-violation of the unicast packet of port 1/8-10 (GB ports) as 10000pps, the port will be block.

Switch(Config)#interface ethernet 1/0/8-10

Switch(Config-Port-Range)#rate-violation unicast 10000

Switch(Config-Port-Range)#rate-violation control block

2.1.16 remote-statistics interval

This command is not supported by the switch.

2.1.17 show interface

Command: show interface [ethernet *<interface-number>* | port-channel *<port-channel-number>* | vlan *<vlan-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. ***<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; As for Ethernet port, this command will show port speed rate, duplex mode, flow control switch state, broadcast storm suppression 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 suppression 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.

statistic field name	description
input errors	total statistic of CRC 、undersize、fragments、jabber field
CRC	the total number of packets received that had a length of between 64 and 1518 octets, inclusive, but had either FCS Error or Alignment Error
frame alignment	total number of packets received that had a bad FCS with a non-integral number of octets (Alignment Error)
undersize	total number of packets received that were less than 64 octets
jabber	total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
fragments	total number of packets received that were less than 64 octets in length and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
pause frame（input）	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation (from RFC2665 dot3InPauseFrames)
pauseframe (output)	A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation (from RFC2665 dot3OutPauseFrames)
output errors	total number of packets received that were less than 64 octets

collisions	The best estimate of the total number of collisions on this Ethernet segment (from RFC2819 etherStatsCollisions)
late collisions	The number of times that a collision is detected on a particular interface later than one slotTime into the transmission of a packet (from RFC2665 dot3StatsLateCollisions)

Example: Show the information of **VLAN** 1

```
Switch #show interface vlan 1
Vlan1 is up, line protocol is up, dev index is 11001
   Device flag 0x1003(UP BROADCAST MULTICAST)
   Time since last status change:0w-0d-4h-10m-59s    (15059 seconds)
   IPv4 address is:
      192.168.1.1          255.255.255.0          (Primary)
   VRF Bind: Not Bind
   Hardware is EtherSVI, address is 00-03-0f-04-03-02
   MTU is 1500 bytes , BW is 0 Kbit
   Encapsulation ARPA, loopback not set
   5 minute input rate 172207769 bits/sec, 174144 packets/sec
   5 minute output rate 494 bits/sec, 1 packets/sec
   The last 5 second input rate 172204454 bits/sec, 175342 packets/sec
   The last 5 second output rate 397 bits/sec, 0 packets/sec
   Input packets statistics:
      Input queue 0/1200, 0 drops
      2665793249 packets input, 4017750506 bytes, 2664563783 no buffer
      29 input errors, 6 CRC, 0 oversize, 0 undersize
       0 jabber, 23 fragments
   Output packets statistics:
      7759 packets output, 961906 bytes, 0 underruns
0 output errors, 0 collisions
```

Show the information of port 1/0/1:

```
Switch#show interface e1/0/1
Switch #show interface ethernet 1/0/1
Interface brief:
   Ethernet1/0/1 is down, line protocol is down
   Ethernet1/0/1 is layer 2 port, alias name is (null), index is 1
         Hardware is Gigabit-TX, address is 00-03-0f-04-03-01
         PVID is 1
         MTU 1500 bytes, BW 10000 Kbit
         Time since last status change:0w-0d-4h-30m-59s    (16259 seconds)
         Encapsulation ARPA, Loopback not set
         Auto-duplex, Auto-speed
```

FlowControl is off, MDI type is auto
Statistics:
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
The last 5 second input rate 0 bits/sec, 0 packets/sec
The last 5 second output rate 0 bits/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 undersize 0 jabber, 0 fragments, 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 late 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
1/0/1	DOWN/DOWN	auto	auto	1	G-TX	
1/0/2	DOWN/DOWN	auto	auto	1	G-TX	
1/0/3	UP/UP	a-100M	a-FULL	1	G-TX	
1/0/4	UP/UP	a-100M	a-FULL	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)
1/0/1	IN	0	0	0	0
	OUT	0	0	0	0
1/0/2	IN	0	0	0	0
	OUT	0	0	0	0
1/0/3	IN	0	0	1338508690	20
	OUT	0	0	7769	0
1/0/4	IN	0	0	1338506502	9
	OUT	0	0	23	0

…

Show the rate statistics information of all layer 2 ports:
Switch #show interface ethernet counter rate

Interface		IN(pkts/s)	IN(bits/s)	OUT(pkts/s)	OUT(bits/s)
1/0/1	5m	0	0	0	0

	5s	0	0	0	0
1/0/2	5m	0	0	0	0
	5s	0	0	0	0
1/0/3	5m	86,780	86,108,687	0	494
	5s	87,671	86,089,926	0	397
1/0/4	5m	86,780	86,108,684	0	0
	5s	87,671	86,089,926	0	0

…

2.1.18 shutdown

Command: shutdown

no shutdown

Function: Shuts down the specified Ethernet port; the no 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 ports 1/0/1-8.

Switch(config)#interface ethernet1/0/1-8

Switch(Config-If-Port-Range)#no shutdown

2.1.19 speed-duplex

Command: speed-duplex {auto [10 [100 [1000]] [auto | full | half |]] | 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 command restores the default speed and duplex mode setting, i.e., auto speed negotiation and duplex.

Parameters: auto is the auto speed and duplex negotiation, 10 is 10Mbps speed, 100 is 100Mbps speed, 1000 is 1000Mbps speed, auto is duplex negotiation, full is full-duplex, half is half-duplex; **force10-half** is the forced 10Mbps at half-duplex mode; **force10-full** is the forced 10Mbps at full-duplex mode; **force100-half** is the forced 100Mbps at half-duplex mode; **force100-full** is the forced 100Mbps at full-duplex mode; **force100-fx** is the forced 100Mbps at full-duplex mode; **module-type** is the type of 100Base-FX module; **auto-detected:** automatic detection; **no-phy-integrated:** there is no phy-integratd 100Base-FX module; **phy-integrated:** phy-integratd 100Base-FX module; **force1g-half** is the forced 1000Mbps speed at half-duplex mode; **force1g-full** is the forced 1000Mbps speed at full-duplex mode; **nonegotiate** disables auto-negotiation forcibly for 1000Mb port; **master** forces the 1000Mb port to be **master** mode; **slave** forces 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 Switch1 is **connected** to port 1 of Switch2, the following will set both ports **in** forced 100Mbps at half-duplex mode.
Switch1(config)#interface ethernet1/0/1
Switch1(Config-If-Ethernet1/0/1)#speed-duplex force100-half
Switch2(config)#interface ethernet1/0/1
Switch2(Config-If-Ethernet1/0/1)#speed-duplex force100-half

2.1.20 storm-control

Command: storm-control { kbps | pps }
no storm-control pps
Function: Sets the traffic limit for broadcasts, multicasts and unknown destination unicasts on all ports in the switch, namely set the limit unit of limit broadcast, multicast or unknown destination unicast is kbps or pps; the no command is recover the default value (kbps) to be limit mode.
Parameters: kbps means the unit of limit is kbits/s; pps means the limit unit ispackets/s.
Command Mode: Global Mode.
Default: The default is kbps.
Usage Guide: Configure the kbps or pps as the limit mode in global mode, then set broadcast, multicast or unknown unicast limit value in port mode.
Example: Setting ports 1-8 allow 1000kbit broadcast packets per second.
Switch(config)#storm-control pps
Switch(config-if-port-range)#storm-control broadcast 1000

2.1.21 storm-control

Command: storm-control {unicast | broadcast | multicast} <*value*>
no storm-control {unicast | 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 suppression 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 **unicast** to limit unicast traffic for unknown destination; **multicast** to limit

multicast traffic; **broadcast** to limit broadcast traffic. ***<value>*** means the number of packets allowed to pass per second or the packets numbers, the Kbps ranging from 1 to 1000000, the pps ranging from 1 to 1488095.
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. If the allowed traffic is set to 1000kbps, this means allow 1000 kbit per second and suppress the rest. The switch supports two kind of speed limit, it includes kbps which is limit by bandwidth and pps which is limit by the numbers of packets. It only can select one from the two ways and cannot set the two way in the same time (by global mode).
Broadcast suppression is similar to bandwidth control. There is granularity limitation for the chip; the switch support 16Kbps granularities. If the <Kbits> that user input is not the integer times of 16, the system will adjust to the integer times of 16 automatically and print the true limit value to user.
Example: Setting ports 1-8 allow 1000kbit broadcast packets per second.
Switch(config-if-port-range)#storm-control broadcast 1000

2.1.22 virtual-cable-test

Command: virtual-cable-test interface (ethernet |)IFNAME
Function: Test the link of the twisted pair cable connected to the Ethernet port. The response may include: well, short, open, fail. If the test information is not well, the location of the error will be displayed (how many meters it is away from the port).
Parameter: <*interface-list*>: Port ID
Command Mode: Admin Mode.
Default Settings: No link test.
Usage Guide: The RJ-45 port connected with the twisted pair under test should be in accordance with the wiring sequence rules of IEEE802.3, or the wire pairs in the test result may not be the actual ones. On a 100M port, only two pairs are used: (1, 2) and (3, 6), whose results are the only effective ones. If a 1000M port is connected to a 100M port, the results of (4, 5) and (7, 8) will be of no meaning. The result may have deviations according to the type of the twisted pair, the temperature, working voltage and other conditions. When the temperature is 20 degree Celsius, and the voltage is stable without interference, and the length of the twisted pair is not longer than 100 meters, a deviation of +/-2 meters is allowed. When the port is at Link UP status, a deviation of +/-10 meters is allowed. Notice: the test procedure will block all data flow on the line for 5-10 seconds, and then restore the original status.
568A wiring sequence: (1 green white, 2 green), (3 orange white, 6 orange), (4 blue, 5 blue white),

(7 brown white, 8 brown).
568B wiring sequence: (1 orange white, 2 orange), (3 green white, 6 green), (4 blue, 5 blue white), (7 brown white, 8 brown).
Example: Test the link status of the twisted pair connected to the 1000M port 1/0/1.

```
Switch#virtual-cable-test interface ethernet 1/0/1
Interface Ethernet1/0/1:
------------------------------------------------------------------------------
Cable pairs       Cable status       Error length (meters)
---------------   -----------------  --------------------------
(1, 2)              open               5
(3, 6)              open               5
(4, 5)              open               5
(7, 8)              short              5
```

2.1.23 switchport discard packet

Command：switchport discard packet { all | untag }
no switchport discard packet { all | untag }
Function：Configure the port not to receive any packet or untag; the no command cancel the restriction of discard, it means the port is allowed to receive any packet or untag.
Parameters：all means it does not receive any packet including untag, tag and the deal packet. untag means it does not receive untag.
Command Mode：Port Mode
Default：The default does not have the restriction.
Usage Guide：This command is not suggested to be configured only if there is the special requirement.
Example： Configure the port of 1/0/8 not to receive all packets.

```
Switch(config)#interface ethernet 1/0/8
Switch(config-if-ethernet1/0/8)#switchport discard packet all
```

2.1.24 switchport flood-control

Command: switchport flood-control { bcast|mcast|ucast }
no switchport flood-control { bcast|mcast|ucast }
Function: Configure that switch does not transmit broadcast, unknown multicast or unknown unicast packets any more to the specified port; no command restores the default configuration.
Parameter: bcast: prevents that broadcast packets cannot be transmitted to the specified port; mcast: prevents that unknown multicast packets cannot be transmitted to the specified port; ucast: prevents that unknown unicast packets cannot be transmitted to the specified port.
Command Mode: Port configuration mode.
Default: Switch transmits broadcast, unknown multicast and unknown unicast packets to other

port in broadcast domain.

Usage Guide: This command takes effect for 100M and 1000M ports; it is also takes effect for Access, Trunk and Hybrid ports. When this command is valid, the port will allow unicast or multicast flow to pass after port learned the corresponding unicast mac or multicast mac.

This command only control that broadcast, multicast and unknown unicast packets sent by other ports cannot be transmitted to the specified port, but it cannot control these packets from the specified port. For example, set switchport flood-control bcast command in port 1/0/1, broadcast packets cannot be transmitted from other ports to port 1/0/1, but port 1/0/1 can receive and transmit broadcast packets.

Example: Configure flood-control of bcast and mcast for port 1/0/1 or port 1/0/8-10 respectively.

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#switchport flood-control bcast

Switch(config)#interface ethernet 1/0/8-10

Switch(config-if-port-range)#switchport flood-control mcast

2.1.25 switchport flood-forwarding

Command: switchport flood-forwarding mcast

no switchport flood-forwarding mcast

Function: Configure that switch transmit unknown multicast or unknown unicast packets to the specified port; no command restores the default configuration.

Parameters: mcast: prevents that unknown multicast packets can be transmitted to the specified port.

Command Mode: Port Mode.

Default: Switch transmits unknown multicast packets to other port in broadcast domain.

Usage Guide: This command takes effect for 100M and 1000M ports; it is also takes effect for Access, Trunk and Hybrid ports. The command is usually combined with ip imgp snooping, ip imgp snooping does not supports unknown multicast and broadcast, it can transfer unknown multicast flow after configure switchport flood-forwarding mcast.

Example: Set switch 1/0/1 port broadcast flood-forwarding.

switch#

switch#confi

switch(config)#interface ethernet 1/0/1

switch(config-if-ethernet1/0/1)# switchport flood-forwarding mcast

switch(config-if-ethernet1/0/1)#exit

switch(config)#

2.2 Port Isolation

2.2.1 isolate-port group

Command: isolate-port group <*WORD*>

no isolate-port group <*WORD*>

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

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

Command Mode: Global Mode.

Default: None.

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

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

Switch>enable

Switch#config

Switch(config)#isolate-port group test

2.2.2 isolate-port group switchport interface

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

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

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

Vlan mode: Add *one* port or a group of ports into *a* port isolation group to isolate, which will become isolated from the other ports in a vlan. The no operation of this command will remove one port or a group of ports out of a port isolation group, which will be able to communicate will ports in that group normally.

Parameters: <WORD> is the name identification of the group, no longer than 32 characters. If there is no such group with the specified name, create one; ethernet means that the ports to be isolated is Ethernet ones, followed by a list of Ethernet ports, supporting symbols like ';' and '-'. For example: 'ethernet 1/0/1;3;4-7;8'; <IFNAME> is the name of the interface,

such as e1/0/1. If users use interface name, the parameter of ethernet will not be required.

Command Mode: ***Global*** Mode or Vlan Configuration Mode.

Default: None.

Usage Guide: Users can add Ethernet ports into a port isolation group according to their requirements, the isolation group can isolation it from each other (Global mode) in all vlan, it also can isolate it from each other (vlan mode) in some vlan or remove them from a port isolation **group** according to their requirements. When an Ethernet port is a ***member*** of more than one port isolate group, it will be isolated from every port of all groups it belongs to.

Example: Add Ethernet ports 1/0/1-2 and 1/0/5 into a port isolation group named as 'test', add Ethernet ports 1/0/3-4 into a port isolation group named as '1' in vlan10.

Switch(config)#isolate-port group test switchport interface ethernet 1/0/1-2; 1/0/5

Switch(config-vlan10)#isolate-port group 1 switchport interface ethernet 1/0/3-4

2.2.3 isolate-port apply

This command is not supported by the switch.

2.2.4 show isolate-port group

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

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

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

Command Mode: Admin Mode and Global Mode.

Default: Display the configuration of all port isolation groups.

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

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

Switch(config)#show isolate-port group test

Isolate-port group test

The isolate-port Ethernet1/0/5

The isolate-port Ethernet1/0/2

2.3 Port Loopback Detection

2.3.1 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 00:07:45:106 2006 Send loopback detection probe packet:dev Ethernet1/0/5, vlan id 1

%Jan 01 00:07:45:107 2006 Send loopback detection probe packet:dev Ethernet1/0/5, vlan id 1

%Jan 01 00:07:45:110 2006 Loopback detected on port Ethernet1/0/5, VLAN 1

2.3.2 loopback-detection control

Command: loopback-detection control {shutdown |block }

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.

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 1/0/2

Switch(Config-If-Ethernet1/0/2)#loopback-detection control shutdown

Switch(Config-If-Ethernet1/0/2)#no loopback-detection control

2.3.3 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

2.3.4 loopback-detection interval-time

Command: loopback-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

2.3.5 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 1/0/2

Switch(Config-If-Ethernet1/0/2)#switchport mode trunk

Switch(Config-If-Ethernet1/0/2)#switchport trunk allowed vlan all

Switch(Config-If-Ethernet1/0/2)#loopback-detection specified-vlan 1;3;5-20

Switch(Config-If-Ethernet1/0/2)#no loopback-detection specified-vlan 1;3;5-20

2.3.6 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 1/0/1.

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 1/0/4

loopback detection config and state information in the switch!

PortName	Loopback Detection	Control Mode	Is Controlled
Ethernet1/4	Enable	Shutdown	No

2.4 ULDP

2.4.1 debug uldp

Command: debug uldp (hello | probe | echo | unidir | all) [receive | send] interface [ethernet] IFNAME

no debug uldp (hello | probe | echo | unidir | all) [receive | send] interface [ethernet] IFNAME

Function: Enable the debugging for receiving and sending the specified packets or all ULDP packets on port. After enable the debugging, show the information of the received and sent packets in terminal. The no command disables the debugging.

Parameters: hello: packet's type is hello, it's announcement packet, including common announcement packet, RSY and Flush packet

probe: packet's type is probe, it's detection packet

echo: packet's type is echo, it means response of detection packet

unidir: packet's type is unidir, it's announcement packet that discover the single link

all: All ULDP packets

Command mode: Admin mode

Default: Disable.

Usage Guide: With this command, user can check probe packets received by port 1/0/2.

Switch#debug uldp probe receive interface ethernet 1/0/2

2.4.2 debug uldp error

Command: debug uldp error

no debug uldp error

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

Parameter: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: Use this command to display the error message.

Example: Display the error message.

Switch#debug uldp error

2.4.3 debug uldp event

Command: debug uldp event

no debug uldp event

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

Parameter: None.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: Use this command to display all kinds of event information.

Example: Display event information.

Switch#debug uldp event

2.4.4 debug uldp fsm interface ethernet

Command: debug uldp fsm interface ethernet *<IFname>*

no debug uldp fsm interface ethernet *<IFname>*

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

Parameters: *<IFname>* is the interface name.

Command Mode: Admin Configuration Mode.

Default: Disabled by default.
Usage Guide: This command can be used to display the information about state transitions of the specified interfaces.
Example: Print the information about state transitions of interface ethernet 1/0/1.
Switch#debug uldp fsm interface ethernet 1/0/1

2.4.5 debug uldp interface ethernet

Command: debug uldp {hello|probe|echo|unidir|all} [receive|send] interface ethernet <*IFname*>
no debug uldp {hello|probe|echo|unidir|all} [receive|send] interface ethernet <*IFname*>
Function: Enable the debug function of display the packet details. After that, display some kinds of the packet details of terminal interface.
Parameter: <*IFname*>: Name of the interface.
Command Mode: Admin Mode.
Default: Disabled.
Usage Guide: Use this command to display the Hello packet details receiving on the interface Ethernet 1/0/1.
Switch#debug uldp hello receive interface Ethernet 1/0/1

2.4.6 debug uldp packet

Command: debug uldp packet [receive|send]
no debug uldp packet [receive|send]
Function: Enable receives and sends packet debug function, after that. Display the type and interface of the packet which receiving and sending on the client. The no form command disables this function.
Parameter: None.
Command Mode: Admin Mode.
Default: Disabled.
Usage Guide: Use this command to display the packet that receiving on each interface.
Switch#debug uldp packet receive

2.4.7 uldp aggressive-mode

Command: uldp aggressive-mode
no uldp aggressive-mode
Function: To configure ULDP to work in aggressive mode. The no form of this command will restore the normal mode.
Parameters: None.
Command Mode: Global Configuration Mode and Port Configuration Mode.
Default: Normal mode.

Usage Guide: The ULDP working mode can be configured only if it is enabled globally. When ULDP aggressive mode is enabled globally, all the existing fiber ports will work in aggressive mode. For the copper ports and fiber ports which are available after the configuration is available, aggressive mode should be enabled in port configuration mode.
Example: To enable ULDP aggressive mode globally.
Switch(config)#uldp aggressive-mode

2.4.8 uldp enable

Command: uldp enable
Function: ULDP will be enabled after issuing this command. In global configuration mode, this command will enable ULDP for the global. In port configuration mode, this command will enable ULDP for the port.
Parameters: None.
Command Mode: Global Configuration Mode and Port Configuration Mode.
Default: By default ULDP is not configured.
Usage Guide: ULDP can be configured for the ports only if ULDP is enabled globally. If ULDP is enabled globally, it will be effect for all the existing fiber ports. For copper ports and fiber ports which are available after ULDP is enabled, this command should be issued in the port configuration mode to make ULDP be effect.
Example: Enable ULDP in global configuration mode.
Switch(config)#uldp enable

2.4.9 uldp disable

Command: uldp disable
Function: To disable ULDP configuration through this command.
Parameters: None.
Command Mode: Global Configuration Mode and Port Configuration Mode.
Default: By default ULDP is not configured.
Usage Guide: When ULDP is disabled globally, then ULDP in all the ports will be disabled.
Example: To disable the ULDP configuration in global configuration mode.
Switch(config)#uldp disable

2.4.10 uldp hello-interval

Command: uldp hello-interval <*integer*>
no uldp hello-interval
Function: To configure the interval for ULDP to send hello messages. The no form of this command will restore the default interval for the hello messages.
Parameters: <*integer*>: The interval for the Hello messages, with its value limited between 5 and 100 seconds, 10 seconds by default.
Command Mode: Global Configuration Mode.

Default: 10 seconds by default.
Usage Guide: Interval for hello messages can be configured only if ULDP is enabled globally, its value limited between 5 and 100 seconds.
Example: To configure the interval of Hello messages to be 12 seconds.
Switch(config)#uldp hello-interval 12

2.4.11 uldp manual-shutdown

Command: uldp manual-shutdown
no uldp manual-shutdown
Function: To configure ULDP to work in manual shutdown mode. The no command will restore the automatic mode.
Parameters: None.
Command Mode: Global Configuration Mode.
Default: Auto mode.
Usage Guide: This command can be issued only if ULDP has been enabled globally.
Example: To enable manual shutdown globally.
Switch(config)#uldp manual-shutdown

2.4.12 uldp recovery-time

Command: uldp recovery-time*<integer>*
no uldp recovery-time
Function: To configure the interval for ULDP recovery timer. The no form of this command will restore the default configuration.
Parameters: *<integer>*: the time out value for the ULDP recovery timer. Its value is limited between 30 and 86400 seconds.
Command Mode: Global Configuration Mode.
Default: 0 is set by default which means the recovery is disabled.
Usage Guide: If an interface is shutdown by ULDP, and the recovery timer times out, the interface will be reset automatically. If the recovery timer is set to 0, the interface will not be reset.
Example: To set the recovery timer to be 600 seconds.
Switch(config)#uldp recovery-time 600

2.4.13 uldp reset

Command: uldp reset
Function: To reset the port when ULDP is shutdown.
Parameters: None.
Command Mode: Globally Configuration Mode and Port Configuration Mode.
Default: None.
Usage Guide: This command can only be effect only if the specified interface is disabled by ULDP.
Example: To reset all the port which are disabled by ULDP.

services Switch(config)#uldp reset

2.4.14 show uldp

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

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

Parameters: ***<interface-name>*** is the interface name.

Command Mode: Admin and Configuration Mode.

Default: None.

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

Example: To display the global ULDP information.

Switch(config)#show uldp

2.5 LLDP

2.5.1 clear lldp remote-table

Command: clear lldp remote-table

Function: Clear the Remote-table on the port.

Parameters: None.

Default: Do not clear the entries.

Command Mode: Port Configuration Mode.

Usage Guide: Clear the Remote table entries on this port.

Example: Clear the Remote table entries on this port.

Switch(Config-If-Ethernet 1/0/1)# clear lldp remote-table

2.5.2 debug lldp

Command: debug lldp

no debug lldp

Function: Enable the debug information of LLDP function, the no operation of this command will disable the debug information of LLDP function.

Parameters: None.

Default: Disable the debug information of LLDP function.

Command Mode: Admin Mode.

Usage Guide: When the debug switch is enabled, users can check the receiving and sending of packets and other information.

Example: Enable the debug switch of LLDP function on the switch.

Switch#debug lldp

2.5.3 debug lldp packets

Command: debug lldp packets interface ethernet <*IFNAME*>

no debug lldp packets interface ethernet <*IFNAME*>

Function: Display the message-receiving and message-sending information of LLDP on the port; the no operation of this command will disable the debug information switch.

Parameters: None.

Default: Disable the debug information on the port.

Command Mode: Admin Mode.

Usage Guide: When the debug switch is enabled, users can check the receiving and sending of packets and other information on the port.

Example: Enable the debug switch of LLDP function on the switch.

Switch#debug lldp packets interface ethernet 1/0/1

%Jan 01 00:02:40 2006 LLDP-PDU-TX PORT= ethernet 1/0/1

2.5.4 lldp enable

Command: lldp enable

lldp disable

Function: Globally enable LLDP function; **disable** command globally disables LLDP function.

Parameters: None.

Default: Disable LLDP function.

Command Mode: Global Mode.

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

Example: Enable LLDP function on the switch.

Switch(config)#lldp enable

2.5.5 lldp enable (Port)

Command: lldp enable

lldp disable

Function: Enable the LLDP function module of ports in port configuration mode; **disable** command will disable the LLDP function module of port.

Parameters: None.

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

Command Mode: Port Configuration Mode.

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

Example: Disable LLDP function of port on the port ethernet 1/0/5 of the switch.
Switch(config)#in ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#lldp disable

2.5.6 lldp management-address tlv

Command: lldp management-address tlv [A.B.C.D]
no lldp management-address tlv
Function: Configure to enable the management address tlv of lldp port.
Parameters: A.B.C.D: it is the optional parameter, and it is the management address that user appoints for the port, it must be the unicast IPv4 address.
Default: Disable. The LLDP packet does not have the management address information of the port.
Command Mode: Port Mode.
Usage Guide: User can choose the feat management IPv4 address according to the configuration. If user appointed the management address when enable the function, this address will be used to send the management address TLV; if user does not appoint the management address, choose the IPv4 address from the VLAN layer3 as the management address to send the management address TLV. When the address is not appointed, if there is no feat address, the management address TLV information will not be sent.
Example: Enable the management address TLV function of ethernet 1/0/1 and appoint the address.
Switch1(Config-If-Ethernet1/0/1)# lldp management-address tlv 192.168.24.32

2.5.7 lldp mode

Command: lldp mode <*send | receive | both | disable*>
Function: Configure the operating state of LLDP function of the port.
Parameters: send: Configure the LLDP function as only being able to send messages.
receive: Configure the LLDP function as only being able to receive messages.
both: Configure the LLDP function as being able to both send and receive messages.
disable: Configure the LLDP function as not being able to send or receive messages.
Default: The operating state of the port is “both”.
Command Mode: Port Configuration Mode.
Usage Guide: Choose the operating state of the lldp Agent on the port.
Example: Configure the state of port ethernet 1/0/5 of the switch as “receive”.
Switch(config)#in ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#lldp mode receive

2.5.8 lldp msgTxHold

Command: lldp msgTxHold <*value*>

no lldp msgTxHold

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

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

Default: the value of the multiplier is 4 by default.

Command Mode: Global Mode.

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

Example: Set the value of the aging time multiplier as 6.

Switch(config)#lldp msgTxHold 6

2.5.9 lldp neighbors max-num

Command: lldp neighbors max-num <*value*>

no lldp neighbors max-num

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

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

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

Command Mode: Port Configuration Mode.

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

Example: Set the Remote as 200 on port ethernet 1/0/5 of the switch.

Switch(config)#in ethernet 1/0/5

Switch(Config-If-Ethernet1/0/5)# lldp neighbors max-num 200

2.5.10 lldp notification interval

Command: lldp notification interval <*seconds*>

no lldp notification interval

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

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

Default: The time interval is 5 seconds.

Command Mode: Global Mode.

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

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

Switch(config)#lldp notification interval 20

2.5.11 lldp tooManyNeighbors

Command: lldp tooManyNeighbors {discard | delete}

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

Parameters: discard: discard the current message.
delete: Delete the message with the least TTL in the Remoter Table.
Default: Discard.
Command Mode: Port Configuration Mode.
Usage Guide: When the Remote MIB is full, Discard means to discard the received message; Delete means to the message with the least TTL in the Remoter Table.
Example: Set port ethernet 1/0/5 of the switch as delete.
Switch(config)#in ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#lldp tooManyNeighbors delete

2.5.12 lldp transmit delay

Command: lldp transmit delay <*seconds*>
no lldp transmit delay
Function: Since local information might change frequently because of the variability of the network environment, there could be many update messages sent in a short time. So a delay is required to guarantee an accurate statistics of local information.
When transmit delay is the default value and tx-interval is configured via some commands, transmit delay will become one fourth of the latter, instead of the default 2.
Parameters: <*seconds*>is the time interval, ranging from 1 to 8192 seconds.
Default: The interval is 2 seconds by default.
Command Mode: Global Mode.
Usage Guide: When the messages are being sent continuously, a sending delay is set to prevent the Remote information from being updated repeatedly due to sending messages simultaneously.
Example: Set the delay of sending messages as 3 seconds.
Switch(config)#lldp transmit delay 3

2.5.13 lldp transmit optional tlv

Command: lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap]
no lldp transmit optional tlv
Function: Configure the type of optional TLV of the port.
Parameters: portDesc: the description of the port; **sysName:** the system name; **sysDesc:** The description of the system; **sysCap:** the capability of the system.
Default: The messages carry no optional TLV by default.
Command Mode: Port Configuration Mode.
Usage Guide: When configuring the optional TLV, each TLV can only appear once in a message, **portDesc** optional TLV represents the name of local port; **sysName** optional TLV represents the name of local system; **sysDesc** optional TLV represents the description of local system; **sysCap** optional TLV represents the capability of local system.
Example: Configure that port ethernet 1/0/5 of the switch carries portDesc and sysCap TLV.
Switch(config)#in ethernet 1/0/5

services Switch(Config-If-Ethernet1/0/5)# lldp transmit optional tlv portDesc sysCap

2.5.14 lldp trap

Command: lldp trap <*enable* | *disable*>

Function: enable: configure to enable the Trap function on the specified port; **disable:** configure to disable the Trap function on the specified port.

Parameters: None.

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

Command Mode: Port Configuration Mode.

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

Example: Enable the Trap function on port ethernet 1/0/5 of the switch.

Switch(config)#in ethernet1/0/5

Switch(Config-If-Ethernet1/0/5)#lldp trap enable

2.5.15 lldp tx-interval

Command: lldp tx-interval <*integer*>

no lldp tx-interval

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

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

Default: 30 seconds.

Command Settings: Global Mode.

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

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

Example: Set the interval of sending messages as 40 seconds.

Switch(config)#lldp tx-interval 40

2.5.16 show debugging lldp

Command: show debugging lldp

Function: Display all ports with lldp debug enabled.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: With show debugging lldp, all ports with lldp debug enabled will be displayed.
Example: Display all ports with lldp debug enabled.
Switch(config)#show debugging lldp
====BEGINNING OF LLDP DEBUG SETTINGS====
debug lldp
debug lldp packets interface Ethernet1/0/1
debug lldp packets interface Ethernet1/0/2
debug lldp packets interface Ethernet1/0/3
debug lldp packets interface Ethernet1/0/4
debug lldp packets interface Ethernet1/0/5
==========END OF DEBUG SETTINGS==========

2.5.17 show lldp

Command: show lldp
Function: Display the configuration information of global LLDP, such as the list of all the ports with LLDP enabled, the interval of sending update messages, the configuration of aging time, the interval needed by the sending module to wait for re-initialization, the interval of sending TRAP, the limitation of the number of the entries in the Remote Table.
Parameters: None.
Default: Do not display the configuration information of global LLDP.
Command Mode: Admin Mode, Global Mode.
Usage Guide: Users can check all the configuration information of global LLDP by using 'show lldp'.
Example: Check the configuration information of global LLDP after it is enabled on the switch.
Switch(config)#show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP has been enabled globally.
LLDP enabled port : Ethernet1/0/3 Ethernet1/0/4
LLDP interval :30
LLDP txTTL :120
LLDP NotificationInterval :5
LLDP txDelay :2
LLDP-MED FastStart Repeat Count :4
----------END----------

2.5.18 show lldp interface ethernet

Command: show lldp interface ethernet *<IFNAME>*
Function: Display the configuration information of LLDP on the port, such as: the working state of LLDP Agent.

Parameters: <*IFNAME*>: Interface name.
Default: Do not display the configuration information of LLDP on the port.
Command Mode: Admin Mode, Global Mode.
Usage Guide: Users can check the configuration information of LLDP on the port by using "show lldp interface ethernet XXX".
Example: Check the configuration information of LLDP on the port after LLDP is enabled on the switch.
Switch (config-if-ethernet1/0/1)#show lldp int e 1/0/1

```
 Port name :Ethernet1/0/1
 LLDP Agent Adminstatus : Both
 LLDP Operation TLV : default

 LLDP Management Address TLV :
 LLDP Management Address TLV status       : enable
 Management address type                    : ipv4
 Management address                         : 192.168.23.3
 Management address interface type          : IfIndex
  Management address interface id           : 0
 Management address OID                     : 0

 LLDP Trap Status : disable
 LLDP maxRemote :100
 LLDP Overflow handle : discard
 LLDP interface remote status : Free

 MED Optional TLV : default
 MED Trap Status:Disable
 MED TLV Transmit Status:Disable
 MED Fast Transmit Status:Disable
 Master(config-if-ethernet1/0/1)#
```

2.5.19 show lldp neighbors interface ethernet

Command: show lldp neighbors interface ethernet < *IFNAME* >
Function: Display the LLDP neighbor information of the port.
Parameters: None.
Default: Do not display the LLDP neighbor information of the port.
Command Mode: Admin Mode, Global Mode.
Usage Guide: Users can check the LLDP neighbor information of the port by using "show lldp neighbors interface ethernet XXX".
Example: Check the LLDP neighbor information of the port after LLDP is enabled on the port.

Switch (config-if-ethernet1/0/1)#show lld nei int e 1/0/1

Port name : Ethernet1/0/1
Port Remote Counter : 1
TimeMark :120
ChassisIdSubtype :4
ChassisId :00-03-0f-01-01-03
PortIdSubtype :Local
PortId :16

LLDP Management Address TLV :
Management address type : ipv4
Management address : 192.168.23.1
Management address interface type : IfIndex
Management address interface id : 0
Management address OID : 0

2.5.20 show lldp traffic

Command: show lldp traffic
Function: Display the statistics of LLDP data packets.
Parameters: None.
Default: Do not display the statistics of LLDP data packets.
Command Mode: Admin Mode, Global Mode.
Usage Guide: Users can check the statistics of LLDP data packets by using “show lldp traffic”.
Example: Check the statistics of LLDP data packets after LLDP is enabled on the switch.
Switch(config)#show lldp traffic

PortName	Ageouts	FramesDiscarded	FramesInErrors	FramesIn	FramesOut	TLVsDiscarded	TLVsUnrecognized
Ethernet1/0/1	0	0	0	0	7	0	0

2.6 LLDP-MED

2.6.1 civic location

Command: civic location {dhcp server | switch | endpointDev} *<country-code>*
no civic location
Function: Configure device type and country code of the location with Civic Address LCI format and enter Civic Address LCI address mode. The no command cancels all configurations of the location with Civic Address LCI format.

Parameters: dhcp server: Set device type to be DHCP server

switch: Set device type to be Switch

endpointDev: Set device type to be LLDP-MED Endpoint

country-code: Set country code which consist of 2 letters, such as DE or US, it should accord the country code of ISO 3166 standard.

Default: No location with Civic Address LCI format is configured on the port.

Command Mode: Port mode

Usage Guide: Configure device type and country code of the location with Civic Address LCI format and enter Civic Address LCI address mode to configure the more detailed location.

Example: Configure device type as switch and country code as US for the location with Civic Address LCI format on Ethernet 19.

Switch(Config-If-Ethernet1/0/19)# civic location switch US

Switch(Med-Civic)#

2.6.2 {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}

Command: {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo} *<address>*

no {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}

Function: Configure the detailed location after enter Civic Address LCI address mode of the port.

Parameters: description-language: language for describing location, such as 'English'

province-state: state, canton, region, province prefecture, and so on, such as 'clara'

city: city, such as 'New York'

county: county, parish, such as 'santa clara'

street: street, such as '1301 Shoreway Road'

locationNum: house number, such as '9'

location: name and occupant of a location, such as 'Carrillo's Holiday Market'

floor: floor number, such as '13'

room: room number, such as '1308'

postal: postal/zip code, such as '10027-1234'

otherInfo: Additional location information, such as 'South Wing'

address: detailed address information, it cannot exceed 250 characters

Default: No detailed information of the location with Civic Address LCI is configured on the port.

Command Mode: Civic Address LCI address mode

Usage Guide: With this command, configure the detailed information of the location with Civic Address LCI on the port, it is able to configure 10 kinds of address types at most.

Example: Configure the detailed location information in Civic Address LCI address mode.

Switch(Med-Civic)# city Beijing

services Switch(Med-Civic)# street shangdi

2.6.3 ecs location

Command: ecs location <*tel-number*>
no ecs location
Function: Configure the location with ECS ELIN format on the port, the no command cancels the configured location.
Parameter: <*tel-number*>: location characters with ECS ELIN format, such as emergent telephone number, it is character string with the length between 10 and 25.
Default: No location with ECS ELIN format is configured.
Command Mode: Port mode
Usage Guide: Length range of the location character string between 10 and 25 with ECS ELIN format.
Example: Configure the location of ECS ELIN format on port 19.
Switch(Config-If-Ethernet1/0/19)# ecs location 880-445-3381

2.6.4 lldp med device type endpoint

Command: lldp med device type endpoint
no lldp med device type endpoint
Function: Set the device as the endpoint node, the no command restores the default value.
Parameter: None.
Default: Device is a non-endpoint node.
Command Mode: Global mode
Usage Guide: Only when the device is set as an endpoint node, the LLDP packets sent can carry MED information. This command must be used together with the lldp transmit med command on the port.
Example:
Switch(config)#lldp med device type endpoint

2.6.5 lldp med fast count

Command: lldp med fast count <*value*>
no lldp med fast count
Function: When the fast LLDP-MED startup mechanism is enabled, it needs to fast send LLDP packets with LLDP-MED TLV, this command sets the value of sending the packets fast, the no command restores the default value.
Parameter: value: The number of sending the packets fast, its range from 1 to 10, unit is entries.
Default: 4.
Command Mode: Global mode
Usage Guide: With this command, set the number for sending the packets fast.
Example:

services Switch(config)#lldp med fast count 5

2.6.6 lldp med trap

Command: lldp med trap {enable | disable}
Function: Configure the specified port to enable or disable the function for sending TRAP message when LLDP-MED network topology is changed.
Parameters: enable: Enable LLDP-MED TRAP for the port
disable: Disable LLDP-MED TRAP for the port
Default: Disable LLDP-MED TRAP.
Command Mode: Port mode
Usage Guide: Enable or disable LLDP-MED TRAP of the port.
Example: Enable LLDP-MED TRAP of the port 19.
Switch(Config-If-Ethernet1/0/19)# lldp med trap enable

2.6.7 lldp transmit med tlv all

Command: lldp transmit med tlv all
no lldp transmit med tlv all
Function: Configure the specified port to send all LLDP-MED TLVs, the no command disables the function.
Parameter: None.
Default: Port does not enable the function for Sending LLDP-MED TLV.
Command Mode: Port mode
Usage Guide: After configuring this command, if the port is able to send LLDP-MED TLV, the sent LLDP packets with LLDP-MED TLV supported by all switches. However, LLDP packets sent by the port without any LLDP-MED TLV after the switch configured the corresponding no command.
Example: Port 19 enables the function for sending LLDP-MED TLV.
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv all

2.6.8 lldp transmit med tlv capability

Command: lldp transmit med tlv capability
no lldp transmit med tlv capability
Function: Configure the specified port to send LLDP-MED Capability TLV. The no command disables the capability.
Parameter: None.
Default: The function is disabled for sending LLDP-MED Capability TLV.
Command Mode: Port mode
Usage Guide: After configuring this command, if the port is able to send LLDP-MED TLV, the sent LLDP packets with LLDP-MED Capability TLV. However, LLDP packets sent by the port without LLDP-MED Capability TLV after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV is the important LLDP-MED TLV, if do not configure the port to send

LLDP-MED Capability TLV firstly, other LLDP-MED TLV will not be sent.
Example: Port 19 enables the function for sending LLDP-MED Capability TLV.
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv capability

2.6.9 lldp transmit med tlv extendPoe

Command: lldp transmit med tlv extendPoe
no lldp transmit med tlv extendPoe
Function: Configure the specified port to send LLDP-MED Extended Power-Via-MDI TLV. The no command disables the capability.
Parameter: None.
Default: The function is disabled for sending LLDP-MED Extended Power-Via-MDI TLV.
Command Mode: Port mode
Usage Guide: After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Extended Power-Via-MDI TLV sent by the port. However, LLDP packets without LLDP-MED Extended Power-Via-MDI TLV sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Extended Power-Via-MDI TLV, or else the configuration cannot be successful. If the device does not support PoE or PoE function of the port is disabled, although configuring this command, LLDP-MED Extended Power-Via-MDI TLV will not be sent.
Example: Port 19 enables the function for sending LLDP-MED Extended Power-Via-MDI TLV.
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv extendPoe

2.6.10 lldp transmit med tlv location

Command: lldp transmit med tlv location
no lldp transmit med tlv location
Function: Configure the specified port to send LLDP-MED Location Identification TLV. The no command disables this capability.
Parameters: None.
Default: Disable.
Command Mode: Port Mode.
Usage Guide: Configure the specified port to send LLDP-MED Location Identification TLV. After configured this command, if the port has the capability of sending LLDP-MED TLV, the LLDP packets sent from the port will include LLDP-MED Location Identification TLV. Otherwise, the LLDP packets sent from the port will not include LLDP-MED Location Identification TLV by the no command even if the port has the capability of sending LLDP-MED TLV. Notice: Before configuring this function, the capability of sending LLDP-MED Capability TLV must be configured. If the device does not support POE or the POE function of the port is disabled by the command, this TLV will not be sent.
Example: Enable the port 19 to send LLDP-MED Location Identification TLV.
Switch(Config-If-Ethernet1/0/19)#lldp transmit med tlv location

2.6.11 lldp transmit med tlv inventory

Command: lldp transmit med tlv inventory

no lldp transmit med tlv inventory

Function: Configure the specified port to send LLDP-MED Inventory Management TLVs aggregation, TLVs aggregation includes 7 TLVs, they are Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model Name TLV, Asset ID TLV. The no command disables the capability.

Parameter: None.

Default: The function is disabled for sending LLDP-MED Inventory Management TLVs.

Command Mode: Port mode

Usage Guide: After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Inventory Management TLVs sent by the port. However, LLDP packets without LLDP-MED Inventory Management TLVs sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Inventory Management TLVs, or else the configuration cannot be successful.

Example: Port 19 enables the function for sending LLDP-MED Inventory Management TLVs.

Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv inventory

2.6.12 lldp transmit med tlv networkPolicy

Command: lldp transmit med tlv networkPolicy

no lldp transmit med tlv networkPolicy

Function: Configure the specified port to send LLDP-MED Network Policy TLV. The no command disables the capability.

Parameter: None.

Default: The function is disabled for sending LLDP-MED Network Policy TLV.

Command Mode: Port mode

Usage Guide: After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Network Policy TLV sent by the port. However, LLDP packets without LLDP-MED Network Policy TLV sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Network Policy TLV, or else the configuration cannot be successful.

Example: Port 19 enables the function for sending LLDP-MED Network Policy TLV.

Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv networkPolicy

2.6.13 network policy

Command: network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} [status {enable | disable}] [tag {tagged | untagged}] [vid {*<vlan-id>* | dot1p}] [cos *<cos-value>*] [dscp *<dscp-value>*]

no network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming- video | video-signaling}

Function: Configure the network policy of the port, including VLAN ID, the supported application (such as voice and video), the application priority and the used policy, and so on.

Parameters: voice, voice-signaling, guest-voice, guest-voice-signaling, softphone-voice, video-conferencing, streaming-video and video-signaling: the application types are supported by the port.

status: Whether the network policy is usable.

enable: Network Policy of the specified application type has been defined, enable is the default value of the network policy.

disable: Network Policy of the specified application type is unknown, the fields (such as VLAN ID, L2 priority and DSCP) are ignored, network connection device will not send TLV of the specified application type.

tag: Configure the specified application to uses **tagged** or **untagged** VLAN method.

tagged: Configure the flow of the specified application to use the tagged vlan method, here, the fields (such as VLAN ID, Layer2 priority and DSCP value) are take effect.

untagged: Configure the flow without tag for the specified application, the fields (such as VLAN ID, Layer2 priority) are ignored, only DSCP value field takes effect. Untagged is the default value of VLAN method.

vid: Configure VLAN ID that the specified application belongs to. When the peer sends the flow of the specified application, it will tag the notified VLAN ID, or else the vlan-id value is 1.

vlan-id: Configure the value of VLAN ID, its range from 1 to 4094.

dot1p: Configure the specified application to tag the flow by using 802.1p priority, at the same time, use vlan 0 to load the flow.

cos: Configure the priority of Ethernet frame for VLAN.

cos-value: Configure the value of Ethernet frame priority for VLAN, its range from 0 to 7, the default value is 5.

dscp: Configure DSCP of VLAN.

dscp-value: DSCP value input by the user, its range from 0 to 63, the default value is 46.

Default: No network policy is configured on the port.

Command Mode: Port mode

Usage Guide: User is able to configure the network policy of many kinds on a port, but their application types cannot repeat, and a kind of network policy corresponds to a LLDP-MED network policy TLV. If user configures multi-policy for a port, it will send multi-LLDP-MED network policy TLV to a LLDP packet. If user does not configure any network policy, no LLDP-MED network policy TLV is sent to LLDP packet.

Example: Configure the network policy with the application type of voice on port 19.

Switch(Config-If-Ethernet1/0/19)# network policy voice tag tagged vid 2 cos 6 dscp 23

2.6.14 show lldp

Command: show lldp

Function: Show the global LLDP and LLDP-MED configuration.

Parameter: None.

Default: None.

Command Mode: Admin mode

Usage Guide: None.

Example: Show the global LLDP and LLDP-MED configuration.

```
Switch#show lldp
-----LLDP GLOBAL INFORMATIONS-----
LLDP has been enabled globally.
LLDP enabled port : Ethernet1/0/19
LLDP interval :5
LLDP txTTL :20
LLDP NotificationInterval :5
LLDP txDelay :1
LLDP-MED FastStart Repeat Count :4
-------------END------------------
```

2.6.15 show lldp [interface ethernet <IFNAME>]

Command: show lldp [interface ethernet <IFNAME>]

Function: Show LLDP and LLDP-MED configurations on the current port.

Parameter: [interface ethernet <IFNAME>]: Port name

Command Mode: Admin mode

Default: None.

Usage Guide: None.

Example: Show LLDP and LLDP-MED configuration of the port 19.

```
Switch#show lldp interface ethernet 1/0/19

  Port name :Ethernet1/0/19
  LLDP Agent Adminstatus : Both
  LLDP Operation TLV : default
  LLDP Trap Status : disable
  LLDP maxRemote :100
  LLDP Overflow handle : discard
  LLDP interface remote status : Free

  MED Optional TLV : capabilities  networkPolicy  location  power  inventory
  MED Trap Status:Enable
  MED TLV Transmit Status:Disable
  MED Fast Transmit Status:Disable
```

2.6.16 show lldp neighbors

Command: show lldp neighbors [interface ethernet <*IFNAME*>]

Function: Show LLDP and LLDP-MED information of the neighbors for the port.
Parameter: None.
Default: None.
Command Mode: Admin mode
Usage Guide: With this command, checking LLDP and LLDP-MED information of the neighbors after the port received LLDP packets sent by the neighbors.
Example: Show the neighbor information on port 1.
Switch #show lldp neighbors interface ethernet 1/0/1

Port name : Ethernet1/0/1
Port Remote Counter : 1
TimeMark :20
ChassisIdSubtype :4
ChassisId :00-03-0f-00-00-02
PortIdSubtype :Local
PortId :3
PortDesc :Ethernet1/0/1
SysName :switch
SysDesc :switch Device, Compiled Feb 12 17:39:53 2011
SoftWare Version 6.2.30.0
BootRom Version 4.0.1
HardWare Version
Device serial number
Copyright (C) 2001-2011 by Vendor.
All rights reserved

2.6.17 show lldp traffic

Command: show lldp traffic
Function: Show the statistics of the sent and received packets of LLDP and LLDP-MED.
Parameters: None.
Default: None.
Command Mode: Admin Mode.
Usage Guide: After the port received the LLDP packets from the neighbor, this command can be used to view the statistics of the sent and received packets of LLDP and LLDP-MED.
Example: View the statistics of the sent and received packets after the LLDP function is enabled.
Switch(config)#show lldp traffic

PortName	Ageouts	FramesDiscarded	FramesInErrors	FramesIn	FramesOut	TLVsDiscarded	TLVsUnrecognized
Ethernet1/0/1	0	0	0	0	7	0	0

2.7 Port Channel

2.7.1 debug port-channel

Command: debug port-channel <*port-group-number*> {all | event | fsm | packet | timer}
no debug port-channel [<*port-group-number*>]

Function: Open the debug switch of port-channel.

Parameters: <*port-group-number*> is the group number of port channel, ranging from 1～128
all: all debug information
event: debug event information
fsm: debug the state machine
packet: debug LACP packet information
timer: debug the timer information

Command mode: Admin mode.

Default: Disable the debugging of port-channel.

Usage Guide: Open the debug switch to check the debug information of port-channel.

Notice: it can create 16 port group at most.

Example:

(1)debug the state machine for port-group 1.

Switch#debug port-channel 1 fsm

(2) debug LACP packet information for port-group 2.

Switch#debug port-channel 2 packet

(3) debug all for port-group 1.

Switch#debug port-channel 1 all

2.7.2 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

services Switch(Config-If-Port-Channel1)#

2.7.3 lacp port-priority

Command: lacp port-priority <*port-priority*>

no lacp port-priority

Function: Set the port priority of LACP protocol.

Parameters: <*port-priority*>: the port priority of LACP protocol, the range from 0 to 65535.

Command mode: Port Mode.

Default: The default priority is 32768 by system.

Usage Guide: Use this command to modify the port priority of LACP protocol, the no command restores the default value.

Example: Set the port priority of LACP protocol.

Switch(Config-If-Ethernet1/0/1)# lacp port-priority 30000

2.7.4 lacp system-priority

Command: lacp system-priority <*system-priority*>

no lacp system-priority

Function: Set the system priority of LACP protocol.

Parameters: <*system-priority*>: The system priority of LACP protocol, ranging from 0 to 65535.

Command mode: Global Mode

Default: The default priority is 32768.

Usage Guide: Use this command to modify the system priority of LACP protocol, the no command restores the default value.

Example: Set the system priority of LACP protocol.

Switch(config)#lacp system-priority 30000

2.7.5 lacp timeout

Command: lacp timeout {short | long}

no lacp timeout

Function: Set the timeout mode of LACP protocol.

Parameters: The timeout mode includes long and short.

Command mode: Port Mode

Default: Long.

Usage Guide: Set the timeout mode of LACP protocol.

Example: Set the timeout mode as short in LACP protocol.

Switch(Config-If-Ethernet1/0/1)#lacp timeout short

2.7.6 load-balance

Command: load-balance {src-mac | dst-mac | dst-src-mac | src-ip | dst-ip | dst-src-ip |

ingress-port | dst-src-mac-ip}

no load-balance

Function: Set load-balance mode for port-group, the no command return it to load-balance mode.

Parameter: src-mac performs load-balance according to the source MAC

dst-mac performs load-balance according to the destination MAC

dst-src-mac performs load-balance according to the source and destination MAC

src-ip performs load-balance according to the source IP

dst-ip performs load-balance according to the destination IP

dst-src-ip performs load-balance according to the destination and source IP

dst-src-mac-ip: performs load-balance according to the destination and source mac and destination, source IP

ingress-port: performs load-balance according to the port of receive flow.

Command mode: Global mode.

Default: Perform load-balance according to the source MAC.

Usage **Guide**: Use port-channel to implement load-balance, user can configure the load-balance mode according to the requirements. If the specific load-balance mode of the command line is different with the current load-balance mode of port-group, then modify the load-balance of port-group as the specific load-balance of command line; otherwise return a message to notice that the current mode is already configured.

Example: Set load-balance mode of port-group.

Switch(config)#interface port-channel 1

Switch**(**Config-If-Port-Channel1)#load-balance src-mac

2.7.7 load-balance enhanced profile

This command is not supported by the switch.

2.7.8 l2 field

This command is not supported by the switch.

2.7.9 l2 mpls field l2payload

This command is not supported by the switch.

2.7.10 l2 mpls field l3payload

This command is not supported by the switch.

2.7.11 ipv4 field

This command is not supported by the switch.

2.7.12 ipv6 field

This command is not supported by the switch.

2.7.13 l3 mpls field

This command is not supported by the switch.

2.7.14 mpls tunnel field

This command is not supported by the switch.

2.7.15 mim field l2payload

This command is not supported by the switch.

2.7.16 mim field l3payload

This command is not supported by the switch.

2.7.17 mim tunnel field

This command is not supported by the switch.

2.7.18 trill field l2payload

This command is not supported by the switch.

2.7.19 trill field l3payload

This command is not supported by the switch.

2.7.20 trill tunnel field l2payload

This command is not supported by the switch.

2.7.21 trill tunnel field l3payload

This command is not supported by the switch.

2.7.22 trill tunnel field outerl2

This command is not supported by the switch.

2.7.23 port-group

Command: port-group <*port-group-number*>

no port-group <*port-group-number*>

Function: Creates a port group. The no command deletes that group.

Parameters: <*port-group-number*> is the group number of a port channel from 1～128.

Default: There is no port-group.

Command mode: Global Mode

Notice: it can create 16 port group at most

Example: Creating a port group.

Switch(config)# port-group 1

Delete a port group.

Switch(config)#no port-group 1

2.7.24 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 1～128; **active** enables LACP on the port and sets it in Active mode; **passive** enables LACP on the port and sets it in Passive mode; **on** forces the port to join a port channel without enabling LACP.

Command mode: Port Mode.

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

Usage Guide: Every port joined the port-group must be consistent on the rate, configuration and physical property. 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.

Notice: it can create 16 port group at most

Example: Under the Port Mode of Ethernet1/0/1, add current port to “port-group 1” in “active” mode.

Switch(Config-If-Ethernet1/0/1)#port-group 1 mode active

2.7.25 show port-group

Command: show port-group [*<port-group-number>*] {brief | detail |}

Function: Display the specified group number or the configuration information of all port-channel which have been configured.

Parameters: ***<port-group-number>*** is the group number of port channel to be displayed, from 1～128; **brief** displays summary information; **detail** displays detailed information.

Command mode: All Configuration Mode.

Usage Guide: If the user does not input port-group-number, that means the information of all the existent port-group are showed; if the port channel corresponds to port-group-number parameter and is not exist, then print a error message, otherwise display the current port-channel information of the specified group number.

Example: 1. Display summary information for port-group 1.

```
Switch#show port-group brief
ID: port group number; Mode: port group mode such as on active or passive;
Ports: different types of port number of a port group,
    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  0x8000,00-12-cf-4d-e1-a1  8,1,1       dst-src-mac
10   passive 0x8000,00-12-cf-4d-e1-b2  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: 0x8000,00-03-0f-0c-16-6d
Local:
Port                Status          Priority  Oper-Key    Flag
--------------------------------------------------------------
  Ethernet1/0/1     Selected        32768     1           {ACDEF}
  Ethernet1/0/2     Selected        32768     1           {ACDEF}
  Ethernet1/0/3     Selected        32768     1           {ACDEF}
  Ethernet1/0/4     Selected        32768     1           {ACDEF}
  Ethernet1/0/5     Selected        32768     1           {ACDEF}
  Ethernet1/0/6     Selected        32768     1           {ACDEF}
```

```
   Ethernet1/0/7        Selected      32768       1           {ACDEF}
   Ethernet1/0/8        Selected      32768       1           {ACDEF}
   Ethernet1/0/20       Unselected    32768       1           {ACG}
Ethernet1/0/23       Standby       32768       1           {AC}

Remote:
Actor                Partner   Priority   Oper-Key    SystemID                        Flag
--------------------------------------------------------------------------------
Ethernet1/0/1        1           32768       1           0x8000,00-03-0f-01-02-04      {CDEF}
   Ethernet1/0/2       2           32768       1           0x8000,00-03-0f-01-02-04      {CDEF}
   Ethernet1/0/3       3           32768       1           0x8000,00-03-0f-01-02-04      {CDEF}
   Ethernet1/0/4       4           32768       1           0x8000,00-03-0f-01-02-04      {CDEF}
   Ethernet1/0/5       5           32768       1           0x8000,00-03-0f-01-02-04      {CDEF}
   Ethernet1/0/6       6           32768       1           0x8000,00-03-0f-01-02-04      {CDEF}
   Ethernet1/0/7       7           32768       1           0x8000,00-03-0f-01-02-04      {CDEF}
   Ethernet1/0/8       8           32768       1           0x8000,00-03-0f-01-02-04      {CDEF}
   Ethernet1/0/23      23          32768       1           0x8000,00-03-0f-01-02-04      {C}
Switch#
```

2.7.26 show load-balance enhanced-profile

This command is not supported by the switch.

2.8 MTU

2.8.1 mtu

Command: mtu [<mtu-value>]

no mtu

Function: Configure the MTU size of JUMBO frame, enable the jumbo receiving/sending function. The no **command** restores to the normal frame receiving function.

Parameter: mtu-value: the MTU value of frames that can be received, in byte, ranging from <1500-12270>. The corresponding frame size is <1518/1522-12288/12292>. Without setting is parameter, the allowed max frame size is 12288/12292.

Default: MTU function not enabled by default.

Command Mode: Global Mode

Usage Guide: Set switch of both ends mtu necessarily, or mtu frame will be dropped at the switch

has not be set.

Example: Enable the mtu function of the switch.

Switch(config)#mtu

2.9 bpdu-tunnel

2.9.1 bpdu-tunnel dmac

This command is not supported by the switch.

2.9.2 bpdu-tunnel stp

This command is not supported by the switch.

2.9.3 bpdu-tunnel gvrp

This command is not supported by the switch.

2.9.4 bpdu-tunnel uldp

This command is not supported by the switch.

2.9.5 bpdu-tunnel lacp

This command is not supported by the switch.

2.9.6 bpdu-tunnel dot1x

This command is not supported by the switch.

2.9.7 bpdu-tunnel-protocol

Command: bpdu-tunnel-protocol{stp| gvrp| dot1x| user-defined-protocol <name>}

no bpdu-tunnel-protocol {stp| gvrp| dot1x| user-defined-protocol <name>}

Function: Enable bpdu-tunnel-protocol function of some protocol in port.

Parameter: stp: enable bpdu-tunnel-protocol of stp function in port.

gvrp: enable bpdu-tunnel-protocol of avrp function in port.

dot1x: enable bpdu-tunnel-protocol of dot1x function in port.

name: enable bpdu-tunnel-protocol of neme function in port, the protocol name range from 1 to 32 bytes, and it made up with character, data, underline and the head and tail

character can not be underline.
Default: None.
Command Mode: Port Mode.
Usage Guide**:** When finished configure bpdu-tunnel-protocol destination MAC address of some protocol, users can enable bpdu-tunnel-protocol function of protocol in port. Stp, gvrp or dot1x function mutex with bpdu-tunnel-protocol function in port, namely, if configured stp, gvrp or dot1x function in port, the bpdu-tunnel-protocol function of the protocol configured failed; if configured bpdu-tunnel-protocol function of this protocol in port, stp, gvrp or dot1x function can not configured in port.
Example: Configure bpdu-tunnel-protocol to enable stp protocol in port 1/0/1.
Switch(Config-If-Ethernet1/0/1)# bpdu-tunnel-protocol stp

2.9.8 bpdu-tunnel-protocol group-mac

Command: bpdu-tunnel-protocol {stp| gvrp| dot1x} {group-mac <mac> | default-group-mac}
no bpdu-tunnel-protocol {stp| gvrp| dot1x}
Function: Configure bpdu-tunnel-protocol address of specified protocol. After switch received protocol packets, if receive port enable bpdu-tunnel-protocol function, for configured this command packets, it will change destination mac address to specified bpdu-tunnel-protocol mac address. If input port of transfer protocol packets enables bpdu-tunnel-protocol function, it will receive destination mac address of packets to configure address for the command, and change mac of protocol packets to itself mac of protocol packets.
Parameters: stp: configure bpdu-tunnel-protocol mac of stp protocol;
Gvrp: configure bpdu-tunnel-protocol mac of gvrp protocol;
dot1x: configure bpdu-tunnel-protocol mac of dot1x protocol;
<mac>: bpdu-tunnel-protocol mac address must be multicast address and it can not be protocodl saved address, namely address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30;
default-group-mac: the default mac address is 01-00-0c-cd-00-02.
Default: None.
Command Mode: Global Mode.
Usage Guide: This command must be configured before configure bpdu-tunnel-protocol in port.
Example: Configure 01-01-00-0c -00-02 bpdu-tunnel-protocol of stp protocol.
Switch(Config)# bpdu-tunnel-protocol stp group-mac 01-01-00-0c -00-02

2.9.9 bpdu-tunnel-protocol protocol-mac

Command: bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> {group-mac <mac> | default-group-mac}
no bpdu-tunnel-protocol user-defined-protocol <name>
Function: Configure mac address to identify characteristics of agreement and satisfy the protocol of bpdu-tunnel-protocol mac.

Parameters: name: it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline;
protocol-mac <mac>: it is the mac address of protocol;
group-mac <mac> : it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30;
default-group-mac: The default mac address is 01-00-0c-cd-00-02.
Default: None.
Command Mode: Global Mode.
Usage Guide: The command must be configured before bpdu-tunnel-protocol in port.
Example: Configure 01-01-00-0c-00-03 to be the bpdu-tunnel-protocol of mrpp protocol.
Switch(Config)# bpdu-tunnel-protocol user-defined-protocol mrpp protocol-mac 00-03-0f-00-00-02 group-mac 01-01-00-0c -00-03

2.9.10 bpdu-tunnel-protocol ethernetii

Command: bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> encape-type ethernetii protocol-type <type> {group-mac <mac> | default-group-mac}
no bpdu-tunnel-protocol user-defined-protocol <name>
Function: Configure protocol feature that aimed at mac address and protocol type, the encapsulation type of the protocol is EthernetII and appointed the bpdu-tunnel-protocol mac of the protocol.
Parameters: name: it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline;
protocol-mac <mac>: it is the mac address of protocol;
<type>: the value of protocol and the format is xx-xx.
group-mac <mac> : it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30;
default-group-mac: The default mac address is 01-00-0c-cd-00-02.
Default: None.
Command Mode: Global Mode.
Usage Guide: The command must be configured before bpdu-tunnel-protocol in port.
Example: Configure 01-01-00-0c-00-04 to be the bpdu-tunnel-protocol of lldp protocol.
Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac 01-80-c2-00-00-0e encape-type ethernetii protocol-type 88-cc group-mac 01-01-00-0c -00-04

2.9.11 bpdu-tunnel-protocol snap

Command: bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac>

encape-type snap {oui <oui>| } protocol-type <type> {group-mac <mac> | default-group-mac}
no bpdu-tunnel-protocol user-defined-protocol <name>

Function: Configure protocol feature that aimed at mac address, oui and protocol type, the encapsulation type of the protocol is 802.3/802.2 SNAP or 802.3/802.2 SNAP RFC 1042 (Not configure OUI) and appointed the bpdu-tunnel-protocol mac of the protocol.

Parameters: name: it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline;

protocol-mac <mac>: it is the mac address of protocol;

<oui>: the value of oui and the format is xx-xx-xx;

<type>: the value of protocol and the format is xx-xx.

group-mac <mac> : it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30;

default-group-mac: The default mac address is 01-00-0c-cd-00-02.

Default: None.

Command Mode: Global Mode.

Usage Guide: The command must be configured before bpdu-tunnel-protocol in port.

Example: Configure 01-01-00-0c-00-05 to be the bpdu-tunnel-protocol of Apple Talk protocol.

Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac 00-03-c2-00-00-05 encape-type snap oui 08-00-07 protocol-type 80-9b group-mac 01-01-00-0c -00-05

2.9.12 bpdu-tunnel-protocol llc

Command: bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> encape-type llc dsap <dsap> ssap <ssap> {group-mac <mac> | default-group-mac}
no bpdu-tunnel-protocol user-defined-protocol <name>

Function: Configure protocol feature that aimed at mac address, dsap and ssap type, the encapsulation type of the protocol is 802.3/802.2 LLC and appointed the bpdu-tunnel-protocol mac of the protocol.

Parameters: name: it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline;

protocol-mac <mac>: it is the mac address of protocol;

<dsap>: The dsap value of protocol and it ranges from 0 to 255;

<ssap>: The ssap value of protocol and it ranges from 0 to 255;

group-mac <mac> : it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30;

default-group-mac: The default mac address is 01-00-0c-cd-00-02.

Default: None.

Command Mode: Global Mode.

Usage Guide: The command must be configured before bpdu-tunnel-protocol in port.

Example: Configure 01-01-00-0c-00-06 to be the bpdu-tunnel-protocol of NetBIOS protocol.

Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac 00-03-c2-00-00-06 encape-type llc dsap 240 ssap 224 group-mac 01-01-00-0c -00-06

2.10 DDM

2.10.1 clear transceiver threshold-violation

Command: clear transceiver threshold-violation [interface ethernet <interface-list>]

Function: Clear the threshold violation of the transceiver monitoring.

Parameter: interface ethernet <interface-list>: The interface list that the threshold violation of the transceiver monitoring needs to be cleared.

Command Mode: Admin mode

Default: None.

Usage Guide: None.

Example: Clear he threshold violation of the transceiver monitoring on port 21, 25, 26, 28.

Switch#clear transceiver threshold-violation interface ethernet 1/0/21;25-26;28

2.10.2 debug transceiver

Command: debug transceiver {on | off}

Function: Enable/disable DDM debugging.

Parameter: on/off: Enable or disable the debugging.

Command Mode: Admin mode

Default: Off.

Usage Guide: Disable the DDM debugging with ctrl+o.

Example: Enable DDM debugging.

Switch#debug transceiver on

2.10.3 show transceiver

Command: show transceiver [interface ethernet <interface-list>] [detail]

Function: Show the monitoring of the transceiver.

Parameter: interface ethernet <interface-list>: The interface list that the monitoring of the transceiver needs to be shown.

detail：Show the detailed monitoring of the transceiver.

Command Mode: User mode, admin mode and global mode

Default: None.

Usage Guide: Temperature can be accurate to the integer, other values can be accurate to the second bit after the radix point. When the parameter exceeds the warning threshold, it is shown with 'W+' or 'W-', when the parameter exceeds the alarm threshold, it is shown with 'A+' or 'A-', no tagged parameter is normal.

Example: Show the brief DDM information of all ports.

```
Switch#show transceiver
Interface   Temp（℃）  Voltage（V）  Bias（mA）  RX Power（dBM）  TX Power（dBM）
    1/0/21      33          3.31          6.11          -30.54(A-)          -6.01
1/0/23      33          5.00（W+）  6.11          -20.54(W-)          -6.02
```

2.10.4 show transceiver threshold-violation

Command: show transceiver threshold-violation [interface ethernet <interface-list>]

Function: Show the transceiver monitoring.

Parameter: interface ethernet <interface-list>: The interface list that the transceiver monitoring needs to be shown.

Command Mode: Admin mode and global mode

Default: None.

Usage Guide: None.

Example: Show the transceiver monitoring.

```
Switch(config)#show transceiver threshold-violation interface ethernet 1/0/21-22
Ethernet 1/0/21 transceiver threshold-violation information：
Transceiver monitor is enabled. Monitor interval is set to 30 minutes.
The current time is Jan 02 12:30:50 2010.
The last threshold-violation time is Jan 01 1:30:50 2010.
Brief alarm information:
  RX loss of signal
  RX power low
Detail diagnostic and threshold information:
                          Diagnostic                                  Threshold
                    Realtime Value   High Alarm   Low Alarm    High Warn    Low Warn
                    ----------------  ----------  ----------  -----------  ---------
Temperature（℃）  33               70           0           70           0
Voltage（V）      7.31             10.00        0.00        5.00         0.00
Bias current（mA） 3.11            10.30        0.00        5.00         0.00
RX Power（dBM）   -30.54(A-)       9.00         -25.00（-34） 9.00         -25.00
TX Power（dBM）   -1.01            9.00         -12.05      9.00         -10.00

Ethernet 1/0/26 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30 minutes.
The last threshold-violation doesn't exist.
```

2.10.5 transceiver-monitoring

Command: transceiver-monitoring {enable | disable}
Function: Enable/ disable the transceiver monitoring.
Parameter: enable/ disable: Enable or disable the function.
Command Mode: Port mode
Default: Disable.
Usage Guide: None.
Example: Enable the transceiver monitoring of ethernet1/0/1.
Switch(config-if-ethernet1/0/1)#transceiver-monitoring enable

2.10.6 transceiver-monitoring interval

Command: transceiver-monitoring interval <minutes>
no transceiver-monitoring interval
Function: Set the interval of the transceiver monitoring. The no command sets the interval to be the default interval of 15 minutes.
Parameter: <minutes>: The interval of the transceiver monitoring needs to be set.
Command Mode: Global mode
Default: 15 minutes.
Usage Guide: None.
Example: Set the interval of the transceiver monitoring as 1 minute.
Switch(config)#transceiver-monitoring interval 1

2.10.7 transceiver threshold

Command: transceiver threshold {default | {temperature | voltage | bias | rx-power | tx-power} {high-alarm | low-alarm | high-warn | low-warn} {<value> | default}}
Function: Set the threshold defined by the user.
Parameters: default: Restore the threshold as the default threshold set by the manufacturer. If the monitoring index is not specified, restore all thresholds, if the monitoring index is specified, restore the corresponding threshold only.
temperature：The monitoring index—temperature
voltage：The monitoring index—voltage
bias：The monitoring index—bias current
rx-power：The monitoring index—receiving power
tx-power：The monitoring index—sending power
high-alarm：High-alarm of the monitoring index, namely there is alarm with A+ if exceeding the threshold.
low-alarm：Low-alarm of the monitoring index, namely there is alarm with A- if exceeding the threshold.
high-warn：High-warn of the monitoring index, namely there is warning with W+ if exceeding the threshold.

low-warn： Low-warn of the monitoring index, namely there is warning with W- if exceeding the threshold.

Command Mode: Port mode

Default: The threshold is set by the manufacturer.

Usage Guide: The range of the threshold parameters is shown for each monitoring index in the following:

Temperature: -128.00~128.00 ℃

Voltage: 0.00~7.00 V

Bias current: 0.00~140.00 mA

x-power: -50.00~9.00 dBM

tx-power: -50.00~9.00 dBM

The maximum length of the threshold parameter configured by the user is 20 bits. After the user configured a parameter threshold, the threshold set by the manufacturer will be labeled with the bracket when showing the threshold, and decide whether give an alarm according to the user's configuration.

Example: Configure tx-power threshold of the fiber module, the low-warn threshold is configured as -12 on ethernet1/0/1.

Switch(config-if-ethernet1/0/1)#transceiver threshold tx-power low-warning -12

2.10.8 optician monitor enable|disable

This command is not supported by the switch.

2.11 EFM OAM

2.11.1 clear ethernet-oam

Command: clear ethernet-oam [interface {ethernet |} <*IFNAME*>]

Function: Clear the statistic information of packets and link event on specific or all ports for OAM.

Parameters: <*IFNAME*>, the name of the port needs to clear OAM statistic information

Command Mode: Admin mode

Default: N/A.

Usage Guide: N/A.

Example: Clear the statistic information of OAM packets and link event on all ports.

Switch(config)#clear ethernet-oam

2.11.2 debug ethernet-oam error

Command: debug ethernet-oam error [interface {ethernet |} <*IFNAME*>]

no debug ethernet-oam error [interface {ethernet |} <*IFNAME*>]

Function: Enable the debugging of OAM error information, no command disables it.

Parameters: <*IFNAME*>: name of the port that the debugging will be enabled or disabled.

Command Mode: Admin mode
Default: Disable.
Usage Guide: N/A.
Example: Enable the debugging of OAM error information for ethernet1/0/1.
Switch#debug ethernet-oam error interface ethernet1/0/1

2.11.3 debug ethernet-oam event

This command is not supported by the switch.

2.11.4 debug ethernet-oam fsm

Command: debug ethernet-oam fsm {all | Discovery | Transmit} [interface {ethernet |} <*IFNAME*>]

no debug ethernet-oam fsm {all | Discovery | Transmit} [interface {ethernet |} <*IFNAME*>]

Function: Enable the debugging of OAM state machine, no command disables it.
Parameters: <IFNAME>: name of the port that the debugging will be enabled or disabled
Command Mode: Admin mode
Default: Disable.
Usage Guide: N/A.
Example: Enable the debugging of Discovery state machine for ethernet1/0/1.
Switch#debug ethernet-oam fsm Discovery interface ethernet1/0/1.

2.11.5 debug ethernet-oam packet

Command: debug ethernet-oam packet [detail] {all | send | receive} [interface {ethernet |} <*IFNAME*>]

no debug ethernet-oam packet [detail] {all | send | receive} interface {ethernet |} <*IFNAME*>

Function: Enable the debugging of packets received or sent by OAM, no command disables the debugging.
Parameters: <*IFNAME*>: name of the port that the debugging will be enabled or disabled
Command Mode: Admin mode
Default: Disable.
Usage Guide: N/A.
Example: Enable the debugging of packets received or sent for ethernet1/0/1.
Switch#debug ethernet-oam packet detail all interface ethernet1/0/1

2.11.6 debug ethernet-oam timer

Command: debug ethernet-oam timer {all | pdu_timer | local_lost_link_timer} [interface {ethernet |} <IFNAME>]

no debug ethernet-oam timer {all | pdu_timer | local_lost_link_timer} [interface {ethernet | } <IFNAME>]

Function: Enable the debugging of refreshing information for specific or all timers, no this command disables the debugging.

Parameters: <*IFNAME*>: name of the port that the debugging will be enabled or disabled

Command Mode: Admin mode

Default: Disable.

Usage Guide: N/A.

Example: Enable the debugging of refreshing information for all timers of ethernet1/0/1.

Switch#debug ethernet-oam timer all interface ethernet1/0/1

2.11.7 ethernet-oam

Command: ethernet-oam

no ethernet-oam

Function: Enable ethernet-oam of ports, no command disables ethernet-oam of ports.

Parameters: None.

Command Mode: Port mode

Default: Disable.

Usage Guide: N/A.

Example: Enable ethernet-oam of Ethernet 1/0/4.

Switch(config)#interface ethernet 1/0/4

Switch(Config-If-Ethernet1/0/4)#ethernet-oam

2.11.8 ethernet-oam errored-frame threshold high

Command: ethernet-oam errored-frame threshold high {<*high-frames*> | none}

no ethernet-oam errored-frame threshold high

Function: Configure the high threshold of errored frame event, no command restores the default value.

Parameters: <*high-frames*>, the high detection threshold of errored frame event, ranging from 2 to 4294967295.

none, cancel the high threshold configuration.

Command Mode: Port mode

Default: none.

Usage Guide: During the specific detection period, serious link event is induced if the number of errored frame is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold can not be less than the low threshold.

Example: Configure the high threshold of errored frame event on Ethernet 1/0/4 to be 3000.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold high 3000

2.11.9 ethernet-oam errored-frame threshold low

Command: ethernet-oam errored-frame threshold low <*low-frames*>

no ethernet-oam errored-frame threshold low

Function: Configure the low threshold of errored frame event, no command restores the default value.

Parameters: <*low-frames*>, the low detection threshold of errored frame event, ranging from 1 to 4294967295.

Command Mode: Port mode

Default: 1.

Usage Guide: During the specific detection period, errored frame event is induced if the number of errored frame is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold can not be larger than the high threshold.

Example: Configure the low threshold of errored frame event on Ethernet 1/0/4 to 100.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold low 100

2.11.10 ethernet-oam errored-frame window

Command: ethernet-oam errored-frame window <*seconds*>

no ethernet-oam errored-frame window

Function: Configure the detection period of errored frame event, no command restores the default value.

Parameters: <*seconds*> is the time for counting the specified frame number, its range from 5 to 300, unit is 200ms.

Command Mode: Port mode

Default: 5.

Usage Guide: Detect the errored frame number of the port after the time of specific detection period. If the number of errored frame is larger than or equal to the threshold, bring the corresponding event and notify the peer through OAMPDU.

Example: Configure the detection period of errored frame event on port1/0/4 to be 20s.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame window 100

2.11.11 ethernet-oam errored-frame-period threshold high

Command: ethernet-oam errored-frame-period threshold high {<*high-frames*> | none}

no ethernet-oam errored-frame-period threshold high

Function: Configure the high threshold of errored frame period event, no command restores the default value.

Parameters: <*high-frames*>, the high detection threshold of errored frame period event, ranging from 2 to 4294967295.

none, cancel the high threshold configuration.

Command Mode: Port mode

Default: none.

Usage Guide: During the specific detection period, serious link event is induced if the number of errored frame is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold can not be less than the low threshold.

Example: Configure the high threshold of errored frame period event on port 1/0/4 to be 3000.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-period threshold high 3000

2.11.12 ethernet-oam errored-frame-period threshold low

Command: ethernet-oam errored-frame-period threshold low <*low-frames*>

no ethernet-oam errored-frame-period threshold low

Function: Configure the low threshold of errored frame period event, no command restores the default value.

Parameters: <*low-frames*>, the low detection threshold of errored frame period event, ranging from 1 to 4294967295 frames.

Command Mode: Port mode

Default: 1.

Usage Guide: During the specific detection period, errored frame period event is induced if the number of errored frame is larger than or equal to the low threshold and the device notifies the peer by event notification OAMPDU. Note that the low threshold should not be larger than the high threshold.

Example: Configure the low threshold of errored frame period event on port 1/0/4 to be 100.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-period threshold low 100

2.11.13 ethernet-oam errored-frame-period window

Command: ethernet-oam errored-frame-period window <*seconds*>

no ethernet-oam errored-frame-period window

Function: Configure the detection period of errored frame period event, no command restores the default value.

Parameters: <*seconds*> is the time for counting the specified frame number, its range from 1 to 300, unit is 200ms.

Command Mode: Port mode

Default: 5.

Usage Guide: Detect errored frame of the port after the time of specific detection period. If the number of errored frame is larger than or equal to the threshold, corresponding event is induced and the device notifies the peer through OAMPDU. When sending the packets, the maximum number of frames is filled as the value of window in errored frame period event. The conversion rule is maximum number of frames= interface bandwidth×detection period of errored frame period event(s)÷(64×8), of which the detection period is the number of seconds in window of

the configuration.

Example: Configure the detection period of errored frame period event on port 1/0/4 to be 10s.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-period window 50

2.11.14 ethernet-oam errored-frame-seconds threshold high

Command: ethernet-oam errored-frame-seconds threshold high {<*high-seconds*> | none}

no ethernet-oam errored-frame-seconds threshold high

Function: Configure the high threshold of errored frame seconds event, no command restores the default value.

Parameters: <*high-seconds*>, the high detection threshold of errored frame seconds event, ranging from 2 to 65535 seconds.

none, cancel the high threshold configuration.

Command Mode: Port mode

Default: none.

Usage Guide: During the specific detection period, serious link event is induced if the number of errored frame seconds is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold should not be less than the low threshold. The definition of errored frame seconds is the second in which errored frame is received.

Example: Configure the high threshold of errored frame seconds event on port 1/0/4 to be 3000.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold high 3000

2.11.15 ethernet-oam errored-frame-seconds threshold low

Command: ethernet-oam errored-frame-seconds threshold low <*low-seconds*>

no ethernet-oam errored-frame-seconds threshold low

Function: Configure the low threshold of errored frame seconds event, no command restores the default value.

Parameters: <*low-seconds*>, the low detection threshold of errored frame seconds event, ranging from 1 to 65535 seconds.

Command Mode: Port mode

Default: 1.

Usage Guide: During the specific detection period, errored frame seconds event is induced if the number of errored frame seconds is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold should not be larger than the high threshold. The definition of errored frame seconds is the second in which errored frame is received.

Example: Configure the low threshold of errored frame seconds event on port 1/0/4 to be 100.

Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold low 100

2.11.16 ethernet-oam errored-frame-seconds window

Command: ethernet-oam errored-frame-seconds window <*seconds*>

no ethernet-oam errored-frame-seconds window

Function: Configure the detection period of errored frame seconds event, no command restores the default value.

Parameters: <*seconds*> is the time for counting the specified frame number, its range from 50 to 450, unit is 200ms.

Command Mode: Port mode

Default: 300.

Usage Guide: Detect errored frame seconds of the port after the time of specific detection period. If the number of errored frame seconds is larger than or equal to the threshold, corresponding event is induced and the device notified the peer through OAMPDU.

Example: Configure the detection period of errored frame seconds event on port 1/0/4 to be 120s.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds window 600

2.11.17 ethernet-oam errored-symbol-period threshold high

Command: ethernet-oam errored-symbol-period threshold high {<*high-symbols*> | none}

no ethernet-oam errored-symbol-period threshold high

Function: Configure the high threshold of errored symbol event, no command restores the default value.

Parameters: <*high-symbols*>, the high detection threshold of errored symbol event, ranging from 2 to 18446744073709551615 symbols.

none, cancel the high threshold configuration.

Command Mode: Port mode

Default: none.

Usage Guide: During the specific detection period, serious link event is induced if the number of errored symbols is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold should not be less than the low threshold.

Example: Set the high threshold of errored symbol event on port 1/0/4 to none.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold high none

2.11.18 ethernet-oam errored-symbol-period threshold low

Command: ethernet-oam errored-symbol-period threshold low <*low-symbols*>

no ethernet-oam errored-symbol-period threshold low

Function: Configure the low threshold of errored symbol event, no command restores the default value.

Parameters: <*low-symbols*>, the low threshold of errored symbol event, ranging from 1 to 18446744073709551615 symbols.

none, cancel the high threshold configuration.

Command Mode: Port mode

Default: 1.

Usage Guide: During the specific detection period, errored symbol event is induced if the number of errored symbols is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold should not be larger than the high threshold.

Example: Set the low threshold of errored symbol event on port 1/0/4 to be 5.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold low 5

2.11.19 ethernet-oam errored-symbol-period window

Command: ethernet-oam errored-symbol-period window <*seconds*>

no ethernet-oam errored-symbol-period window

Function: Configure the detection period of errored symbol event, no command restores the default value.

Parameters: <*seconds*> is the time for counting the specified frame number, its range from 5 to 300, unit is 200ms.

Command Mode: Port mode

Default: 5.

Usage Guide: Detect errored symbols of the port after the time of specific detection period. If the number of errored symbols is larger than or equal to the threshold, corresponding event is induced and the device notified the peer through OAMPDU.

Example: Set the detection period of errored symbol event on port 1/0/4 to be 2s.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period window 10

2.11.20 ethernet-oam link-monitor

Command: ethernet-oam link-monitor

no ethernet-oam link-monitor

Function: Enable link monitor, no command disables the function.

Parameters: None.

Command Mode: Port mode

Default: Enable.

Usage Guide: Enable OAM to monitor local link errors. Generally link monitor is enabled when enabling OAM function of the port. When OAM link monitor is disabled, although local link error is not monitored, Event information OAMPDU from the peer is still normally received and

processed.

Example: Enable the link monitor of port 1/0/4.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam link-monitor

2.11.21 ethernet-oam mode

Command: ethernet-oam mode {active | passive}

no ethernet-oam mode

Function: Configure the mode of OAM function, no command restores the default value.

Parameters: active, active mode

passive, passive mode

Command Mode: Port mode

Default: active mode.

Usage Guide: At least one of the two connected OAM entities should be configured to active mode. Once OAM is enabled, the working mode of OAM cannot be changed and you need to disable OAM function if you have to change the working mode.

Example: Set the mode of OAM function on ethernet 1/0/4 to passive mode.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam mode passive

2.11.22 ethernet-oam period

Command: ethernet-oam period <*seconds*>

no ethernet-oam mode

Function: Configure the transmission period of Information OAMPDU, no command restores the default value.

Parameters: <*seconds*>, sending period, ranging from 1 to 2 seconds.

Command Mode: Port mode

Default: 1s.

Usage Guide: Use this command to configure the transmission interval of Information OAMPDU which keep OAM connection normally.

Example: Set the transmission interval of Information OAMPDU for ethernet 1/0/4 to be 2s.

Switch(Config-If-Ethernet1/0/4)# ethernet-oam period 2

2.11.23 ethernet-oam remote-failure

Command: ethernet-oam remote-failure

no ethernet-oam remote-failure

Function: Enable remote failure indication of OAM, no command disables the function.

Parameters: None.

Command Mode: Port mode

Default: Enable.

Usage Guide: With remote failure indication is enabled, if critical-event or link fault event is occurred locally, it will notify the peer by sending Information OAMPDU, log the fault information

and send SNMP trap warning. When the remote failure indication is disabled, although local critical-event or link fault event is not monitored, failure indication information from the peer is still normally received and processed.

Example: Enable remote failure indication of ethernet 1/0/4.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-failure

2.11.24 ethernet-oam remote-loopback

Command: ethernet-oam remote-loopback

no ethernet-oam remote-loopback

Function: Local OAM send remote-loopback request to enable remote to come in OAM loopback mode; the no command cancel remote-loopback.

Parameters: None.

Command Mode: port mode.

Default: Disable.

Usage Guide**:** Only OAM can send remote loopback reques in auto mode, the OAM work in passive mode can not send remote loopback; when remote OAM working in loopback mode, all packets except OAM PDU packets will back local port according to the same route (Notice: during OAM loopback, it can not communicate), administrator can check the link delay of loopback, shake and throughput capacity. It can do loopback configuration after create OAM link, if OAM link is broken during loopback, the loopback will be cancel automatically. The command mutex with ethernet-oam remote-loopback supported.

Example: Enable the remote OAM of port 1/0/4 to remote loopback mode.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-loopback

Normal forwarding will be suspended during the remote-loopback, are you sure to start remote-loopback? [Y/N]

2.11.25 ethernet-oam remote-loopback supported

Command: ethernet-oam remote-loopback supported

no ethernet-oam remote-loopback **supported**

Function: Enable the support of port OAM loopback, the no command disable loopback support.

Parameters: None.

Command Mode: Port mode.

Default: Disable.

Usage Guide: The port that only enable loopback support function can receive OAM loopback reques and in loopback mode. So when enable remote and in OAM loopback, please ensure remote configured loopback support. The command mutex with ethernet-oam remote-loopback.

Example: Enable OAM loopback support function of ethernet 1/0/4.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-loopback supported

2.11.26 ethernet-oam timeout

Command: ethernet-oam timeout *<seconds>*

no ethernet-oam timeout

Function: Configure the timeout of OAM connection, no command restores the default value.

Parameters: <*seconds*>, the timeout ranging from 5 to 10 seconds.

Command Mode: Port mode

Default: 5s.

Usage Guide: OAM connection will be disconnected if no OAMPDU is received after specified timeout.

Example: Set the timeout of OAM connection for ethernet 1/0/4 to be 6 seconds.

Switch(Config-If-Ethernet1/0/4)#ethernet-oam timeout 6

2.11.27 show ethernet-oam

Command: show ethernet-oam [{local | remote} interface {ethernet |} <*IFNAME*>]

Function: Show Ethernet OAM connection of specified or all ports.

Parameters: Overview information of all Ethernet OAM connections will be shown if no parameters is input

local, show detailed information of local OAM connection

remote, show detailed information of remote OAM connection

<*IFNAME*>, the port that OAM connection information will be shown

Command Mode: Admin mode

Default: N/A.

Usage Guide: N/A.

Example: Show overview information of Ethernet OAM connection.

Switch#show ethernet-oam

Remote-Capability codes: L - Link Monitor, R - Remote Loopback

U - Unidirection, V - Variable Retrieval

Interface Local-Mode Local-Capability Remote-MAC-Addr Remote-Mode Remote-Capability

1/0/1	active	L	R	0003.0f02.2e5d	active	L	R
1/0/2	active	L	R	0003.0f19.3a3e	avtive	L	R
1/0/4	active	L	R	0003.0f26.480c	passive	L	R
1/0/5	active	L	R	0003.0f28.020a	active	L	R

Field	Description
Interface	port with Ethernet OAM enabled
Local-Mode	Working mode of the local port OAM.
Local-Capability	Functions are supported by local port OAM L - Link Monitor, R - Remote Loopback U - Unidirection, V - Variable Retrieval
Remote-MAC-Addr	MAC address of the peer

Remote-Mode	OAM working mode of the peer
Remote-Capability	Functions are supported by OAM of the peer L - Link Monitor, R - Remote Loopback U - Unidirection, V - Variable Retrieval

Show detailed information of local OAM entity for ethernet 1/0/2:

```
Switch#show ethernet-oam local interface ethernet1/0/2
Ethernet1/0/2 oam local Information：
oam_status=enable
local _mode=active
period=1s
timeout=8s
Loopback Supported=YES
Unidirectional Support=YES
Link Events=YES
Remote Failure=YES
local_pdu=INFO
local_mux_action=FWD
local_par_action=DISCARD
Max_OAMPDU_Size=1518
---------------------------------------------------------------------------
OAM_local_flags_field：
Link Fault=0        Dying Gasp=0        Critical Events=0
---------------------------------------------------------------------------
Packet statistic：
Packets                 Send                    Receive
OAMPDU                  553                     21
Information             552                     21
Event Notification      1                       0
Loopback Control        0                       0
---------------------------------------------------------------------------
```

Field	Description
oam_status	Status of Ethernet OAM: enable, OAM is enabled; disable, OAM is not enabled.
local _mode	Working mode of Ethernet OAM: active, the port is set as active mode; passive, the port is set as passive mode.
Period	Transmission period of packets
Timeout	Timeout of connection
local_pdu	The way in which the local end processes Ethernet OAMPDUs: RX_INFO, the port only receives Information OAMPDUs and does

	not send any Ethernet OAMPDUs. LF_INFO, the port only sends Information OAMPDU packets without Information TLV and with their link error flag bits being set. INFO, the port only sends and receives Information OAMPDU packets. ANY, the port sends and receives any OAMPDU packets.
local_mux_action	Working mode of the local transmitter: FWD, the port can send any packets; DISCARD, the port only sends OAMPDU packets and discards others.
local_par_action	Working mode of the local receiver in the following: FWD, receiving any packets is allowed; DISCARD, only OAMPDU packets is received while others are discarded; LB, OAM remote loopback is enabled on the port. In this case, all the packets except OAMPDU packets received are returned to their sources along the ways they come.
Loopback Supported	Whether support remote loopback: YES for support and NO for not.
Unidirectional Support	Whether support unidirectional transmission: YES for support and NO for not.
Link Events	Whether support general link events: YES for support and NO for not.
Remote Failure	Whether support severe link events (remote failure indication): YES for support and NO for not.
Link Fault	Whether occur a Link Fault event: 0 for no and 1 for yes.
Dying Gasp	Whether occur a Dying Gasp event: 0 for no and 1 for yes.
Critical Event	Whether occur a Critical Event: 0 for no and 1 for yes.
Max_OAMPDU_Size	The maximum length of OAMPDU is supported.
OAMPDU	Show the number of the OAMPDU packets sent and received which is the sum of three kinds of packets.
Information	Show the number of the Information OAMPDU packets sent and received
Event Notification	Show the number of the Event Notification OAMPDU packets sent and received
Loopback Control	Show the number of the Loopback Control OAMPDU packets sent and received

Display detailed information of remote OAM entity for Ethernet 1/0/2

Switch#show ethernet-oam remote interface ethernet1/0/2

Ethernet1/0/2 oam remote Information：

Remote_Mac_Address=0003.0f19.3a3e

local _mode=active

---

local_pdu=INFO

local_mux_action=FWD

local_par_action=DISCARD

Loopback Supported=YES

Unidirectional Support=NO

Link Events=YES

Remote Failure=YES

Max_OAMPDU_Size=1518

OAM Remote Flags Field：

Link Fault=0 Dying Gasp=0 Critical Event=0

Field	Description
Remote_Mac_Address	MAC address of remote OAM entity
local _mode	Working mode of Ethernet OAM: active, the port is set as active mode; passive, the port is set as passive mode.
local_pdu	The way in which the local end processes Ethernet OAMPDUs: RX_INFO, the port only receives Information OAMPDUs and does not send any Ethernet OAMPDUs. LF_INFO, the port only sends Information OAMPDU packets without Information TLV and with their link error flag bits being set. INFO, the port only sends and receives Information OAMPDU packets. ANY, the port sends and receives any OAMPDU packets.
local_mux_action	Working mode of the local transmitter: FWD, the port can send any packets; DISCARD, the port only sends OAMPDU packets and discards others.
local_par_action	Working mode of the local receiver in the following: FWD, receiving any packets is allowed; DISCARD, only OAMPDU packets is received while others are discarded; LB, OAM remote loopback is enabled on the port. In this case, all the packets except OAMPDU packets received are returned to their sources along the ways they come.
Loopback Supported	Whether support remote loopback: YES for support and NO for not.
Unidirectional Support	Whether support unidirectional transmission: YES for support and NO for not.

Link Events	Whether support general link events: YES for support and NO for not.
Remote Failure	Whether support severe link events: YES for support and NO for not.
Max_OAMPDU_Size	The maximum length of OAMPDU is supported.
Link Fault	Whether occur a Link Fault event: 0 for no and 1 for yes.
Dying Gasp	Whether occur a Dying Gasp event: 0 for no and 1 for yes.
Critical Event	Whether occur a Critical Event: 0 for no and 1 for yes.

2.11.28 show ethernet-oam events

Command: show ethernet-oam events {local | remote} [interface {ethernet |} <*IFNAME*>]

Function: Shows the statistic information of link events on specified or all ports with OAM enabled, including general link events and severe link events.

Parameters: local, show the detailed information of the local events;

remote, show the detailed information of the remote events;

<*IFNAME*>, the port that the statistic information of OAM link events needs to be shown, the statistic information of OAM link events for all ports will be shown if this parameter is not specified.

Command Mode: Admin mode

Default: N/A.

Usage Guide: N/A.

Example: Show the statistic information of link events on Ethernet 1/0/1.

```
Switch#show ethernet-oam events local interface 1/0/1
ethernet1/0/1 link-events：
OAM_local_errored-symbol-period-events:
---------------------------------------------------------------------------------------------
event time stamp：3539                    errored symbol window(200ms)：5
errored symbol low threshold：1           errored symbol high threshold：none
errored symbol：1200120                   errored running total：2302512542
event running total：232

OAM_local_errored-frame-period-events:
---------------------------------------------------------------------------------------------
event time stamp：3539                    errored frame window(200ms)：50
errored frame low threshold：1            errored frame high threshold：none
errored frame：1200120                    errored running total：2302512542
event running total：52

OAM_local_errored-frame-events:
---------------------------------------------------------------------------------------------
event time stamp：3539                    errored frame window(200ms)：5
```

errored frame low threshold：1 errored frame high threshold：none
errored frame：1200120 errored running total：2302512542
event running total：75

OAM_local_errored-frame-seconds-summary-events:
---
event time stamp：3520 errored frame seconds summary window(200ms)：300
errored frame low threshold：1 errored frame high threshold：none
errored frame：1200120 errored running total：2302512542
event running total：232

OAM_local_link-fault：0
OAM_local_dying gasp：0
OAM_local_critical event：0

Field	Description
OAM_local_errored-symbol-period-events	Statistic information of the local errored symbol events
OAM_local_errored-frame-period-events	Statistic information of the local errored frame period events
OAM_local_errored-frame-events	Statistic information of the local errored frame events
OAM_local_errored-frame-seconds-summary-events	Statistic information of the local errored frame seconds events
event time stamp	Time stamp of the event
window	Detection period of the event
low threshold	Low threshold of events detection
high threshold	High threshold of events detection
errored frame	the number of errored frames
errored symbol	the number of errored symbols
errored running total	Total number of errors occurred since the reset of OAM function
event running total	Total number of error events occurred since the reset of OAM function
OAM_local_link-fault	The number of the local link-fault faults
OAM_local_dying gasp	The number of the local dying-gasp faults
OAM_local_critical event	The number of the local critical-event faults

2.11.29 show ethernet-oam link-events-configuration

Command: show ethernet-oam link-events-configuration [interface {ethernet | } <*IFNAME*>]

Function: Show configuration of link events on specified or all ports with OAM enabled, including detection period and threshold of the events and so on.

Parameters: <*IFNAME*>, the port that the statistic information of OAM link events needs to be shown, the statistic information of OAM link events for all ports will be shown if this parameter is not specified.

Command Mode: Admin mode

Default: N/A.

Usage Guide: N/A.

Example: Show configuration of link events on ethernet 1/0/1.

```
Switch#show ethernet-oam link-events-configuration interface ethernet 1/0/1
Ethernet1/0/1 link-monitor configuration：
event                          high-threshold    low-threshold    window(200ms)
-------------------------------------------------------------------------------------------------
Err-symbol-Period                   none              1                2
Err-frame-Period                    none              1               10
Err-frame                           none              2                5
Err-frame-second-summary            none              2              600
-------------------------------------------------------------------------------------------------
```

Field	Description
Event	Event type
Err-symbol-Period	Errored symbol event
Err-frame-Period	Errored frame period event
Err-frame	Errored frame event
Err-frame-second-summary	Errored frame seconds event
high-threshold	High threshold
low-threshold	Low threshold
window(200ms)	Detection period, unit is 200ms

2.11.30 show ethernet-oam loopback status

Command: show ethernet-oam loopback status [interface {ethernet | } <IFNAME>]

Function: Display all or specified port OAM loopback status of switch.

Parameters: <*IFNAME*> means display the port of OAM loopback statusinformation, if not appointed the parameters, it will display the OAM loopback status of all port.

Command Mode**:** Admin mode.

Default: None.

Usage Guide**:** None.

Example: Display the OAM loopback status of all port.

Switch(config)#show ethernet-oam loopback status

OAM Loopback Status：

ethernet1/0/1：disable

ethernet1/0/2：loopback_enable_waiting

ethernet1/0/3：loopback_disable_waiting

ethernet1/0/4：loopback_control

ethernet1/0/5：loopback_underControl

Field	Description
disable	Port does not enable OAM loopback support yet.
loopback_enable_waiting	Local is loopback control side, sending remote loopback request and wait remote loopback ensure packets.
loopback_disable_waiting	Local is loopback control side, sending cancel loopback request and wait remote to cancel the ensure packets of loopback.
loopback_control	During loopback and local is loopback control side.
loopback_undercontrol	During loopback and local is loopback controlled end.
no_loopback	Port enable OAM loopback support but not received loopback request.

2.12 PORT SECURITY

2.12.1 clear port-security

Command: clear port-security {all | configured | dynamic | sticky} [[address <*mac-addr*> | interface <*interface-id*>] [vlan <*vlan-id*>]]

Function: Clear the secure MAC entries for the interfaces.

Parameter: all：All secure MAC entries on the interfaces

configured：The configured secure MAC

dynamic：The dynamic secure MAC learnt by the interface

sticky：The secure MAC of sticky

mac-addr：The specified secure MAC address

interface-id：The secure MAC entries of the specified interface

vlan-id：The specified VLAN

Default: None.

Command Mode: Admin mode

Usage Guide: None.

Example: Clear all secure MACs on the interface.

Switch#clear port-security all

2.12.2 show port-security

Command: show port-security [interface <*interface-id*>] [address | vlan]

Function: Show port-security configuration.

Parameter: interface-id： Show port-security configuration of the interface.

address: Show the secure address of the interface.

vlan: Show the maximum number of each VLAN configured on trunk/hybrid interface.

Default: None.

Command Mode: Any modes

Usage Guide: None.

Example: Show all secure MACs on the interfaces.

Switch# show port-security address interface ethernet 1/0/1

2.12.3 switchport port-security

Command: switchport port-security

no switchport port-security

Function: Configure port-security function for the interface, the no command disables port-security.

Parameter: None.

Default: Disable.

Command Mode: Port mode

Usage Guide: Clear all dynamic MACs after the interface enabled port-security, and all MACs learnt from the interfaces are tagged with FDB_TYPE_PORT_SECURITY_DYNAMIC. After disabling port-security of the interfaces, clear all secure MACs or change them into the dynamic MACs.

Example: Enable port-security on the interface.

Switch(config-if- ethernet1/0/1)#switchport port-security

2.12.4 switchport port-security aging

This command is not supported by the switch.

2.12.5 switchport port-security mac-address

Command: switchport port-security mac-address <*mac-address*> [vlan <*vlan-id*>]

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

Function: Configure the static secure MAC on the interface, the no command cancels the configuration.

Parameter: mac-address： Configure the specified MAC address as the static secure MAC.

vlan-id： The specified VLAN of the MAC address, it only takes effect on trunk and hybrid interfaces.

Default: No secure MAC is bound by the interface.

Command Mode: Port mode

Usage Guide: the number of static secure MAC have not been account the maximum MAC limit

Example: Configure the secure MAC address on the interface.
Switch (config-if- ethernet1/0/1)# switchport port-security mac-address 00-00-00-00-00-01

2.12.6 switchport port-security mac-address sticky

Command：switchport port-security mac-address sticky
no switchport *port-security* mac-address sticky
Function：Enable the sticky mac mode for the interface，the type of mac is secure-s, this command is valid for trunk and hybrid port。The no command disables the sticky mac mode for the interface.

Parameter：none

Default：Sticky mac mode is not enabled for *the interface,* the type of mac learned on the interface is dynamic secure mac.
Command Mode: Port mode
Usage Guide：
Configuration of sticky enablement converts macs that have been dynamically learned under secure ports into sticky macs, and the newly learned dynamic macs are also sticky macs. Sticky mac is limited by the number of port security. The difference between sticky mac and dynamic secure mac is that sticky mac does not age.
Cancel configuration sticky enablement and restore the dynamic mac learned under the secure port to the dynamic secure mac.

Example：Enable the sticky mac mode for the interface。
Switch (config-if-ethernet1/0/1)#switchport port-security mac-address sticky

2.12.7 switchport port-security maximum

Command: switchport port-security maximum <*value*> [vlan <*vlan-list*>]
no switchport port-security maximum <*value*> [vlan <*vlan-list*>]
Function: Configure the maximum number of the secure MAC allowed by the interface, if specifying VLAN parameter, it means the maximum number in the configured VLANs. The no command cancels the maximum number of the secure MAC configured by the interface.
Parameter: value：Configure the maximum number of the secure MAC allowed by the interface, its range between 0 and 4096. It is determined by the maximum MAC number of the device.

vlan-id: Configure the maximum value for the specified VLAN, it only takes effect on trunk and hybrid interfaces.
Default: After enabling port-security, if there is no other configuration, the maximum number of the secure MAC is 1 on the interface. The interface number in VLAN is no limit by default
Command Mode: Port mode
Usage Guide: Pay attention to the coupling relation about the number between the interface and VLAN, set the maximum number configured by the interface as the standard firstly.
Example: Configure the maximum number of the secure MAC on the interface.

services Switch(config-if- ethernet1/0/1)# switchport port-security maximum 100

2.12.8 switchport port-security violation

Command: switchport port-security violation {protect | recovery | restrict | shutdown}

no switchport port-security violation

Function: When exceeding the maximum number of the configured MAC addresses, MAC address accessing the interface does not belongs to this interface in MAC address table or a MAC address is configured to several interfaces in same VLAN, both of them will violate the security of the MAC address.

Parameter: protect：Protect mode, it will trigger the action that do not learn the new MAC, drop the package and do not send the warning.

recovery：After triggering the violation action of the port, the mac learning function can be recovered.

restrict：Restrict mode, it will trigger the action that do not learn the new MAC, drop the package, send snmp trap and record the configuration in syslog.

shutdown：Shutdown mode is the default mode. Under this condition, the interface is disabled directly, send snmp trap and record the configuration in syslog.

Default: Shutdown.

Command Mode: Port mode

Usage Guide: None.

Example: Configure violation mode as protect for the interface.

Switch(config-if-ethernet1/0/1)#switchport port-security violation protect

2.13 EEE Energy-saving

2.13.1 eee enable

Command: eee enable

no eee enable

Function: Configure the port to enable eee energy-saving function; the no command deletes it.

Parameters: None.

Command Mode: Port Mode.

Default: None.

Usage Guide: It supports that configure EEE energy-saving function for the appointed port. There is not the EEE energy-saving function on port as default. After configuring the port to enable EEE energy-saving function, the port will enter the energy-saving state if stop to send packets to the port, the state of port is down. When sending packets to the port, the mode will changed from power saving mode to normal mode.

Example: Enable EEE energy-saving function:
Switch(config-if-ethernet1/0/1)#eee enable

2.14 LED shut-off

2.14.1 port-led shutoff time-range

Command: port-led shutoff time-range <time-range-name>
no port-led shutoff
Function: Configure all the LEDs to be off in the appointed time-range. The no command recovers it.
Parameters: time-range-name: it is the name of the time-range defined by user, it is made up by 1 to 64 characters including letters, numbers, underlines. The first and last characters cannot be the underlines.
Command Mode: Global Configuration Mode.
Default: None.
Usage Guide: The LED shut-off function of the port can make all the LEDs off according to the configured time-range by user no matter what the link-act status is. It can save power. When there is no configured time-range, the default is all the times; when the range is exceeded, the port LED can be on according to the link-act status.
Example: Configure all the LEDs to be off in t1.
switch(config)#: port-led shutoff time-range t1

2.15 VLAN

2.15.1 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)#

2.15.2 vlan internal

This command is not supported by the switch.

2.15.3 vlan ingress enable

Command: vlan ingress enable

no vlan ingress enable

Function: Enable the VLAN ingress filtering for a port; the "**no vlan ingress enable**" command disables the ingress filtering.

Command mode: Port Mode

Default: Enable VLAN ingress filtering function.

Usage Guide: After VLAN ingress filtering is 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 the VLAN member port, or else drop the data.

Example: Disable VLAN ingress rules on the port.

Switch(Config-If-Ethernet1/0/1)# no vlan ingress enable

2.15.4 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 an 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 1/0/5

Switch(Config-If-Ethernet1/0/5)#switchport mode trunk

Switch(Config-If-Ethernet1/0/5)#switchport trunk native vlan 100

Switch(Config-If-Ethernet1/0/5)#exit

2.15.5 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 1/0/5

Switch(Config-If-Ethernet1/0/5)#switchport mode trunk

Switch(Config-If-Ethernet1/0/5)#switchport trunk allowed vlan 1;3;5-20

Switch(Config-If-Ethernet1/0/5)#exit

2.15.6 switchport mode trunk allow-null

Command: switchport mode trunk allow-null

Function: Add a port as trunk mode. When enabling GVRP, the mode that adds the ports with trunk mode to all VLANs is not appropriate. Therefore, add a port as trunk port and does not join any VLANs by default for enabling GVRP on trunk port is appropriate. It is recommended to configure a port as trunk with this command before enabling GVRP. This command can also be used when a port has been configured as trunk already, which equals to clearing allow-list and quits all VLANs.

Parameters: None

Command Mode: Port mode

Default: access mode.

Usage Guide: Configure the port as trunk, enable it to leave all VLANs and clear allow-list.

Example: Switch(config-if-ethernet1/0/1)#switchport mode trunk allow-null

2.15.7 switchport mode

Command: switchport mode {trunk | access | hybrid}

Function: Set the port in access mode, trunk mode or hybrid mode.

Parameter: trunk means the port allows traffic of multiple VLAN; **access** indicates the port belongs to one VLAN only; **hybrid** means the port allows the traffic of multi-VLANs to pass with

tag or untag mode.

Command mode: Port Mode.

Default: The port is in Access mode by default.

Usage Guide: Ports in trunk mode is called Trunk ports. Trunk ports can allow traffic of multiple VLANs to pass through. VLAN in different switches can be interconnected with the Trunk ports. Ports under access mode are called Access ports. An access port can be assigned to one and only one VLAN at a time. Hybrid ports can allow traffic of multiple VLANs to pass through, receive and send the packets of multiple VLANs, used to connect switch, or user's computer. When Hybrid ports and Trunk ports receive the data, the deal way is same, but the deal way is different in sending the data. Because Hybrid ports can allow the packets of multiple VLANs to send with no tag, however, Trunk ports can only allow the packets of the default VLAN to send with no tag. The attribute of ports can not directly convert between Hybrid and Trunk, it must configure to be access at first, then configure to be Hybrid or Trunk. When the Trunk or Hybrid attribute is cancelled, the port attribute restores the default (access) attribute and belongs to vlan1.

Example: Set port 5 to trunk mode and port 8 to access mode, port 10 to hybrid mode.

```
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode trunk
Switch(Config-If-Ethernet1/0/5)#exit
Switch(config)#interface ethernet 1/0/8
Switch(Config-If-Ethernet1/0/8)#switchport mode access
Switch(Config-If-Ethernet1/0/8)#exit
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/10)#exit
```

2.15.8 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 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 e1/0/1. 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: ethernet1/0/1;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 1/0/1;3;4-7;8
```

2.15.9 switchport hybrid native vlan

Command: switchport hybrid native vlan <*vlan-id*>

no switchport hybrid native vlan

Function: Set the PVID for Hybrid port; the "**no switchport hybrid native vlan**" command restores the default setting.

Parameter: <*vlan-id*> is the PVID of Hybrid port.

Command mode: Port Mode.

Default: The default PVID of Hybrid port is 1.

Usage Guide: When an untagged frame enters a Hybrid port, it will be added a tag of the native PVID which is set by this command, and is forwarded to the native VLAN.

Example: Set the native vlan to 100 for a Hybrid port.

Switch(config)#interface ethernet 1/0/5

Switch(Config-If-Ethernet1/0/5)#switchport mode hybrid

Switch(Config-If-Ethernet1/0/5)#switchport hybrid native vlan 100

Switch(Config-If-Ethernet1/0/5)#exit

2.15.10 switchport hybrid allowed vlan

Command: switchport hybrid allowed vlan {WORD | all | add WORD | except WORD | remove WORD} {tag | untag}

no switchport hybrid allowed vlan

Function: Set hybrid port which allow the VLAN to pass with tag or untag method; the "**no switchport hybrid allowed vlan**" command restores the default setting.

Parameter: WORD: Set vlan List to allowed vlan, and the late configuration will cover the previous configuration;

all: Set all VLANs to allowed vlan;

add WORD: Add vlanList to the existent allowed vlanList;

except WORD: Set all VLANs to allowed vlan except the configured vlanList;

remove WORD: Delete the specific VLAN of vlanList from the existent allow vlanList;

tag: Join the specific VLAN with tag mode;

untag: Join the specific VLAN with untag mode.

Command mode: Port Mode.

Default: Deny all VLAN traffic to pass.

Usage Guide: The user can use this command to set the VLANs whose traffic allowed to pass through the Hybrid port, traffic of VLANs not included are prohibited. The difference between tag and untag mode by setting allowed vlan: set VLAN to untag mode, the frame sent via hybrid port without VLAN tag; set VLAN to tag mode, the frame sent via hybrid port with corresponding VLAN tag. The same VLAN can not be allowed with tag and untag mode by a Hybrid port at the same time. If configure the tag (or untag) allowed VLAN to untag (or tag) allowed VLAN, the last configuration will cover the previous.

Example: Set hybrid port allowed vlan 1, 3, 5-20 with untag mode and allow vlan 100; 300;

500-2000 with tag mode.
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/5)#switchport hybrid allowed vlan 1;3;5-20 untag
Switch(Config-If-Ethernet1/0/5)#switchport hybrid allowed vlan 100;300;500-2000 tag
Switch(Config-If-Ethernet1/0/5)#exit

2.15.11 switchport forbidden vlan

Command: switchport forbidden vlan {WORD | all | add WORD | except WORD | remove WORD}

no switchport forbidden vlan

Function: Configure the forbidden vlan for a port. Note that this command can only be used to configure on trunk or hybrid ports and the port with GVRP not enabled. No command cancels the forbidden vlanlist for a port.

Parameters: WORD, add the vlanList as forbidden vlan and cover the previous configuration

all, set all VLANs as forbidden vlan

add WORD, add vlanList to the current forbidden vlanList

except WORD, set all VLANs as forbidden vlan except vlanList

remove WORD, remove vlan specified by vlanList from current forbidden vlanList

Command Mode: Port mode

Default: Forbidden vlanList is empty

Usage Guide: Tag the corresponding position for forbidden vlanList and clear allow vlanList flags in ports. A port leaves these VLANs if it joins them statically, and it sends message to GVRP module to enable corresponding registered machine of the port to enter forbidden mode.

Example: Port quits the corresponding VLAN and the corresponding registered machine of GVRP to enter forbidden mode.

Switch(config-if-ethernet1/0/1)#switchport forbidden vlan all

2.15.12 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 1/0/8
Switch(Config-If-Ethernet1/0/8)#switchport mode access
Switch(Config-If-Ethernet1/0/8)#switchport access vlan 100
Switch(Config-If-Ethernet1/0/8)#exit

2.15.13 show vlan

Command: show vlan [brief | summary] [id <vlan-id>*]* [name <vlan-name>] [internal usage [id <*vlan-id*> / name <*vlan-name*>*]*]

Function: Display 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	Ethernet1/0/1 Ethernet1/0/2 **Ethernet1/0**/3 Ethernet1/0/4 Ethernet1/0/9 Ethernet1/0/10 **Ethernet1/0**/11 Ethernet1***/0/***12
2	***VLAN0002***	Static	ENET	Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8

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

2.15.14 private-vlan association

Command: private-vlan association <secondary-vlan-list>

no private-vlan association

Function: Set Private VLAN association; the no 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

2.15.15 private-vlan

Command: private-vlan {primary | isolated | community}

no private-vlan

Function: Configure current VLAN to Private VLAN. The no 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

2.15.16 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

2.16 GVRP

2.16.1 garp timer join

Command: garp timer join <200-500>

Function: Set the value of garp join timer, note that the value of join timer must be less than half leave timer.

Parameters: <200-500>, the value of timer in millisecond

Command Mode: Global mode

Default: 200 ms.

Usage Guide: Check whether the value satisfy the range. If so, modify the value of garp timer to the specified value, otherwise return a configuration error.

Example: Set the value of garp join timer as 200ms.
Switch(config)#garp timer join 200

2.16.2 garp timer leave

Command: garp timer leave <500-1200>
Function: Set the value of garp leave timer, note that the value of leave timer must be double of join timer and less than leaveAll timer.
Parameters: <500-1200>, the value of timer in millisecond
Command Mode: Global mode
Default: 600 ms.
Usage Guide: Check whether the value satisfy the range. If so, modify the value of garp timer to the specified value, otherwise return a configuration error.
Example: Set the value of garp leave timer as 600ms.
Switch(config)#garp timer leave 600

2.16.3 garp timer leaveAll

Command: garp timer leaveall <5000-60000>
Function: Set the value of garp leaveAll timer, note that the value of leaveAll timer must be larger than leave timer.
Parameters: <5000-60000>, the value of timer in millisecond
Command Mode: Global mode
Default: 10000 ms.
Usage Guide: Check whether the value satisfy the range. If so, modify the value of garp leaveAll timer to the specified value, otherwise return a configuration error.
Example: Set the value of garp leaveAll as 20000ms.
Switch(config)#garp timer leaveall 20000

2.16.4 gvrp (Global)

Command: gvrp
no gvrp
Function: Enable/disable GVRP funciton globally.
Parameters: None.
Command Mode: Global mode
Default: Disabled.
Usage Guide: Enable GVRP function globally and only in this way GVRP module can work normally.
Example: Enable GVRP function globally.
Switch(config)#gvrp

2.16.5 gvrp (Port)

Command: gvrp

no gvrp

Function: Enable/disable GVRP function on port. Notice: although GVRP can be enabled on port when GVRP is not enabled globally, it will not take effect until global GVRP is enabled.

Parameters: None

Command Mode: Port mode

Default: Disabled

Usage Guide: GVRP function can only be enabled on trunk and hybrid ports, and enabling GVRP will return an error on access port. After GVRP enabled on port, this port will be added to GVRP (i.e. adding corresponding state machine to GVRP of the port).

Example: Enable GVRP of port.

Switch(config-if-ethernet1/0/1)#gvrp

2.16.6 no garp timer

Command: no garp timer (join | leave | leaveall)

Function: Restore garp join | leave | leaveAll timer to the default value.

Parameters: join, join timer

leave, leave timer

leaveAll, leaveAll timer

Command Mode: Global mode

Default: 200 | 600 | 10000 milliseconds for join | leave | leaveall timer respectively.

Usage Guide: Check whether the default value satisfy the range. If so, modify the value of garp join | leave | leaveAll timer to the default value, otherwise return a configuration error.

Example: Restore garp timer to the default value.

Switch(config)#no garp timer leaveall

2.16.7 show garp timer

Command: show garp timer (join | leave | leaveall |)

Function: Show the value of each timer. Note that the value is not the remaining time to run the timer but the initial value when enabling the timer.

Parameters: join, join timer

leave, leave timer

leaveAll, leaveAll timer

Command Mode: Admin mode

Default: 200|600|10000 milliseconds for join | leave | leaveAll timer respectively.

Usage Guide: Show the corresponding value of the timer specified in the command.

Example: Show the value of all garp timers currently.

Switch#show garp timer join

Garp join timer's value is 200(ms)

2.16.8 show gvrp fsm information

Command: show gvrp fsm information interface (ethernet | port-channel) IFNAME

Function: Show the current state of all registered machines and request state machines on specified or all ports.

Parameters: ethernet, physical port

port-channel, aggregate port

IFNAME, port name

Command Mode: Admin mode

Default: MT for registered machine and VO for request state machine.

Usage Guide: Show the corresponding state of all registered machines and request state machines.

Example: Show the state of all state machines.

Switch#show gvrp fsm information interface ethernet 1/0/1

VA：Very anxious Active member，AA：Anxious Active member，QA：Quiet Active member

VP：Very anxious Passive member，AP：Anxious Passive member，QP：Quiet Passive member

VO：Very anxious Observer，AO：Anxious Observer，QO：Quiet Observer

LA：Leaving Acitve member，LO：leaving Observer

Interface ethernet 1/0/1 gvrp fsm information:

Index	VLANID	Applicant	Registrar
1	100	VO	LV
2	300	VP	IN

2.16.9 show gvrp leaveAll fsm information

Command: show gvrp leaveall fsm information interface (ethernet | port-channel) IFNAME

Function: Show the state of leaveAll state machine on specified or all ports.

Parameters: ethernet, physical port

port-channel, aggregate port

IFNAME, port name

Command Mode: Admin mode

Default: Passive.

Usage Guide: Check the state of leaveAll state machine.

Example: Show the state of leaveAll state machine on port.

Switch#show gvrp leaveall fsm information interface ethernet 1/0/1

Interface	leaveAll fsm
Ethernet1/0/1	passive

2.16.10 show gvrp leavetimer running information

Command: show gvrp leavetimer running information (vlan <1-4094> |) interface (Ethernet | port-channel |) IFNAME

Function: Show running of all leavetimer on current port.

Parameters: <1-4094>, VLAN tag
Ethernet, physical port
port-channel, aggregate port
IFNAME, port name

Command Mode: Admin mode

Default: leavetimer is disabled.

Usage Guide: Show running state and expiration time of each leave timer.

Example: Show running state and expiration time of each leave timer on current port.

```
Switch#show gvrp leavetimer running information interface ethernet 1/0/1
VLANID        running state        expired time
------------        ----------        ---------
100                   UP                  0.2 s
300                 DOWN                non
```

2.16.11 show gvrp port-member

Command: show gvrp (active|) port-member

Function: Shows all ports with GVRP enabled. “active” means the port is in active state with GVRP enabled.

Parameters: active means the port is in active state

Command Mode: Admin mode

Default: GVRP is disabled on port.

Usage Guide: Show all ports (enable GVRP) saved in GVRP.

Example: Show all ports with GVRP enabled.

```
Switch#show gvrp port member
Ports which were enabled gvrp included：
Ethernet1/0/3（T）      Ethernet1/0/4（T）
Ethernet1/0/5（T）      Ethernet1/0/6（T）
Ethernet1/0/7（T）      Ethernet1/0/8（T）
Ethernet1/0/9（T）      Ethernet1/0/10（T）
```

2.16.12 show gvrp port registerd vlan

Commmand: show gvrp port (dynamic | static |) registerd vlan interface (Ethernet | port-channel |) IFNAME

Function: Show the dynamic or static registration VLANs on current port.

Parameters: dynamic, dynamic registration
static, static registration
Ethernet, physical port
port-channel, aggregate port
IFNAME, port name

Command Mode: Admin mode

Default: No dynamic or static registration VLANs on port.

Usage Guide: Show the corresponding VLANs of the registered machines by dynamic or static registration.

Example: Show all dynamic or static registration VLANs on current port.

Switch#show gvrp port registerd vlan interface ethernet 1/0/1

Current port dynamic registerd vlan included：

Vlan10 vlan20

Vlan40 vlan60

Current port static registerd vlan included：

Vlan10 vlan30

Vlan40 vlan200

2.16.13 show gvrp timer running information

Command: show gvrp timer (join | leaveall) running information interface (ethernet | port-channel |) IFNAME

Function: Show running of all join|leaveAll timer on current port.

Parameters: join, join timer

leaveall, leaveAll timer

ethernet, physical port

port-channel, aggregate port

IFNAME, port name

Command Mode: Admin mode

Default: Join timer is disabled and leaveAll timer is enabled.

Usage Guide: Check running state of join|leaveAll timer on port.

Example: Show running state and expiration time of each timer.

Switch(config)#show gvrp timer join running information interface ethernet 1/0/1

Current port’s jointimer running state is: UP

Current port’s jointimer expired time is: 0.2 s

2.16.14 show gvrp vlan registerd port

Command: show gvrp vlan <1-4094> registerd port

Function: Show the ports with specified VLAN registered.

Parameters: <1-4094>: VLAN tag

Command Mode: Admin mode

Default: No ports with specified VLAN registered.

Usage Guide: None.

Example: Show all ports with current VLAN registered.

Switch#show gvrp vlan 100 registerd port

Ethernet1/0/3（T） Ethernet1/0/4（T）

Ethernet1/0/5（T） Ethernet1/0/6（T）

Ethernet1/0/7（T） Ethernet1/0/8（T）

Ethernet1/0/9（T） Ethernet1/0/10（T）

2.16.15 debug gvrp event

Command: debug gvrp event interface (ethernet | port-channel |) IFNAME

no debug gvrp event interface (ethernet | port-channel |) IFNAME

Function: Enable/disable GVRP event debugging including the transfer of state machine and the expiration of timer.

Parameters: ethernet, physical port

port-channel, aggregate port

IFNAME, port name

Command Mode: Admin mode

Default: GVRP event debugging is disabled.

Usage Guide: Use this command to enable GVRP event debugging.

Example: Show GVRP event debugging.

Switch(config)#debug gvrp event interface ethernet 1/0/1

%Jan 16 02:25:14 2006 GVRP EVENT: LO -> VO ， interface ethernet 1/0/1, vlan 100

%Jan 16 02:35:15 2006 GVRP EVENT: join timer expire， interface ethernet 1/0/1

2.16.16 debug gvrp packet

Command: debug gvrp packet (receive | send) interface (ethernet | port-channel |) IFNAME

no debug gvrp packet (receive | send) interface (ethernet | port-channel |) IFNAME

Function: Enable/disable GVRP packet debugging.

Parameters: receive, enabling the debugging of receiving GVRP packet

send, enabling the debugging of sending GVRP packet

ethernet, physical port

port-channel, aggregate port

IFNAME, port name

Command Mode: Admin mode

Default: GVRP packet debugging is disabled.

Usage Guide: Use this command to enable the debugging of GVRP packet.

Example: Show information of sending and receiving GVRP packet.

Switch(config)#debug gvrp packet receive interface ethernet 1/0/1

Receive packet, smac 00-21-27-aa-0f-46, dmac 01-80-C2-00-00-21,

length 90, protocol ID:1,attribute type:0x01,

Attribute Index	Length	Event	Value
1	10	joinIn	100
2	10	joinEmpty	140
3	10	leaveIn	150
4	10	leaveEmpty	180

2.17 Dot1q-tunnel

2.17.1 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 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 the global configuration TPID. it default value is 0x8100, 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. This command can not be used when vlan-translation enabled.

Example: Join port1 into VLAN3, enable dot1q-tunnel function.

Switch**(**config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/0/1
Switch(Config-Vlan3)#exit
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# dot1q-tunnel enable
Switch(Config-If-Ethernet1/0/1)# exit
Switch(config)#

2.17.2 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 port 10 of the switch to trunk port and sends data packet with a TPID of

0x9100.
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport mode trunk
Switch(Config-If-Ethernet1/0/10)#dot1q-tunnel tpid 0x9100
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#

2.17.3 show dot1q-tunnel

Command: show dot1q-tunnel
Function: Display the information of all the ports at dot1q-tunnel state.
Parameter: None.
Command Mode: Admin and 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 Ethernet1/0/1:
dot1q-tunnel is enable
Interface Ethernet1/0/3:
dot1q-tunnel is enable

2.18 Selective QinQ

2.18.1 dot1q-tunnel selective enable

Command: dot1q-tunnel selective enable
no dot1q-tunnel selective enable
Function: Specify a port to enable selective QinQ, the no command restores the default value.
Parameter: None.
Command Mode: Port mode
Default: Do not enable selective QinQ.
Usage Guide: Enable selective QinQ command should associates with hybrid mode, and it should not be used with dot1q-tunnel enable synchronously.
Example: Enable dot1q-tunnel selective enable of port1.
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#dot1q-tunnel selective enable

2.18.2 dot1q-tunnel selective s-vlan

Command: dot1q-tunnel selective s-vlan <s-vlan> c-vlan <*c-vid-list*>

no dot1q-tunnel selective s-vlan <*s-vlan*> c-vlan <*c-vid-list*>

Function: Add the mapping relation between user's VLAN ID list and SP VLAN ID for selective QinQ, the no command deletes the mapping.

Parameters: s-vlan is SP VLAN ID, c-vid-list is the range of user's VLAN ID.

Command Mode: Port mode

Default: There is no mapping relation.

Usage Guide: This command is used to configure the mapping relation for selective QinQ. If packets match the mapping relation, they will be tagged with SP vlan tag as the outer VLAN tag.

Example: Packets of VLAN 100 through VLAN 200 are tagged with the tag of VLAN 1000 as the outer VLAN tag on Ethernet1/1.

Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# dot1q-tunnel selective s-vlan 1000 c-vlan 100-200
Switch(Config-If-Ethernet1/0/1)# dot1q-tunnel selective enable
Switch(Config-If-Ethernet1/0/1)#exit
Switch(config)#

2.19 VLAN translation

2.19.1 vlan-translation

Command: vlan-translation <*old-vlan-id*> to <*new-vlan-id*> {in | out}

no vlan-translation <*old-vlan-id*> {in | out}

Function: Add VLAN translation by creating a mapping between original VLAN ID and current VLAN ID; the no form of this command deletes corresponding mapping.

Parameter: old-vlan-id is the original VLAN ID; new-vlan-id is the translated VLAN ID; in indicates ingress translation; out indicates outgress translation.

Command Mode: Port Mode.

Default: There is no VLAN translation relation.

Usage Guide: The command is for configuring the translation relation of the VLAN translation function. The data packets will be matched according to the configured translation relations, and its VLAN ID will be changed to the one in the configured item once matched, while forward the packets of the original VLAN if not match. This command cannot be used with dot1q-tunnel enable at the same time.

Example: Move the VLAN100 data entered from the port1 to VLAN2 after ingress translation.

Switch#config
Switch(config)#vlan-translation 100 to 2 in
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#vlan-translation enable
Switch(Config-If-Ethernet1/0/1)#exit
Switch(config)#

2.19.2 vlan-translation enable

Command: vlan-translation enable

no vlan-translation enable

Function: Enable VLAN translation on the port; the no command restores to the default value.

Parameter: None.

Command Mode: Port Mode.

Default: VLAN translation has not been enabled on the port by default.

Usage Guide: vlan-translation and dot1q-tunnel are mutually exclusive, it is recommended to enable vlan-translation on trunk port and manually disable port filtering.

Example: Enable VLAN translation function on port1.

Switch#config

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#vlan-translation enable

2.19.3 vlan-translation miss drop

Command: vlan-translation miss drop {in|out|both}

no vlan-translation miss drop {in|out|both}

Function: Define miss drop when translation failed; the no command reback the default value.

Parameters: in is the entrance, out is export; both is two-way.

Command Mode: Port Mode.

Default: Not miss drop when translation failed.

Usage Guide: During translate the mapping relation between original VID and present VID, if not configure related translation, the default is not packets miss. After using the command, it will miss data packets when translation failed.

Example: Set port 1 translation failed and miss packets in entrance.

Switch(Config-If-Ethernet1/0/1)#vlan-translation miss drop in

2.19.4 show vlan-translation

Command: show vlan-translation

Function: Display the information of all the ports at VLAN-translation state.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: Display the information of all the ports at VLAN-translation state.

Example: Display current VLAN translation state information.

Switch#show vlan-translation

Interface Ethernet1/0/1:
vlan-translation is enable
Interface Ethernet1/0/2:
vlan-translation is enable
Interface Ethernet1/0/3:
vlan-translation is enable

2.20 Dynamic VLAN

2.20.1 dynamic-vlan mac-vlan prefer

Command: dynamic-vlan mac-vlan prefer
Function: Set the MAC-based VLAN preferred.
Parameter: None.
Command Mode: Global Mode.
Default: MAC-based VLAN is preferred by default.
Usage Guide: Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN、IP-subnet-based VLAN、Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. After the IP-subnet-based VLAN is set to be preferred and the user wish to restore to preferring the MAC-based VLAN, please use this command.
Example: Set the MAC-based VLAN preferred.
Switch#config
Switch(config)#dynamic-vlan mac-vlan prefer

2.20.2 dynamic-vlan subnet-vlan prefer

Command: dynamic-vlan subnet-vlan prefer
Function: Set the IP-subnet-based VLAN preferred.
Parameter: None.
Command Mode: Global Mode.
Default: MAC-based VLAN is preferred by default.
Usage Guide: Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN、IP-subnet-based VLAN、Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. This command is used to set to preferring the IP-subnet-based VLAN.
Example: Set the IP-subnet-based VLAN preferred.
Switch#config

services Switch(config)#dynamic-vlan subnet-vlan prefer

2.20.3 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, mac-mask is the MAC address mask which is shown in the form of 为 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 00-03-0f-11-22-33 to VLAN 100.
Switch#config
Switch(config)#mac-vlan mac 00-03-0f-11-22-33 ff-ff-ff-ff-ff-ff vlan 100 priority 0

2.20.4 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.
Example: Set VLAN100 to MAC VLAN.
Switch#config
Switch(config)#mac-vlan vlan 100

2.20.5 protocol-vlan

Command: protocol-vlan etype <etype-id> vlan *<vlan-id>*
no protocol-vlan {etype *<etype-id>* vlan *<vlan-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: etype-id is *the* type of *the* packet protocol, with a *valid* range of *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 etype 2048 vlan 200

2.20.6 show dynamic-vlan prefer

Command: show dynamic-vlan prefer

Function: Display the preference of the dynamic VLAN.

Parameter: None.

Command Mode: Admin Mode and Configuration Mode.

Usage Guide: Display the dynamic VLAN preference.

Example: Display current dynamic VLAN preference.

Switch#show dynamic-vlan prefer

Mac Vlan/Voice Vlan

IP Subnet Vlan

Protocol Vlan

2.20.7 show mac-vlan

Command: show mac-vlan

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

Parameter: None.

Command Mode: Admin Mode and other configuration Mode.

Usage Guide: Display the configuration of MAC-based VLAN on the switch.

Example: Display the configuration of the current MAC-based VLAN.

Switch#show mac-vlan

MAC-Address	VLAN_ID	Priority
00-e0-4c-77-ab-9d	2	2

00-0a-eb-26-8d-f3 2 2

00-03-0f-11-22-33 5 5

2.20.8 show mac-vlan interface

Command: show mac-vlan interface

Function: Display the ports at MAC-based VLAN.

Parameter: None.

Command Mode: Admin Mode and other configuration Mode.

Usage Guide: Display the ports of enabling MAC-based VLAN, the character in the bracket indicate the ports mode, A means Access port, T means Trunk port, H means Hybrid port.

Example: Display the ports of enabling MAC-based VLAN currently.

Switch#show mac-vlan interface

Ethernet1/0/1(A) Ethernet1/0/2(A)

Ethernet1/0/3(A) Ethernet1/0/4(A)

Ethernet1/0/5(H) Ethernet1/0/6(T)

2.20.9 show protocol-vlan

Command: show portocol-vlan

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

Parameter: None.

Command Mode: Admin Mode and Configuration Mode

Usage Guide: Display the configuration of Protocol-based VLAN on the switch.

Example: Display the configuration of the current Protocol-based VLAN.

Switch#show protocol-vlan

Protocol_Type	VLAN_ID	Priority
etype 0x800	200	4
etype 0x860	200	4
etype 0xabc	100	5

2.20.10 show subnet-vlan

Command: show subnet-vlan

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

Parameter: None.

Command Mode: Admin Mode and other Configuration Mode.

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

Example: Display the configuration of the current IP-subnet-based VLAN.

Switch#show subnet-vlan

IP-Address Mask VLAN_ID

192.168.1.165	255.255.255.0	2
202.200.121.21	255.255.0.0	2
10.0.0.1	255.248.0.0	5

2.20.11 show subnet-vlan interface

Command: show subnet-vlan interface

Function: Display the port at IP-subnet-based VLAN.

Parameter: None.

Command Mode: Admin Mode and other Configuration Mode.

Usage Guide: Display the port of enabling IP-subnet-based VLAN, the character in the bracket indicate the ports mode, A means Access port, T means Trunk port, H means Hybrid port.

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

```
Switch#show subnet-vlan interface
Ethernet1/0/1(A)        Ethernet1/0/2(A)
Ethernet1/0/3(A)        Ethernet1/0/4(A)
Ethernet1/0/5(H)        Ethernet1/0/6(T)
```

2.20.12 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.

```
Switch#config
Switch(config)#subnet-vlan ip-address 192.168.1.1 mask 255.255.255.0 vlan 300 priority 0
```

2.20.13 switchport mac-vlan enable

Command: switchport mac-vlan enable
no switchport mac-vlan enable
Function: Enable the MAC-based VLAN function on the port; the no form of this command will disable the MAC-based VLAN function on the port.
Parameter: None.
Command Mode: Port Mode.
Default: The MAC-base VLAN function is enabled on the port by default.
Usage Guide: After adding a MAC address to specified VLAN, the MAC-based VLAN function will be globally enabled. This command can disable the MAC-based VLAN function on specified port to meet special user applications.
Example: Disable the MAC-based VLAN function on port1.
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#no switchport mac-vlan enable

2.20.14 switchport subnet-vlan enable

Command: switchport subnet-vlan enable
no switchport subnet-vlan enable
Function: Enable the IP-subnet-based VLAN on the port; the no form of this command disables the IP-subnet-based VLAN function on the port.
Parameter: None.
Command Mode: Port Mode.
Default: The IP-subnet-based VLAN is enabled on the port by default.
Usage Guide: After adding the IP subnet to specified VLAN, the IP-subnet-based VLAN function will be globally enabled. This command can disable the IP-subnet-based VLAN function on specified port to meet special user applications.
Example: Disable the IP-subnet-based VLAN function on port1.
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#no switchport subnet-vlan enable

2.21 Voice VLAN

2.21.1 show voice-vlan

Command: show voice-vlan
Function: Display the configuration status of the Voice VLAN on the switch.
Parameter: None.
Command Mode: Admin Mode and other Configuration Mode.
Usage Guide: Display Voice VLAN Configuration.

Example: Display the Current Voice VLAN Configuration.

```
Switch#show voice-vlan
Voice VLAN ID:2
Ports:ethernet1/0/1;ethernet1/0/3
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          00-03-0f-11-22-33          0x80            5
NULL            00-03-0f-11-22-33          0x0             5
```

2.21.2 switchport voice-vlan enable

Command: switchport voice-vlan enable

no switchport voice-vlan enable

Function: Enable the Voice VLAN function on the port; the “no” form of this command disables Voice VLAN function on the port.

Parameter: None.

Command Mode: Port Mode.

Default: Voice VLAN is enabled by default.

Usage Guide: When voice equipment is added to the Voice VLAN, the Voice VLAN is enabled globally by default. This command disables Voice VLAN on specified port to meet specified application of the user.

Example: Disable the Voice VLAN function on port3.

```
Switch#config
Switch(config)#interface ethernet1/0/3
switch(Config-If-Ethernet1/0/3)#no switchport voice-vlan enable
```

2.21.3 voice-vlan

xx-xx-xx-xx-xx-xx

2.21.4 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

2.22 Multi-to-One VLAN Translation

2.22.1 vlan-translation n-to-1

Command: vlan-translation n-to-1 *<WORD>* to *<new-vlan-id>*
no vlan-translation n-to-1 *<WORD>*
Function: Enable/disable Multi-to-One VLAN translation of the port.
Parameters: WORD is the original VLAN ID, its range from 1 to 4094, connect them with ';' and '-'. If there are two VLANs with different range are translated into different VLAN ID in the same port, two VLAN ranges should not be superposed.
new-vlan-id is the translated VLAN ID, its range from 1 to 4094.
Command Mode: Port mode
Default: Disable
Usage Guide: Multi-to-One VLAN translation is used to network edge to map multiple VLANs to one VLAN of backbone network. When data traffic returns from backbone network to network edge, it will restore VLAN of network edge to implement Multi-to-One VLAN translation and save VLAN resource of backbone network. Note: When using this function, the device must establish the original and the translated VLAN firstly, and enabling the downlink port of this function and the uplink port for connecting backbone network, which must be join in the original and the translated VLAN with tagged mode. This function should not be used with dot1q-tunnel and VLAN translation at the same time
Note: Multi-to-One VLAN translation should be enabled after MAC learning.

Example: On Ethernet 1/0/1, translate the data traffic from VLAN with the range between 1 to 5 into VLAN 100, and translate the data traffic (belongs to VLAN with the range between 1 to 5) out from VLAN100 into the corresponding VLAN ID, connect the uplink port of the backbone network as Ethernet 1/0/5.
Switch(config)#vlan 1-5;100
Switch(config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)# switchport mode trunk
Switch(Config-If-Ethernet1/0/1)# vlan-translation n-to-1 1-5 to 100
Switch(config)#interface ethernet 1/0/5
Switch(Config-If-Ethernet1/0/5)# switchport mode trunk

2.22.2 show vlan-translation n-to-1

Command: show vlan-translation n-to-1 [<*interface-name*>]
Function: Show the port configuration with Multi-to-One VLAN translation.

Parameter: interface-name: Specify the name of the port which will be shown. If there is no parameter, show all port configurations with this function.
Command Mode: Admin mode.
Default: There is no Multi-to-One VLAN translation information.
Usage Guide: If appointed vlan when show, it will display the n-to-1 translation of specified vlan, if not appointed vlan, it will display all n-to-1 information.
Example: Show all port configurations with Multi-to-One VLAN translation function.
Switch# show vlan-translation n-to-1
Interface Ethernet1/0/1:
vlan-translation n-to-1 enable, vlan 1-4 to 100
vlan-translation n-to-1 enable,vlan 5-8;13 to 101
Interface Ethernet1/0/2:
vlan-translation n-to-1 enable,vlan 1-4 to 100

2.23 MAC Address Table

2.23.1 mac-address-table avoid-collision

This command is not supported by switch.

2.23.2 clear collision-mac-address-table

Command：clear collision-mac-address-table
Function： Clear the hash collision mac table.
Parameter： None.
Command mode： Admin Mode.
Usage Guide： If enable the function of the hash collision mac table that issued ffp (**mac-address-table avoid-collision**), the mac cannot be cleared.
Example： Clear the hash collision mac table.
Switch#clear collision-mac-address-table

2.23.3 clear mac-address-table dynamic

Command: clear mac-address-table dynamic [address *<mac-addr>*] [vlan *<vlan-id>*] [interface [ethernet | portchannel] *<interface-name>*]
Function: Clear the dynamic address table.
Parameter: ***<mac-addr>*:** MAC address will be deleted; ***<interface-name>*** the port name for forwarding the MAC packets; ***<vlan-id>*** VLAN ID.
Command mode: Admin mode.
Usage Guide: Delete all dynamic address entries which exist in MAC address table, except application, system entries. MAC address entries can be classified according to different sources,

the types are as follows: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC is the dynamic MAC address entries learned by switch, it can be aged by switch automatically.

Example: Delete all dynamic MAC.

Switch#clear mac-address-table dynamic

2.23.4 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 from 10 to 1000000; **0** to disable aging.

Command Mode: Global Mode.

Default: Default aging-time is 300 seconds.

Usage Guide: If no destination address of the packets is same with the address entry in aging-time, the address entry will get aged. The user had better set the aging-time according to the network condition, it usually use the default value.

Example: Set the aging-time to 600 seconds.

Switch(config)#mac-address-table aging-time 600

2.23.5 mac-address-table bucket size

This command is not supported by the switch.

2.23.6 mac-address-table static | static-multicast | blackhole

Command: mac-address-table {static | blackhole} address <*mac-addr*> vlan <*vlan-id*> [interface ethernet <*interface-name*>] | [source | destination | both]

no mac-address-table {static | blackhole | dynamic} [address <*mac-addr*>] [vlan <*vlan-id*>] [interface ethernet <*interface-name*>]

Function: Add or modify static address entries and filter *address entries*. The no *command* deletes the three **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 a 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 application, system entries. MAC address entries can be classified according to the different source, the types are as follows: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC is the dynamic MAC address entries learned by switch, it can be aged by switch automatically. STATIC is the static MAC address entries (including blackhole entries) added by user. APPLICATION is the static MAC address entries added by application protocol (such as dot1x, security port…). SYSTEM is the additive static MAC address entries according to VLAN interface. When adding STATIC entries, it can cover the conflictive DYNAMIC, except APPLICATION, SYSTEM entries.

After configure the static multicast MAC by this command, the multicast MAC traffic will be forwarded to the specified port of the specified VLAN.

Example: Port 1/0/1 belongs to VLAN200, and establishes address mapping with MAC address 00-03-0f-f0-00-18.

Switch(config)#mac-address-table static address 00-03-0f-f0-00-18 vlan 200 interface ethernet 1/0/1

Configure a static multicast MAC 01-00-5e-00-00-01, the egress is ehernet 1/0/1.

Switch(config)#mac-address-table static-multicast address 01-00-5e-00-00-01 vlan 1 interface ethernet1/0/1

2.23.7 l2-address-table static-multicast address

Command: l2-address-table static-multicast address {<ip-addr> |<mac-addr**>} vlan <*vlan-id*> {interface [ethernet <*interface-name*>] | port-channel <port-channel-id>}**

no l2-address-table static-multicast address {<*ip-addr*> |<*mac-addr*>} vlan <*vlan-id*> {interface [ethernet <*interface-name*>] | port-channel <port-channel-id>}

Function: <*ip-addr*> means add or delete IP address, **<*mac-addr*>** means add or delete MAC address; **<*interface-name*>** is the port that transfer MAC data packets; **<port-channel-id>** is the aggregate port name of transfer MAC data packets, **<*vlan-id*>** is VLAN number.

Command Mode: Global Mode.

Default: When VLAN interface is configured and is up, the system will generate a 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.

After configure the static multicast MAC by this command, the multicast MAC traffic will be forwarded to the specified port of the specified VLAN.

Example: Configure a static multicast ip 232.0.0.1, the egress is ehernet 1/0/1.

Switch(config)# l2-address-table static-multicast address 232.0.0.1 vlan 200 interface ethernet

1/0/1

2.23.8 show collision-mac-address-table

Command：show collision-mac-address-table
Function： Show the hash collision mac table.
Parameter： None.
Command mode： Global Mode.
Usage Guide： If enable the function of the hash collision mac table that issued ffp (**mac-address-table avoid-collision**), the collision mac which issued ffp use * to sign.
Example： Show the hash collision mac table.
Switch(Config)#show collision-mac-address-table
The max number can be recorded is 200
The max number of collision is 0
The current number recorded is 0

MAC Address VLAN Collision-count

2.23.9 show mac-address-table

Command: show mac-address-table [static | blackhole | 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, ***<mac-addr>*** entry's MAC address; ***<vlan-id>*** entry's VLAN number; ***<interface-name>*** entry's interface name.
Command mode: Admin and Configuration Mode.
Default: MAC address table is not displayed by default.
Usage guide: This command can display various classes 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

2.23.10 Show l2-address-table multicast

Command: show l2-address-table multicast {[count]|[vlan <*vlan-id*>]}
Function: Show the current multicast table.
Parameter: *<vlan-id>* entry's VLAN number.
Command mode: Admin and Configuration Mode.
Default: MAC address table is not displayed by default.
Usage guide: This command can display various classes of multicast address entries.
Example: Display all the vlan1 multicast address entries.

services Switch#show l2-address-table multicast vlan 1

2.24 MAC Notification

2.24.1 clear mac-notification statistics

Command: clear mac-notification statistics
Function: Clear the statistics of MAC notification trap.
Parameter: None.
Default: None.
Command Mode: Admin mode
Usage Guide: When this command is used with show command, it is able to check the executive result by show command after executing this command.
Example:
Switch# clear mac-notification statistics

2.24.2 mac-address-table notification

Command: mac-address-table notification
no mac-address-table notification
Function: Enable the MAC address notification globally, the no command disables the global MAC address notification.
Parameter: None.
Default: Disable.
Command Mode: Global mode
Usage Guide: This command is used with trap switch of snmp. When disabling the MAC address notification, other configuration can be shown, but the function is invalid.
Example: Enable the MAC address notification.
Switch(Config)#mac-address-table notification

2.24.3 mac-address-table notification history-size

Command: mac-address-table notification history-size <0-500>
no mac-address-table notification history-size
Function: Configure the maximum history-size for storing MAC changing message, the no command restores the default value.
Parameter: history-size: data length of sending the notification, its range from 1 to 500.
Default: 10.
Command Mode: Global mode
Usage Guide: After the global switch is disabled, this command is also able to be configured sequentially.

Example: Change the maximum history-size to be 256.
Switch(Config)#mac-address-table notification history-size 256

2.24.4 mac-address-table notification interval

Command: mac-address-table notification interval <0-86400>
no mac-address-table notification interval
Function: Configure the interval for sending the MAC address notification, the no command restores the default interval.
Parameter: interval: interval for sending the notification, unit is second, its range from 0 to 86400.
Default: 30s.
Command Mode: Global mode
Usage Guide: After the global switch is disabled, this command is also able to be configured sequentially.
Example: Configure the interval as 30s for sending the MAC address notification.
Switch(Config)#mac-address-table notification interval 30

2.24.5 mac-notification

Command: mac-notification {added | both | removed}
no mac-notification
Function: Configure the MAC address notification for the specified port, the no command cancels the function.
Parameter: added: the added MAC address
removed: the removed MAC address
both: the added and the removed MAC addresses
Default: No MAC address notification.
Command Mode: Port mode
Usage Guide: After the global switch is disabled, this command is also able to be configured sequentially.
Example: Send the trap notification after the MAC address is added to Ethernet 1/0/5.
Switch(Config)#in ethernet 1/0/5
Switch(Config-if-ethernet 1/0/5)#mac-notification added

2.24.6 show mac-notification summary

Command: show mac-notification summary
Function: Show the configuration of MAC notification and the data of the notification packet.
Parameter: None.
Default: Do not show the summary.
Command Mode: Admin mode
Usage Guide: With this command, check the configuration of MAC address and the sending

status of MAC notification trap.

Example:

Switch#show mac-notification summary

MAC address notification:enabled

MAC address snmp traps:enabled

MAC address notification interval = 10

MAC address notification history log size = 120

MAC address added = 0

MAC address removed = 0

MAC address snmp traps generated = 0

2.24.7 snmp-server enable traps mac-notification

Command: snmp-server enable traps mac-notification

no snmp-server enable traps mac-notification

Function: Enable the trap notification of MAC address globally, the no command disables the trap notification.

Parameter: None.

Default: Disable trap notification globally.

Command Mode: Global mode

Usage Guide: This command is used with MAC notification switch. When the switch is disabled, other configuration can be shown, but the function is invalid.

Example: Enable the trap notification of MAC address.

Switch(Config)#snmp-server enable traps mac-notification

Chapter 3 Commands for IP services

3.1 Layer 3 Interface

3.1.1 Bandwidth

This command is not supported by the switch.

3.1.2 description

Command: description <*text*>

no description

Function: Configure the description information of VLAN interface. The no command will cancel the description information of VLAN interface.

Parameter: <*text*> is the description information of VLAN interface, the length should not exceed 256 characters.

Default: Do not configure.

Command Mode: VLAN interface mode

Usage Guide: The description information of VLAN interface behind description and shown under the configured VLAN.

Example: Configure the description information of VLAN interface as test vlan.

Switch(config)#interface vlan 2

Switch(config-if-vlan2)#description test vlan

3.1.3 description (VRF mode)

This command is not supported by the switch.

3.1.4 interface loopback

This command is not supported by the switch.

3.1.5 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. Configure 16 interface vlan to manage device that is supported by layer 2 switch, but layer 3 forward is not supported.

Example: Create a VLAN interface (layer 3 interface).

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#

3.1.6 ip vrf

This command is not supported by the switch.

3.1.7 ip vrf forwarding vrfName

This command is not supported by the switch.

3.1.8 no interface IFNAME

Command: no interface IFNAME

Function: Delete the interface, deal with the interface vlan and interface loopback only.

Parameters: IFNAME: interface name.

Command Mode: Global mode.

Usage Guide: This command is used to delete the layer 3 interface. It can deal with the situation that the interface name is spelt in special way. IFNAME can match multiple ways, such as vlan1, Vlan1, v1, V1 and etc.

Example: Delete interface vlan1.

(config)# no interface vlan1

3.1.9 rd

This command is not supported by the switch.

3.1.10 route-target

This command is not supported by the switch.

3.1.11 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.

3.1.12 show ip route vrf

This command is not supported by the switch.

3.1.13 show ip vrf

This command is not supported by the switch.

3.1.14 shutdown

This command is not supported by the switch.

3.2 IP Configuration

3.2.1 clear ip traffic

Command: clear ip traffic
Function: Clear the statistic information of IP protocol.
Parameter: None.
Command mode: Admin Mode.
Default: None.
Usage guide: Clear the statistic information of receiving and sending packets for IP kernel protocol, including the statistic of receiving packets, sending packets and dropping packets and the error information of receiving and sending packets for IP protocol, ICMP protocol, TCP protocol and UDP protocol.
Example: Clear statistic information of IP protocol.
Switch#clear ip traffic

3.2.2 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

3.2.3 debug ip icmp

Command: debug ip icmp
no debug ip icmp
Function: The debugging for receiving and sending ICMP packets.
Parameter: None.
Default: None.
Command mode: Admin Mode
Usage Guide: None.
Example:

Switch#debug ip icmp

IP ICMP: sent, type 8, src 0.0.0.0, dst 20.1.1.1

Display	Description
IP ICMP: sent	Send ICMP packets
type 8	Type is 8（PING request）
src 0.0.0.0	Source IPv4 address
dst 20.1.1.1	Destination IPv4 address

3.2.4 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.

Parameter: None

Default: IP packet debugging information is disabled by default.

Command mode: Admin Mode

Usage Guide: Displays statistics for IP packets received/sent, including source/destination address and bytes, etc.

Example: Enable IP packet debug.

Switch #debug ip packet

IP PACKET: sent, src 200.1.1.35, dst 224.0.0.9, size 312, proto 17, vrf 0

IP PACKET: rcvd, src 101.1.1.1, dst 224.0.0.9, size 312, proto 17, from Vlan200, vrf 0

3.2.5 debug ipv6 packet

Command: debug ipv6 packet

no debug ipv6 packet

Function: IPv6 data packets receive/send debug message.

Parameter: None

Default: None

Command Mode: Admin Mode

Usage Guide:

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

3.2.6 debug ipv6 icmp

Command: debug ipv6 icmp

no debug ipv6 icmp

Function: ICMP data packets receive/send debug message.

Parameter: None

Default: None

Command Mode: Admin Mode

Usage Guide: None

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

3.2.7 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.

Parameter: None.

Default: The debug of receiving and sending operations for all five types of IPv6 ND messages is disabled by default.

Command Mode: Admin Mode

Usage Guide: The ND protocol is an essential part of IPv6. This command can display the ND message of a specified type for troubleshooting.

Example:

Switch#debug ipv6 nd

IPv6 ND: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst <fe80::203:fff:fe01:59ba>

Displayed information	Explanation
IPv6 ND: rcvd	Receive ND data report
type <136>	ND Type
src <fe80::203:fff:fe01:2786>	Source IPv6 address
dst <fe80::203:fff:fe01:59ba>	Destination IPv6 address

3.2.8 debug ipv6 tunnel packet

This command is not supported by the switch.

3.2.9 description

This command is not supported by the switch.

3.2.10 ipv6 proxy enable

This command is not supported by the switch.

3.2.11 ip address

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

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

Function: Set IP address and net mask of switch; the "**no ip address [*<ip-address> <mask>*] [secondary]**" command deletes the IP address configuration.

Parameter: *<ip-address>* is IP address, dotted decimal notation; ***<mask>*** is subnet mask, dotted decimal notation; **[secondary]** indicates that the IP address is configured as secondary IP address.

Command Mode: VLAN interface configuration mode

Default: The system default is no IP address configuration.

Usage Guide: This command configures IP address on VLAN interface manually. If optional parameter **secondary** is not configured, then it is configured as the primary IP address of VLAN interface; if optional parameter **secondary** is configured, then that means the IP address is the secondary IP address of VLAN. One VLAN interface can only have one primary IP address and more than one secondary IP addresses. Primary IP and Secondary IP all can be used on SNMP/Web/Telnet management. Furthermore, the switch also provides BOOTP/DHCP manner to get IP address.

Example: The IP address of switch VLAN1 interface is set to 192.168.1.10/24.

Switch(Config-if-Vlan1)#ip address 192.168.1.10 255.255.255.0

3.2.12 ip default-gateway

Command: ip default-gateway <A.B.C.D>

no ip default-gateway <A.B.C.D>

Function: Configure the default gateway of the router. The no command cancels the configuration.

Parameter: <A.B.C.D> is gateway address, for example 10.1.1.10.

Command mode: Global mode.

Default: There is no default gateway.

Usage Guide: Configure the default gateway of the router to specify the default next hop address to which the packets will be sent.

Example:

Specify a default gateway:

Switch(config)# ip default-gateway 10.1.1.10

Cancel the setting of a default gateway:

Switch(config)# no ip default-gateway 10.1.1.10

3.2.13 ip route

Command: ip route {<ip-prefix> <mask> | ***<ip-prefix>/<prefix-length>*****} {<*****gateway-address*****> | <*****gateway-interface*****>} [<*****distance*****>]**

no ip route {*<ip-prefix> <mask>* | *<ip-prefix>/<prefix-length>*} [*<gateway-address>* | *<gateway-interface>*] [*<distance>*]

Function: Configure the static route. The no command deletes the static route.

Parameter: ***<ip-prefix>*** and ***<mask>*** are respectively destination IP address and subnet mask, shown in dotted decimal notation; ***<ip-prefix>*** and ***<prefix-length>*** are respectively the destination IP address and the length of prefix; ***<gateway-address>*** is the next-hop IP address shown in dotted decimal notation; ***<gateway-interface>*** is the next-hop interface; ***< distance >*** is the distance value of route management, the range is 1 to 255.

Default: The default distance value of route management is 1.

Command Mode: Global Mode.

Usage Guide: When configuring the next-hop of static route, the next-hop IP address of route packets and the manner of egress or interface can be appointed. This command can be also configured on the layer 2 switch. But the configured route is only used for switch sending packets, it will not be issued to the switch chip for the layer 3 forwarding of packets.

Example: Add a static route.

Switch(config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1

3.2.14 ipv6 address

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

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

Function: Configure aggregately global unicast address, site-local address and link-local address

for the interface.

Parameter: Parameter ***<ipv6-address>*** is the prefix of IPv6 address, parameter ***<prefix-length>*** is the prefix length of IPv6 address, which is between 3-128, **eui-64** means IPv6 address is generated automatically based on eui64 interface identifier of the interface.

Command Mode: Interface Configuration Mode.

Default: None.

Usage Guide: IPv6 address prefix can not be multicast address or any other specific IPv6 address, and different layer 3 interfaces can not configure the same address prefix. For global unicast address, the 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 10.

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

3.2.15 ipv6 default-gateway

Command: ipv6 default-gateway <X:X::X:X>

no ipv6 default-gateway <X:X::X:X>

Function: Configure IPv6 default gateway of the router. The no command cancels the configuration.

Parameter: < X:X::X:X > is IPv6 address of the gateway, for example 2002:100::1.

Default: Do not configure IPv6 default gateway of the router.

Command mode: Global mode.

Usage Guide: Configure IPv6 default gateway of the router to specify the default next hop IPv6 address to which the packets will be sent.

Example:

Specify an IPv6 default gateway:

Switch(config)# ipv6 default-gateway 2002:100::1

Cancel the setting of IPv6 default gateway:

Switch(config)# no ipv6 default-gateway 2002:100::1

3.2.16 ipv6 route

This command is not *supported by the* switch**.**

3.2.17 ipv6 redirect

This command is not supported by the switch.

3.2.18 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

3.2.19 ipv6 nd ns-interval

Command: ipv6 nd ns-interval *<seconds>*

no ipv6 nd ns-interval

Function: Set the time interval of Neighbor Solicitation Message sent by the interface.

Parameter: parameter ***<seconds>*** is the time interval of sending Neighbor Solicitation Message, ***<seconds>*** value must be between 1-3600 seconds, **no** command restores the default value 1 second.

Command Mode: Interface Configuration Mode

Default: The default Request Message time interval is 1 second.

Usage Guide: 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

3.2.20 ipv6 nd suppress-ra

This command is not supported by the switch.

3.2.21 ipv6 nd ra-lifetime

This command is not supported *by* the switch.

3.2.22 ipv6 nd min-ra-interval

This command is not supported *by* the switch.

3.2.23 ipv6 nd max-ra-interval

This command is not supported *by* the switch.

3.2.24 ipv6 nd prefix

This command is not supported by the switch.

3.2.25 ipv6 nd ra-hoplimit

This command is not supported by the switch.

3.2.26 ipv6 nd ra-mtu

This command is not supported by the switch.

3.2.27 ipv6 nd reachable-time

This command is not supported by the switch.

3.2.28 ipv6 nd retrans-timer

This command is not supported by the switch.

3.2.29 ipv6 nd other-config-flag

This command is not supported by the switch.

3.2.30 ipv6 nd managed-config-flag

This command is not supported by the switch.

3.2.31 ipv6 neighbor

Command: ipv6 neighbor *<ipv6-address>* *<hardware-address>* interface *<interface-type interface-name>*

no ipv6 neighbor *<ipv6-address>*

Function: Set static neighbor table entry.

Parameters: Parameter ***ipv6-address*** is static neighbor IPv6 address, parameter hardware-address is static neighbor hardware address***,*** interface-type is Ethernet type, interface-name ***is*** Layer 2 interface name***.***

Command Mode: Interface Configuration Mode

Default Situation: There is not static neighbor table entry.

Usage Guide: IPv6 address and multicast address for specific purpose and local address can not be set as neighbor.

Example: Set static neighbor 2001:1:2::4 on port E1/0/1, and the hardware MAC address is 00-03-0f-89-44-bc.

Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface Ethernet 1/0/1

3.2.32 interface tunnel

This command is not *supported by* the switch.

3.2.33 show ip interface

Command: show ip interface [<*ifname*> | vlan <*vlan-id*>] brief

Function: Show the brief information of the configured layer 3 interface.

Parameters: ***<ifname>*** Interface name; ***<vlan-id>*** VLAN ID.

Default: Show all brief information of the configured layer 3 interface when no parameter is specified.

Command mode: All modes.

Usage Guide: None.

Example:

Restarter#show ip interface vlan1 brief

Index	Interface	IP-Address	Protocol
3001	Vlan1	192.168.2.11	up

3.2.34 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	Statistics of total ICMP packets received and classified information

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	Statistics of total ICMP packets sent and classified information
TCP statistics:	TCP packet statistics.
UDP statistics:	UDP packet statistics.

3.2.35 show ipv6 interface

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

Function: Show interface IPv6 parameters.

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

Default: None

Command Mode: Admin 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

3.2.36 show ipv6 route

Command: show ipv6 route [database]
Function: Display IPv6 routing table.
Parameter: database is router database.
Default Situation: None.
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

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 2003:1::/64 via ::, Vlan4 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 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.

3.2.37 show ipv6 neighbors

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

Function: Display neighbor table entry information.

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

Default Situation: None

Command Mode: Admin and Configuration Mode

Usage Guide:

Example:

Switch#show ipv6 neighbors
IPv6 neighbour unicast items: 14, valid: 11, matched: 11, incomplete: 0, delayed: 0,
manage items 5
IPv6 Address Hardware Addr Interface Port

```
State
2002:ca60:c801:1:250:baff:fef2:a4f4    00-50-ba-f2-a4-f4    Vlan1    Ethernet1/0/2
reachable
3ffe:3240:800d:1::100                  00-03-0f-01-27-86    Vlan1
Ethernet1/0/3       reachable
3ffe:3240:800d:1::8888                 00-02-01-00-00-00    Vlan1
Ethernet1/0/1       permanent
3ffe:3240:800d:1:250:baff:fef2:a4f4    00-50-ba-f2-a4-f4    Vlan1    Ethernet1/0/4
reachable
3ffe:3240:800d:2::8888                 00-02-01-00-01-01    Vlan2
Ethernet1/0/16      permanent
3ffe:3240:800d:2:203:fff:fefe:3045     00-03-0f-fe-30-45    Vlan2    Ethernet1/0/15
reachable
fe80::203:fff:fe01:2786                00-03-0f-01-27-86    Vlan1
Ethernet1/0/5       reachable
fe80::203:fff:fefe:3045                00-03-0f-fe-30-45    Vlan2
Ethernet1/0/17      reachable
fe80::20c:ceff:fe13:eac1               00-0c-ce-13-ea-c1    Vlan12
Ethernet1/0/20      reachable
fe80::250:baff:fef2:a4f4               00-50-ba-f2-a4-f4    Vlan1    Ethernet1/0/6
reachable

IPv6 neighbour table: 11 entries
```

Displayed information	Explanation
IPv6 Addres	Neighbor IPv6 address
Hardware Addr	Neighbor MAC address
Interface	Exit interface name
Port	Exit interface name
State	Neighbor status (reachable、statle、delay、probe、permanent、incomplete、unknow)

3.2.38 show ipv6 traffic

Command: show ipv6 traffic

Function: Display IPv6 transmission data packets statistics information.

Parameter: None

Default: None

Command Mode: Admin and Configuration 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

3.2.39 show ipv6 redirect

This command is not supported by the switch.

3.2.40 show ipv6 tunnel

This command is not supported by *the* switch.

3.2.41 tunnel source

This command is not supported by the switch.

3.2.42 tunnel destination

This command is *not supported by the* switch.

3.2.43 tunnel nexthop

This command is not *supported* by the switch.

3.2.44 tunnel 6to4-relay

This command is not supported by the switch.

3.2.45 tunnel mode

This command is not supported by the switch.

3.3 ARP

3.3.1 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 field 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 00-03-0f-f0-12-34 interface eth 1/0/2

3.3.2 clear arp-cache

Command: clear arp-cache

Function: Clears ARP table.

Command mode: Admin Mode

Example:

Switch#clear arp-cache

3.3.3 clear arp traffic

Command: clear arp traffic

Function: Clear the statistic information of ARP messages of the switch. For box switches, this command will only clear statistics of APP messages received and sent from the current boardcard.

Command mode: Admin Mode

Example:

Switch#clear arp traffic

3.3.4 debug arp

Command: debug arp {receive|send|state}

no debug arp {receive|send|state}

Function: Enables the ARP debugging function; the "**no debug arp {receive|send|state}**" command disables this debugging function.

Parameter: receive the debugging-switch of receiving ARP packets of the switch; **send** the debugging-switch of sending ARP packets of the switch; **state** the debugging-switch of APR state changing of the switch.

Default: ARP debug is disabled by default.

Command mode: Admin Mode.

Usage Guide: Display contents for ARP packets received/sent, including type, source and destination address, etc.

Example: Enable 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.

3.3.5 clear ip arp dynamic

Command: clear ip arp dynamic

Function: Clear all of dynamic ARP on interface.

Parameter: None

Command Mode: Interface Configuration

Usage Guide: This command will clear dynamic entries before binding ARP. Once implemented, this command will lose its effect.

Example:

Switch(Config-if-Vlan1)#clear ip arp dynamic

3.3.6 clear ipv6 nd dynamic

Command: clear ipv6 nd dynamic
Function: Clear all dynamic ND on interface.
Parameter: None
Command mode: Interface Configuration
Usage Guide: This command will clear dynamic entries before binding ND. Once implemented, this command will lose its effect.
Example:
Switch(Config-if-Vlan1)#clear ipv6 nd dynamic

3.3.7 ip proxy-arp

This command is not supported by the switch.

3.3.8 l3 hashselect

This command is not supported by the switch.

3.3.9 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	Ethernet1/0/11	Dynamic
50.1.1.9	00-00-00-00-00-09	Vlan50	Ethernet1/0/1	Static
150.1.1.2	00-00-58-fc-48-9f	Vlan150	Ethernet1/0/4	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.

3.3.10 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

3.4 ARP Scanning Prevention

3.4.1 anti-arpscan enable [ip|port]

Command: anti-arpscan enable [ip|port]

no anti-arpscan enable [ip|port]

Function: Globally enable ARP scanning prevention function; "**no anti-arpscan enable**" command globally disables ARP scanning prevention function.

Parameters: None.

Default Settings: Enable or disable ARP scanning prevention function based on ip or port in the same time.

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 ip

3.4.2 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

3.4.3 anti-arpscan ip-based level1|level2 threshold

Command: anti-arpscan ip-based level1|level2 threshold <threshold-value>

no anti-arpscan ip-based level1|level2 threshold

Function: Set the level-1 or level-2 threshold of received messages of the IP-based ARP scanning prevention. By default the level-1 threshold is 4p/s, the level-2 threshold is 8p/s. The level-2 threshold must be high than the level-1 threshold.

Parameters: rate threshold, ranging from 1 to 200.

Default Settings: By default the level-1 threshold is 4p/s, the level-2 threshold is 8p/s.

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 level1 threshold 6

3.4.4 anti-arpscan trust

Command: anti-arpscan trust { port | supertrust-port | iptrust-port }

no anti-arpscan trust {port | supertrust-port | iptrust-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 trusted 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. If a port is set as a trusted IP port, then the IP will not be dealt with, but the port will be dealt with. If the IP is already closed by ARP scanning prevention, it will be opened right after being set as a trusted IP 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 1/0/5 of the switch as a trusted port.

Switch(config)#in e1/0/5

Switch(Config-If-Ethernet1/0/5)# anti-arpscan trust port

3.4.5 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

3.4.6 anti-arpscan recovery enable

Command: anti-arpscan recovery enable

no anti-arpscan recovery enable

Function: Enable the automatic recovery function, “**no anti-arpscan recovery enable**” command will disable the function.

Parameters: None

Default Settings: Disable 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, they can configure this function.

Example: Enable the automatic recovery function of the switch.

Switch(config)#anti-arpscan recovery enable

3.4.7 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

3.4.8 anti-arpscan log enable

Command: anti-arpscan log enable

no anti-arpscan log enable

Function: Enable ARP scanning prevention log function; "**no anti-arpscan log enable**" command will disable this function.

Parameters: None.

Default Settings: Disable 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

3.4.9 anti-arpscan trap enable [level1|level2]

Command: anti-arpscan trap enable [level1|level2]

no anti-arpscan trap enable [level1|level2]

Function: Enable ARP scanning prevention SNMP Trap function; "**no anti-arpscan trap enable [level1|level2]**" command disable ARP scanning prevention SNMP Trap function.

Parameters: None.

Default Settings: By default disable or enable level-1 limited speed or level-2 insulate 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 level1

3.4.10 anti-arpscan ip-based level2 action {isolate | discard-ARP}

Command: anti-arpscan ip-based level2 action {isolate | discard-ARP}

Function: After above level-2 threshold, users can configure ip business isolation and discard ARP packets.

Parameters: isolate—the ip business is isolated, discard-ARP --- Discard APR packets from the ip and keep original ARP item. The default is discard-ARP.

Command Mode: Global configuration mode

User Guide: After above level-2 threshold, the protect action is configure diacard-arp. Discard ARP packets of the ip and ip data transfer normally when port received a ARP packets whose rate above level-2 threshold and the source is a ip. Configure protect action is isloate when above level-2 threshold, discard ARP packets and ip date when port received a ARP packets whose rate above level-2 threshold and the source is a ip.

Example: Switch(config)#anti-arpscan ip-based level2 action isolate

3.4.11 anti-arpscan FFP max-num <num>

Command: anti-arpscan FFP max-num <num>

Function: The maximum quantity of ARP scanning prevention function occupied FFP item.

Parameters: <1-1024>, the default is 200 available resources.

Command Mode: Global configuration mode

User Guide: When port received a arp packets whose source above max-num and arp rate of every source ip above level-1 or level-2 threshold, users can set a higher value for ffp item after ffp resource exhausted.

Example: Switch(config)#anti-arpscan ffp max-num 1024

3.4.12 anti-arpscan ip-based arp-to-cpu speed<pps>

Command: anti-arpscan ip-based arp-to-cpu speed<pps>

no anti-arpscan ip-based arp-to-cpu speed

Function: Configure the rate of ARP send to CPU when level-1 threshold overrun.

Parameters: <1-20>, the default is 1p/s.

Command Mode: Global configuration mode

User Guide: Used for configuring the rate of cpu in arp packets after arp rate above level-1 limited rate, it can be modified on spot.

Example: Switch(config)#anti-arpscan ip-based arp-to-cpu speed 2

3.4.13 clear anti-arpscan attack-list {ip <IP Address>| all}

Command: clear anti-arpscan attack-list {ip <IP Address> | all}

Function: Clear the ARP limit for the specific host or all the hosts manually.

Parameters: <*IP Address*>: the IP address of the specific host.

Command Mode: Admin Mode.

Usage Guide: When the speed of arp packet exceeds the limit value of first or second level, use this command to clear the table and use the command of debug anti-arpscan ip to view the deleted table.

Example: Switch#clear anti-arpscan attack-list ip 30.1.1.6

3.4.14 clear anti-arpscan attack-history-list {ip <IP Address>| all}

Command: clear anti-arpscan attack-history-list {ip <IP Address> | all}

Function: Clear the history attacks source information of the specific host or all hosts manually.

Parameters: <*IP Address*>: the IP address of the specific host.

Command Mode: Admin Mode.

Usage Guide: Use this command to clear the history attacks information of the specific host or all hosts manually. And use the command of show anti-arpscan ip-based attack-list history to view the deleted table.

Example: Switch#clear anti-arpscan attack-history-list ip 30.1.1.6

3.4.15 clear anti-arpscan speed-limit< IP Address>

Command: clear anti-arpscan speed-limit< IP Address>

Function: Flush ARP limited rate for specified host manually.

Parameters: Ip address of specified host.

Command Mode: Admin Mode.

User Guide: Use the command to clear items when arp packets above level-1 limited rate. Users can use debug command debug anti-arpscan ip to show deleted items.

Example: Switch#clear anti-arpscan speed-limit 30.1.1.6

3.4.16 clear anti-arpscan ip-isolate<IP Address>

Command: clear anti-arpscan ip-isolate<IP Address>

Function: Flush IP business isolation for specified host manually.

Parameters: IP address of specified host.

Command Mode: Admin Mode.

User Guide: Use the command to clear items when arp packets above level-2 limited rate. Users can use debug command debug anti-arpscan ip to show deleted items.

Example: Switch#clear anti-arpscan ip-isolate 30.1.1.6

3.4.17 debug anti-arpscan

Command: debug anti-arpscan [port | ip]

no debug anti-arpscan [port | ip]

Function: Enable the debug switch of ARP scanning prevention; "**no debug anti-arpscan [port | ip]**" command disables the switch.

Parameters: None.

Default Settings: Disable the debug switch of ARP scanning prevention

Command Mode: Admin Mode

User Guide: After enabling debug switch of ARP scanning prevention users can check corresponding debug information or enable the port-based or IP-based debug switch separately whenever a port is closed by ARP scanning prevention or recovered automatically, and whenever IP t is closed or recovered .

Example: Enable the debug function for ARP scanning prevention of the switch.

Switch#debug anti-arpscan

3.4.18 show anti-arpscan

Command: show anti-arpscan [trust {ip | port | supertrust-port | iptrust-port} |prohibited {ip | port}]

Function: Display the operation information of ARP scanning prevention function.

Parameters: None.

Default Settings: Display every port to tell whether it is a trusted port and whether it is closed. If the port is closed, then display how long it has been closed. Display all the trusted IP and disabled IP.

Command Mode: Admin Mode

User Guide: Use "**show anti-arpscan trust port**" if users only want to check trusted ports. The reset follow the same rule.

Example: Check the operating state of ARP scanning prevention function after enabling it.

Switch(config)#show anti-arpscan

Total port: 28

Name	Port-property	beShut	shutTime(seconds)
Ethernet1/0/1	untrust	N	0
Ethernet1/0/2	untrust	N	0
Ethernet1/0/3	untrust	N	0
Ethernet1/0/4	untrust	N	0

```
Ethernet1/0/5       untrust        N        0
Ethernet1/0/6       untrust        N        0
Ethernet1/0/7       untrust        N        0
Ethernet1/0/8       untrust        N        0
Ethernet1/0/9       untrust        N        0
Ethernet1/0/10      untrust        N        0
Ethernet1/0/11      untrust        N        0
Ethernet1/0/12      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
```

3.4.19 show anti-arpscan ip-based attack-list [history]

Command: show anti-arpscan ip-based attack-list [history]

Function: Display source information or history source information of ARP scanning attacks prevention.

Parameters: None.

Default: Display the source information of ARP scanning attacks prevention.

Command Mode: Admin Mode, Config Mode.

User Guide: (1) Display ARP scanning attacks prevention source information which includes source ip, corresponding port, vlan, rate and state. When it aboves level-1 threshold, state is Speed-Limit; if above level-2, action is discard-arp and state is Discard-Arp, but state is Isolate when action is isolate.

(2) Display the history source information of ARP scanning attacks prevention, including source IP, port, vlan, times of attacks, state of last attack and internal if attacking. When it aboves level-1 threshold, state is Speed-Limit; if above level-2, action is discard-arp and state is Discard-Arp, but state is Isolate when action is isolate.

Example:

```
Switch#show anti-arpscan ip-based attack-list
SIP-Addr                Port                VLAN    Speed    ARP-Count    State
30.1.1.6                Ethernet2/48        26       4        57
Speed-Limit
30.1.1.4                Ethernet2/48        26       4        56
Speed-Limit
Switch#show anti-arpscan ip-based attack-list history
SIP-Addr                Port                VLAN    Attack-Times    State
Keep-Time
30.1.1.6                Ethernet2/48        26       6              Speed-Limit
0 weeks,0 days,0 hours,8 minutes,46 seconds
30.1.1.4                Ethernet2/48        26       3              Speed-Limit
0 weeks,0 days,0 hours,0 minutes,28 seconds
```

3.4.20 show anti-arpscan ip-based running-config

Command: show anti-arpscan ip-based running-config

Function: Display the current configuration of arp scanning prevention.

Parameters: None.

Command Mode: Admin Mode, Config Mode.

User Guide: Display the current configuration of arp scanning prevention, the action after level-1 threshold and level-2 threshold above level-2 threshold, cpu rate and the size of ffp items and so on after arp above level-1 threshold.

Example:

```
Switch(config)#show anti-arpscan ip-based running-config
level1 thrshould:     4
level2 thrshould:     8
level2 action:        Discard-Arp
```

arp-to-cpu speed: 2
actIp-num: 0
ffp-max: 1024
ffp-used: 0

3.5 Preventing ARP Spoofing

3.5.1 ip arp-security updateprotect

Command: ip arp-security updateprotect
no ip arp-security updateprotect
Function: Forbid ARP table automatic update. The "**no ip arp-security updateprotect**" command re-enables ARP table automatic update.
Parameter: None.
Default: ARP table automatic update.
Command Mode: Global Mode/ Interface configuration.
User Guide: Forbid ARP table automatic update, the ARP packets conflicting with current ARP item (e.g. with same IP but different MAC or port) will be dropped, the others will be received to update aging timer or create a new item; so, the current ARP item keep unchanged and the new item can still be learned.
Example:
Switch(Config-if-Vlan1)#ip arp-security updateprotect.
Switch(config)#ip arp-security updateprotect

3.5.2 ip arp-security learnprotect

Command: ip arp-security learnprotect
no ip arp-security learnprotect
Function: Forbid ARP learning function of IPv4 Version, the "**no ip arp-security learnprotect**" command re-enables ARP learning function.
Parameter: None.
Default: ARP learning enabled.
Command Mode: Global Mode/ Interface Configuration.
Usage Guide: This command is for preventing the automatic learning and updating of ARP. Unlike ip arp-security updateprotect, once this command implemented, there will still be timeout even if the switch keeps sending Request/Reply messages.
Example:
Switch(Config-if-Vlan1)# ip arp-security learnprotect
Switch(config)# ip arp-security learnprotect

3.5.3 ip arp-security convert

Command: ip arp-security convert

Function: Change all of dynamic ARP to static ARP.

Parameter: None

Command Mode: Global Mode/ Interface configuration

Usage Guide: This command will convert the dynamic ARP entries to static ones, which, in combination with disabling automatic learning, can prevent ARP binding. Once implemented, this command will lose its effect.

Example:

Switch(Config-if-Vlan1)#ip arp -security convert

Switch(config)#ip arp -security convert

3.6 ARP GUARD

3.6.1 arp-guard ip

Command: arp-guard ip <addr>

no arp-guard ip <addr>

Function: Add an 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 ethernet1/0/1 as 100.1.1.1.

switch(config)#interface ethernet1/0/1

switch(Config-If-Ethernet 1/0/1)#arp-guard ip 100.1.1.1

Delete the ARP GUARD address on port ethernet1/0/1 as 100.1.1.1.

switch(config)#interface ethernet1/0/1

switch(Config-If-Ethernet 1/0/1)#no arp-guard ip 100.1.1.1

3.7 Gratuitous ARP

3.7.1 ip gratuitous-arp

Command: ip gratuitous-arp [<*interval-time*>]

no ip gratuitous-arp

Function: To enabled gratuitous ARP, and specify update interval for gratuitous ARP. The no form of this command will disable the gratuitous ARP configuration.

Parameters: ***<interval-time>*** is the update interval for gratuitous ARP with its value limited between 5 and 1200 seconds and with default value as 300 seconds.

Command Mode: Global Configuration Mode and Interface Configuration Mode.

Default: Gratuitous ARP is disabled by default.

Usage Guide: When configuring gratuitous ARP in global configuration mode, all the Layer 3 interfaces in the switch will be enabled to send gratuitous ARP request. If gratuitous ARP is configured in interface configuration mode, then only the specified interface is able to send gratuitous ARP requests. When configuring the gratuitous ARP, the update interval configuration from interface configuration mode has higher preference than that from the global configuration mode.

Example:

1) To enable gratuitous ARP in global configuration mode, and set the update interval to be 400 seconds.

```
Switch>enable
Switch#config
Switch(config)#ip gratuitous-arp 400
```

2) To enable gratuitous ARP for interface VLAN 10 and set the update interval to be 350 seconds.

```
Switch(config)#interface vlan 10
Switch(Config-if-Vlan10)#ip gratuitous-arp 350
```

3.7.2 show ip gratuitous-arp

Command: show ip gratuitous-arp [interface vlan <*vlan-id*>]

Function: To display configuration information about gratuitous ARP.

Parameters: ***<vlan-id>*** is the VLAN ID. The valid range for <*vlan-id*> is between 1 and 4094.

Command Mode: All the Configuration Modes.

Usage Guide: In all the configuration modes, the command **show ip gratuitous arp** will display information about the gratuitous ARP configuration in global and interface configuration mode. The command **show ip gratuitous-arp interface vlan *<vlan-id>*** will display information about the gratuitous ARP configuration about the specified VLAN interface.

Example:

1) To display information about gratuitous ARP configuration in both global and interface

configuration modes.

Switch#show ip gratuitous-arp

Gratuitous ARP send is Global enabled, Interval-Time is 300(s)

Gratuitous ARP send enabled interface vlan information:

Name	Interval-Time(seconds)
Vlan1	400
Vlan10	350

2) To display gratuitous ARP configuration information about interface VLAN 10.

Switch#show ip gratuitous-arp interface vlan 10

Gratuitous ARP send interface Vlan10 information:

Name	Interval-Time(seconds)
Vlan10	350

3.8 Dynamic ARP Inspection

3.8.1 ip arp inspection

Command: ip arp inspection vlan <vlan-id>

no ip arp inspection vlan <vlan-id>

Function: Enable the dynamic ARP inspection function based on vlan.

Parameters: <vlan-id> is the vlan which is enabled the dynamic ARP inspection function.

Command Mode: Global Mode.

Default: Disable.

Usage Guide: After configured the dynamic ARP inspection function in global mode, the administrator can intercept, record and drop the ARP data packets which have the invalid MAC address/IP address, This command is generally used in combination with ip dhcp snooping.

Example: Enable the dynamic ARP inspection function of vlan10.

Switch(config)#

Switch(config)#ip arp inspection vlan 10

Switch(config)#exit

3.8.2 ip arp inspection trust

Command: ip arp inspection trust

no ip arp inspection trust

Function: Configure the port as the trusted port of the dynamic ARP inspection.

Parameters: None.

Command Mode: Port Mode.

Default: All the ports are the untrusted ports as default.

Usage Guide: After configured this command under the port mode, the configured port will not inspect the received ARP packet and it will forward it directly. If the ARP data packet is received from the untrusted port, the switch will only forward the lawful data packet. For the illegal data, it will drop the data directly and record this action, This command is generally used in combination with ip dhcp snooping.

Example: Configure the port 1/0/1 as the trusted port.

Switch(config)#

Switch(config)#in e 1/0/1

Switch(config-if-ethernet1/0/1)#ip arp inspection trust

Switch(config-if-ethernet1/0/1)#exit

3.8.3 ip arp inspection limit-rate

Command: ip arp inspection limit-rate <rate>

no ip arp inspection limit-rate

Function: Limit the ARP packet rate of the untrusted port.

Parameters: <rate> is the configured limited rate of the ARP packet of the untrusted port, the unit is pps.

Command Mode: Port Mode.

Default: Do not limit the rate for the ARP packets of the trusted or untrusted ports.

Usage Guide: This command can limit the ARP packet rate of the untrusted port. The rate of the lawful ARP data packets forwarding is in the limited range, This command is generally used in combination with ip dhcp snooping.

Example: Configure the rate of the ARP packet of the untrusted port 1/0/1 as 100pps.

Switch(config)#

Switch(config)#in e 1/0/1

Switch(config-if-ethernet1/0/1)# ip arp inspection limit-rate 100

Switch(config-if-ethernet1/0/1)#exit

3.9 DHCP

3.9.1 DHCP Server

3.9.1.1 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

3.9.1.2 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

3.9.1.3 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

3.9.1.4 clear ip dhcp server statistics

Command: clear ip dhcp server statistics

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

Parameters: None

Command mode: Admin Mode.

Usage Guide: DHCP count statistics can be viewed with "**show ip dhcp server statistics**" command, all information is accumulated. You can use the "**clear ip dhcp server statistics**" command to clear the count for easier statistics checking.

Example: Clearing the count for DHCP server.

Switch#clear ip dhcp server statistics

Related Command: show ip dhcp server statistics

3.9.1.5 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

3.9.1.6 debug ip dhcp client

Command: debug ip dhcp client {event | packet}

no debug ip dhcp server {event | packet}

Function: Enable the debugging of DHCP client, no command disables the debugging of DHCP client.

Command mode: Admin Mode

Default: Disable the debugging.

3.9.1.7 debug ip dhcp relay

Command: debug ip dhcp server packet

no debug ip dhcp server packet

Function: Enable the debugging of DHCP relay, no command disables the debugging of DHCP relay.

Command mode: Admin Mode

Default: Disable the debugging.

3.9.1.8 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.

3.9.1.9 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

3.9.1.10 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

3.9.1.11 domain-name

Command: domain-name *<domain>*

no domain-name

Function: Configures the Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.

Parameters: *<domain>* is the domain name, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Default: None

Usage Guide: Specifies a domain name for the client.

Example: Specifying 'switch.com.cn' as the DHCP clients' domain name.

Switch(dhcp-1-config)#domain_x001F_-name switch.com.cn

3.9.1.12 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

3.9.1.13 host

Command: host <*address*> [<*mask*> | <*prefix-length*>]

no host

Function: Specifies the IP address to be assigned to the user when binding addresses manually; the "**no host**" command deletes the IP address.

Parameters: ***<address>*** is the IP address in decimal format; ***<mask>*** is the subnet mask in decimal format; ***<prefix-length>*** means mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30".

Command Mode: DHCP Address Pool Mode

Default: None

Usage Guide: If no mask or prefix is configured when configuring the IP address, and no information in the IP address pool indicates anything about the mask, the system will assign a mask automatically according to the IP address class.

This command is used with "hardware address" command or "client identifier" command when binding addresses manually. If the identifier or hardware address of the requesting client matches the specified identifier or hardware address, the DHCP server assigns the IP address defined in "host" command to the client.

Example: Specifying IP address 10.1.128.160 to be bound to user with hardware address 00-10-5a-60-af-12 in manual address binding.

Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

Related command: hardware-address, client-identifier

3.9.1.14 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

3.9.1.15 ip dhcp disable

Command: ip dhcp disbale

no ip dhcp disable

Function: The port disables DHCP services, the no command enables DHCP services.

Parameter: None.

Default: Enable.

Command Mode: Port mode.

Usage Guide: After the port disables DHCP services, directly drop all DHCP packets sent by the port.

Example: The port disables DHCP services.

switch(config-if-ethernet1/0/3)#ip dhcp disable

3.9.1.16 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

3.9.1.17 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)#

3.9.1.18 ip dhcp conflict ping-detection enable

Command: ip dhcp conflict ping-detection enable

no ip dhcp conflict ping-detection enable

Function: Enable Ping-detection of conflict on DHCP server; the no operation of this command will disable the function.

Parameters: None.

Default Settings: By default, Ping-detection of conflict is disabled.

Command Mode: Global Configuration Mode.

Usage Guide: To enable Ping-detection of conflict, one should enable the log of conflict addresses, when which is disabled, so will the ping-detection of conflict. When a client is unable to receive Ping request messages (when blocked by firewall, for example), this function will check local ARP according to allocated IP: if a designated IP has a corresponding ARP, then an address conflict exists; otherwise, allocate it to the client.

Examples: Enable Ping-detection of conflict.

Switch(config)#ip dhcp conflict ping-detection enable

Related Command: ip dhcp conflict logging, ip dhcp ping packets, ip dhcp ping timeout

3.9.1.19 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

3.9.1.20 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 ping time out 600

Related Command: ip dhcp conflict ping-detection enable, ip dhcp ping packets

3.9.1.21 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. If the user uses the lease command to allocate a lease time that exceeds the default of 1 day, they need to use the masx-lease-time command to modify the maximum lease time at the same time.

Example: Setting the lease of DHCP pool "1" to 3 days 12 hours and 30 minutes.

Switch(dhcp-1-config)#lease 3 12 30

3.9.1.22 max-lease-time

Command: max-lease-time {[*<days>*] [*<hours>*] [*<minutes>*] | infinite}

no max-lease-time

Function: Set the maximum lease time for the addresses in the address pool; the no 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 time is 1 day.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used to DHCP request packets with option51. If the lease time (user requests the address) exceeds the maximum lease time configured, the lease that DHCP server assigns the address is the maximum lease time configured. If the lease time requested by the user is less than the maximum lease time configured, the lease that DHCP server assigns the address is the lease time requested by the user. The maximum lease time is able to be set by the administrator according to the actual network condition, and the maximum lease time is 1 day by default.

Example: Set the maximum lease time of DHCP address pool1 to 3 days 12 hours and 30 minutes.

Switch(dhcp-1-config)#max-lease-time 3 12 30

3.9.1.23 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

3.9.1.24 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

3.9.1.25 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

3.9.1.26 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

3.9.1.27 option

Command: option *<code>* {ascii *<string>* | hex *<hex>* | ipaddress *<ipaddress>*}
no option *<code>*
Function: Sets the network parameter specified by the option code; the "**no option *<code>***" command cancels the setting for option.
Parameters: ***<code>*** is the code for network parameters; ***<string>*** is the ASCII string up to 255 characters; ***<hex>*** is a value in Hex that is no greater than 510 and must be of even length; ***<ipaddress>*** is the IP address in decimal format, up to 63 IP addresses can be configured.
Command Mode: DHCP Address Pool Mode
Default: None
Usage Guide: The switch provides common commands for network parameter configuration as well as various commands useful in network configuration to meet different user needs. The definition of option code is described in detail in RFC2123.
Example: Setting the WWW server address as 10.1.128.240.
Switch(dhcp-1-config)#option 72 ip 10.1.128.240

3.9.1.28 service dhcp

Command: service dhcp
no service dhcp
Function: Enables DHCP server; the "**no service dhcp**" command disables the DHCP service.
Parameters: None
Default: DHCP service is disabled by default.
Command mode: Global Mode
Usage Guide: Both DHCP server and DHCP relay are included in the DHCP service. When DHCP

services are enabled, both DHCP server and DHCP relay are enabled. Switch can only assign IP address for the DHCP clients and enable DHCP relay when DHCP server function is enabled.

Example: Enabling DHCP server.

Switch(config)#service dhcp

3.9.1.29 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.

3.9.1.30 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.

3.9.1.31 show ip dhcp relay information option

Command: show ip dhcp relay information option

Function: Show the relative configuration for DHCP relay option82.

Parameters: None.

Command mode: Admin and configuration mode

Default: None.

Usage guide: None.

Example: Set the admin mode timeout value to 6 minutes.

Switch#show ip dhcp relay information option

ip dhcp server relay information option(i.e. option 82) is enabled

ip dhcp relay information option(i.e. option 82) is enabled

3.9.1.32 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

3.9.2 DHCP Relay

3.9.2.1 ip dhcp broadcast suppress

Command: ip dhcp broadcast suppress

no ip dhcp broadcast suppress

Function: Enable DHCP broadcast suppress function, the no command disables the function.

Parameter: None.

Default: Disable.

Command Mode: Global mode

Usage Guide: Suppress the forwarding about DHCP broadcast packets, namely, drop or copy DHCP broadcast packets to CPU.

Example: Enable DHCP broadcast suppress function.

Switch(config)#ip dhcp broadcast suppress

3.9.2.2 ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>

Command: ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>

no ip dhcp relay share-vlan

Function: Specify sub-vlan of a share-vlan, the no command cancels sub-vlan.

Parameter: ***<vlanid>*** is VLAN ID of share-vlan, ***<vlanlist>*** is sub-vlan list.

Default: None.

Command Mode: Global mode.

Usage Guide: share-vlan may include many sub-vlan, but a sub-vlan only corresponds to a share-vlan. When layer 2 device of DHCP Relay receive DHCP Request, firstly judge whether VLAN with layer 3 interface for receiving package. If there is layer 3 interface in package, use the interface to process DHCP Relay, or else use layer 3 interface of share-vlan to process DHCP Relay when the vlan is sub-vlan of share-vlan.

3.9.2.3 ip forward-protocol udp bootps

Command: ip forward-protocol udp bootps

no ip forward-protocol udp bootps

Function: Sets DHCP relay to forward UPD broadcast packets on the port; the "**no ip forward-protocol udp bootps**" command cancels the service.

Parameter: bootps forwarding UDP port as 67 DHCP broadcast packets.

Default: Not forward UPD broadcast packets by default.

Command mode: Global Mode

Usage Guide: The forwarding destination address is set in the "**ip helper-address**" command and described later.

Example: Setting DHCP packets to be forwarded to 192.168.1.5.

Switch(config)#ip forward-protocol udp boots

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#ip helper-address 192.168.1.5

3.9.2.4 ip helper-address

Command: ip helper-address *<ip-address>*

no ip helper-address *<ip-address>*

Function: Specifies the destination address for the DHCP relay to forward UDP packets. The "**no ip helper-address *<ip-address>***" command cancels the setting.

Default: None.

Command mode: Interface Configuration Mode

Usage Guide: The DHCP relay forwarding server address corresponds to the port forwarding UDP, i.e. DHCP relay forwards corresponding UDP packets only to the corresponding server instead of all UDP packets to all servers. When this command is run after "**ip forward-protocol udp *<port>***" command, the forwarding address configured by this command receives the UDP packets from ***<port>***. The combination of "**ip forward-protocol udp *<port>***" command and this command should be used for configuration.

3.9.2.5 show ip forward-protocol

Command: show ip forward-protocol

Function: Show the configured port ID of the protocol which support the forwarding of broadcast packets, it means the port ID for forwarding DHCP packets.

Command mode: Admin and configuration mode

Example:

Switch#show ip forward-protocol

Forward protocol(UDP port): 67(active)

3.9.2.6 show ip helper-address

Command: show ip helper-address

Function: Show the configuration relation for the port ID of the protocol (It can forward broadcast packets), the interface (It supports forwarding function) and the forwarded destination IP.

Command mode: Admin and configuration mode

Example:

Switch#show ip helper-address

Forward protocol	Interface	Forward server
67(active)	Vlan1	192.168.1.1

3.10 DHCP Option 82

3.10.1 debug ip dhcp relay packet

Command: debug ip dhcp relay packet

Function: This command is used to display the information of data packets processing in DHCP Relay Agent, including the “add” and “peel” action of option 82.

Parameters: None

Command Mode: Admin Mode.

User Guide: Use this command during the operation to display the procedure of data packets processing of the server and to display the corresponding option82 operation information. Identified option 82 information of the request message and the option 82 information returned by the reply message.

Example: Display the information of data packets processing in DHCP Relay Agent.

Switch(config)# debug ip dhcp relay packet

3.10.2 ip dhcp relay information option

Command: ip dhcp relay information option

no ip dhcp relay information option

Function: Set this command to enable the option82 function of the switch Relay Agent. The “**no**

ip dhcp relay information option" command is used to disable the option82 function of the switch Relay Agent.

Parameters: None.

Default Settings: The system disables the option82 function by default.

Command Mode: Global configuration mode

Usage Guide: Only the DHCP Relay Agents configuring with this command can add option82 to the DHCP request message, and let the server to process it. Before enabling this function, users should make sure that the DHCP service is enabled and the Relay Agent will transmit the udp broadcast messages whose destination port is 67.

Example: Enable the option82 function of the Relay Agent.

Switch(config)#service dhcp

Switch(config)# ip forward-protocol udp bootps

Switch(config)# ip dhcp relay information option

3.10.3 ip dhcp relay information option delimiter

Command: ip dhcp relay information option delimiter [colon | dot | slash | space]

no ip dhcp relay information option delimiter

Function: Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash.

Parameters: None.

Default Settings: slash ("/").

Command Mode: Global mode

Usage Guide: Divide the parameters with the configured delimiters after users have defined them which are used to create suboption (remot-de, circuit-id) of option82 in global mode.

Example: Set the parameter delimiters as dot (".") for suboption of option82.

Switch(config)#ip dhcp relay information option delimiter dot

3.10.4 ip dhcp relay information option remote-id

Command: ip dhcp relay information option remote-id {standard | *<remote-id>*}

no ip dhcp relay information option remote-id

Function: Set the suboption2 (remote ID option) content of option 82 added by DHCP request packets (They are received by the interface). The no command sets the additive suboption2 (remote ID option) format of option 82 as standard.

Parameters: standard means the default VLAN MAC format. ***<remote-id>*** means the remote-id content of option 82 specified by users, its length can not exceed 64 characters.

Command Mode: Global Mode

Default: Use standard format to set remote-id of option 82.

Usage Guide: The additive option 82 information needs to associate with third-party DHCP server, it is used to specify the remote-id content by users when the standard remote-id format can not satisfy server's request.

Example: Set the suboption remote-id of DHCP option82 as street-1-1.

Switch(config)#ip dhcp relay information option remote-id street-1-1

3.10.5 ip dhcp relay information option remote-id format

Command: ip dhcp relay information option remote-id format {default | vs-hp}

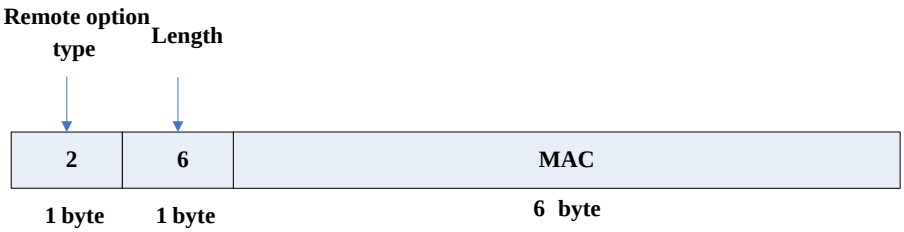
Function: Set remote-id format of Relay Agent option82.

Parameters: default means that remote-id is the VLAN MAC address with hexadecimal format, vs-hp means that remote-id is compatible with the remote-id format of HP manufacturer.

Default: default.

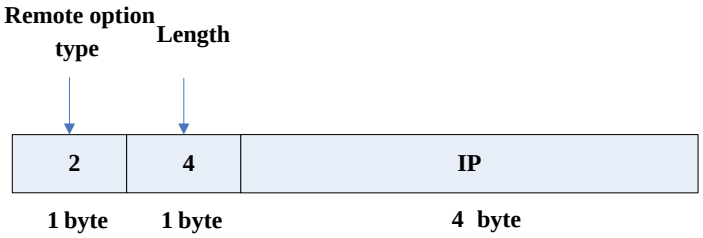
Command Mode: Global mode

Usage Guide: The default remote-id format defined as below:



MAC means VLAN MAC address.

The compatible remote-id format with HP manufacturer defined as below:



IP means the primary IP address of layer 3 interface where DHCP packets from.

Example: Set remote-id of Relay Agent option82 as the compatible format with HP manufacturer.

Switch(config)#ip dhcp relay information option remote-id format vs-hp

3.10.6 ip dhcp relay information option self-defined remote-id

Command: ip dhcp relay information option self-defined remote-id {hostname | mac | string WORD}

no ip dhcp relay information option self-defined remote-id

Function: Set creation method for option82, users can define the parameters of remote-id suboption by themselves.

Parameters: WORD the defined character string of remote-id by themselves, the maximum length is 64.

Command Mode: Global Mode

Default: Using standard method.

Usage Guide: After configure this command, if users do not configure remote-id on interface, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii format, but hex format occupies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp relay information option delimiter** configuration).

Example: Set self-defined method and character string of remote-id suboption are hostname and abc respectively for option82.

Switch(config)#ip dhcp relay information option self-defined remote-id hostname string abc

3.10.7 ip dhcp relay information option self-defined remote-id format

Command: ip dhcp relay information option self-defined remote-id format [ascii | hex]

Function: Set self-defined format of remote-id for relay option82.

Parameters: None.

Command Mode: Global Mode

Default: ascii.

Usage Guide: self-defined format use ip dhcp relay information option type self-defined remote-id to create remote-id format.

Example: Set self-defined method of remote-id as hex for relay option82.

Switch(config)# ip dhcp relay information option self-defined remote-id format hex

3.10.8 ip dhcp relay information option self-defined subscriber-id

Command: ip dhcp relay information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac)| string WORD }

no ip dhcp relay information option self-defined subscriber-id

Function: Set creation method for option82, users can define the parameters of circute-id suboption by themselves.

Parameters: WORD the defined character string of circuit-id by themselves, the maximum length is 64.

Command Mode: Global Mode

Default: Using standard method.

Usage Guide: After configure this command, if users do not configure circuit-id on interface, it will create circuit-id suboption for option82 according to self-defined method. Self-defined format of circuit-id: if self-defined format is ascii, the filled format of vlan such as “Vlan2”, the format of port such as “Ethernet1/0/1”, the format of mac and remote-mac such as “00-02-d1-2e-3a-0d”. If self-defined format is hex, the filled format of vlan occupies 2 bytes, port

occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp relay information option delimiter** configuration).

Example: Set self-defined method of circuit-id suboption as port, mac for option82.

Switch(config)# ip dhcp relay information option self-defined subscriber-id port id switch-id mac

3.10.9 ip dhcp relay information option self-defined subscriber-id format

Command: ip dhcp relay information option self-defined subscriber-id format [ascii | hex]

Function: Set self-defined format of circuit-id for relay option82.

Parameters: None.

Command Mode: Global Mode

Default: ascii.

Usage Guide: self-defined format use ip dhcp relay information option type self-defined subscriber-id to create circuit-id format.

Example: Set self-defined format of circuit-id as hex for relay option82.

Switch(config)# ip dhcp relay information option self-defined subscriber-id format hex

3.10.10 ip dhcp relay information option subscriber-id

Command: ip dhcp relay information option subscriber-id {standard | *<circuit-id>*}

no ip dhcp relay information option subscriber-id

Function: This command is used to set the format of option82 sub-option1 (Circuit ID option) added to the DHCP request messages from interface, **standard** means the standard vlan name and physical port name format, like “Vlan2+Ethernet1/0/12”, ***<circuit-id>*** is the circuit-id contents of option82 specified by users, which is a string no longer than 64 characters. The “**no ip dhcp relay information option subscriber-id**” command will set the format of added option82 sub-option1 (Circuit ID option) as standard format.

Parameters: None

Command Mode: Interface configuration mode.

Default Settings: The system uses the standard format to set the circuit-id of option 82 by default.

User Guide: Because the option 82 information added for the switch should cooperate with the third party DHCP server, if the standard circuit-id format of the switch cannot satisfy the server’s request, this method will be provided for users to specify the contents of circuit-id according to the situation of the server.

Example: Set the sub-option circuit-id of DHCP option82 as foobar.

Switch(config-if-vlan1)#ip dhcp relay information option subscriber-id foobar

3.10.11 ip dhcp relay information option subscriber-id format

Command: ip dhcp relay information option subscriber-id format {hex | acsii | vs-hp}

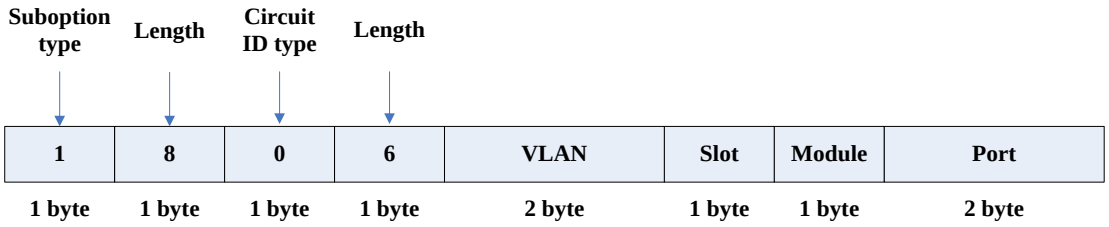
Function: Set subscriber-id format of Relay Agent option82.

Parameters: hex means that subscriber-id is VLAN and port information with hexadecimal format, acsii means that subscriber-id is VLAN and port information with ACSII format. vs-hp means that subscriber-id is compatible with the format of HP manufacturer.

Command Mode: Global mode

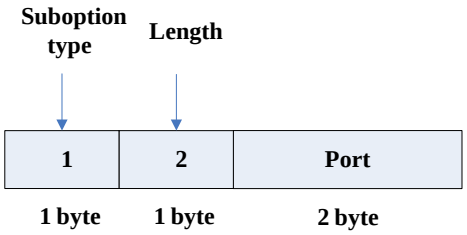
Default: ascii.

User Guide: VLAN and port information with ASCII format, such as "Vlan1+Ethernet1/0/11", VLAN and port information with hexadecimal format defined as below:



VLAN field fills in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.

The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.

Example: Set subscriber-id format of Relay Agent option82 as hexadecimal format.

Switch(config)#ip dhcp relay information option subscriber-id format hex

3.10.12 ip dhcp relay information policy

Command: ip dhcp relay information policy {drop | keep | replace}

no ip dhcp relay information policy

Function: This command is used to set the retransmitting policy of the system for the received DHCP request message which contains option82. The drop mode means that if the message has option82, then the system will drop it without processing; keep mode means that the system will keep the original option82 segment in the message, and forward it to the server to process; replace mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process. The "no ip dhcp relay

information policy" will set the retransmitting policy of the option 82 DCHP message as "replace".

Parameters: None

Command Mode: Interface configuration mode.

Default Settings: The system uses replace mode to replace the option 82 segment in the existing message with its own option 82.

User Guide: Since the DHCP client messages might go through several DHCP Relay Agents when passed to the DHCP server, the latter Relay Agents on the path should set policies to decide how to process the option82 added by Relay Agents before them. The selection of option 82 retransmitting policies should take the configuration policy of the DHCP server into account.

Example: Set the retransmitting policy of DHCP messages option 82 as keep.

Switch(Config-if-Vlan1)# ip dhcp relay information policy keep

3.10.13 ip dhcp server relay information enable

Command: ip dhcp server relay information enable

no ip dhcp server relay information enable

Function: This command is used to enable the switch DHCP server to identify option82. The "no ip dhcp server relay information enable" command will make the server ignore the option 82.

Parameters: None

Command Mode: Global configuration mode

Default Setting: The system disable the option82 identifying function by default.

User Guide: If the users want the switch DHCP server to identify option82 and return option 82 information in the reply message, this command needs to be set, or, the switch DHCP server will ignore the option82.

Example: Set the DHCP server to support option82

Switch(Config-if-Vlan1)# ip dhcp server relay information enable

3.10.14 show ip dhcp relay information option

Command: show ip dhcp relay information option

Function: This command will display the state information of the DHCP option 82 in the system, including option82 enabling switch, the interface retransmitting policy, the circuit ID mode and the switch DHCP server option82 enabling switch.

Parameters: None.

Command Mode: Admin and Global Configuration Mode.

User Guide: Use this command to check the state information of Relay Agent option82 during operation.

Example:

```
Switch#show ip dhcp relay information option
ip dhcp server relay information option(i.e. option 82) is disabled
ip dhcp relay information option(i.e. option 82) is enabled
Vlan2:
        ip dhcp relay information policy keep
```

ip dhcp relay information option subscriber-id standard

Vlan3:

ip dhcp relay information policy replace

ip dhcp relay information option subscriber-id foobar

3.11 DHCP Snooping

3.11.1 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.

3.11.2 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.

3.11.3 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.

3.11.4 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.

3.11.5 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.

3.11.6 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 switch

3.11.7 ip dhcp snooping

Command: ip dhcp snooping enable

no ip dhcp snooping enable

Function: Enable the DHCP Snooping function.

Parameters: None.

Command Mode: Globe mode.

Default Settings: DHCP Snooping is disabled by default.

Usage Guide: When this function is enabled, it will monitor all the DHCP Server packets of non-trusted ports.

Example: Enable the DHCP Snooping function.

switch(config)#ip dhcp snooping enable

3.11.8 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 ethernet1/0/1 as setting blackhole, and the recovery time is 30 seconds.

switch(config)#interface ethernet 1/0/1

switch(Config-Ethernet1/0/1)#ip dhcp snooping action blackhole recovery 30

3.11.9 ip dhcp snooping action MaxNum

Command: ip dhcp snooping action {<maxNum>|default}

Function: Set the number of defense action that can be simultaneously took 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

3.11.10 ip dhcp snooping binding

Command: ip dhcp snooping binding enable

no ip dhcp snooping binding enable

Function: Enable the DHCP Snooping binding funciton

Parameters: None.

Command Mode: Globe mode

Default Settings: DHCP Snooping binding is disabled by default.

Usage Guide: When the function is enabled, it will record the binding information allocated by DHCP Server of all trusted ports. Only after the DHCP SNOOPING function is enabled, the binding function can be enabled.

Example: Enable the DHCP Snooping binding funciton.

switch(config)#ip dhcp snooping binding enable

Relative Command: ip dhcp snooping enable

3.11.11 ip dhcp snooping binding arp

This command is not supported by the switch.

3.11.12 ip dhcp snooping binding dot1x

Command: ip dhcp snooping binding dot1x

no ip dhcp snooping binding dot1x

Function: Enable the DHCP Snooping binding DOT1X funciton.

Parameters: None

Command Mode: Port mode

Default Settings: By default, the binding DOT1X funciton is disabled on all ports.

Usage Guide: When this function is enabled, DHCP SNOOPING will notify the DOT1X module about the captured bindng information as a DOT1X controlled user. This command is mutually exclusive to”ip dhcp snooping binding user-contro“command.

Only after the DHCP SNOOPING binding function is enabled, the binding dot1x function can be set.

Example: Enable the binding DOT1X funciton on port ethernet1/0/1.

switch(config)#interface ethernet 1/0/1

switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding dot1x

Relative Command: ip dhcp snooping binding enable

ip dhcp snooping binding user-control

3.11.13 ip dhcp snooping binding user

Command: ip dhcp snooping binding user <*mac*> address <*ipaddress*> 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*>: The IP address of the static binding user.

<*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 00-03-0f-12-34-56 address 192.168.1.16 interface Ethernet 1/0/16

Relative Command: ip dhcp snooping binding enable

3.11.14 ip dhcp snooping binding user-control

Command: ip dhcp snooping binding user-control

no ip dhcp snooping binding user-control

Function: Enable the binding user funtion.

Parameters: None.

Command Mode: Port Mode.

Default Settings: By default, the binding user funciton is disabled on all ports.

Usage Guide: When this function is enabled, DHCP SNOOPING will treat the captured binding information as trusted users allowed to access all resources. This command is mutually exclusive to “ip dhcp snooping binding dot1x“ command.

Only after DHCP SNOOPING binding function is enabled, the binding user function can be set. This command is not limited by “ip dhcp snooping“ based on VLAN, but it is only limited by the global “ip dhcp snooping enable“ command.

Example: Enable the binding USER funciton on port ethernet1/0/1.

switch(config)#interface ethernet 1/0/1

switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding user-control

Relative Command: ip dhcp snooping binding enable

ip dhcp snooping binding dot1x

3.11.15 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 ethernet1/0/1, setting the max number of user allowed to access by Port Ethernet1/0/1 as 5.

Switch(Config-If-Ethernet1/0/1)# ip dhcp snooping binding user-control max-user 5

Related Command: ip dhcp snooping binding user-control

3.11.16 ip dhcp snooping information enable

Command: ip dhcp snooping information enable

no ip dhcp snooping information enable

Function: This command will enable option 82 function of DHCP Snooping on the switch, the no operation of this command will disable that function.

Parameters: None.

Default Settings: Option 82 function is disabled in DHCP Snooping by default.

Command Mode: Global Configuration Mode.

Usage Guide: Only by implementing this command, can DHCP Snooping add standard option 82 to DHCP request messages and forward the message. The format of option1 in option 82 (Circuit ID option) is standard vlan name plus physical port name, like vlan1+ethernet1/0/12. 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.

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

3.11.17 ip dhcp snooping information option allow-untrusted (replace|)

Command：ip dhcp snooping information option allow-untrusted (replace|)

no ip dhcp snooping information option allow-untrusted (replace|)

Function: This command is used to set that allow untrusted ports of DHCP snooping to receive DHCP packets with option82 option. When the "replace" is setting, the potion82 option is allowed to replace. When disabling this command, all untrusted ports will drop DHCP packets with option82 option.

Parameter: None.

Command Mode: Global Mode

Default: Drop DHCP packets with option82 option received by untrusted ports.

Usage Guide: Usually the switch with DHCP snooping function connects the terminal user directly, so close allow-untrusted by default to avoid option82 option added by user privately. Please set uplink port as trust port when enabling the uplink of DHCP snooping function.

Example: Enable the function that receives DHCP packets with option82.

Switch(config)#ip dhcp snooping information option allow-untrusted

3.11.18 ip dhcp snooping information option delimiter

Command: ip dhcp snooping information option delimiter [colon | dot | slash | space]

no ip dhcp snooping information option delimiter

Function: Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash.

Parameters: None.

Default Settings: slash (“/”).

Command Mode: Global mode

Usage Guide: Divide parameters with the configured delimiters after users have defined them which are used to create suboption (remote-id, circuit-id) of option82 in global mode.

Example: Set the parameter delimiters as dot (“.”) for suboption of option82.

Switch(config)# ip dhcp snooping information option delimiter dot

3.11.19 ip dhcp snooping information option remote-id

Command: ip dhcp snooping information option remote-id {standard | *<remote-id>*}

no ip dhcp snooping information option remote-id

Function: Set the suboption2 (remote ID option) content of option 82 added by DHCP request

packets (they are received by the port). The no command sets the additive suboption2 (remote ID option) format of option 82 as standard.

Parameters: standard means the default VLAN MAC format. ***<remote-id>*** means the remote-id content of option 82 specified by users, its length can not exceed 64 characters.

Command Mode: Global Mode

Default: Use standard format to set remote-id.

Usage Guide: The additive option 82 needs to associate with third-party DHCP server, it is used to specify the remote-id content by users when the standard remote-id format can not satisfy server's request.

Example: Set the suboption remote-id of DHCP option82 as street-1-1.

Switch(config)#ip dhcp snooping information option remote-id street-1-1

3.11.20 ip dhcp snooping information option self-defined remote-id

Command: ip dhcp snooping information option self-defined remote-id {hostname | mac | string WORD}

no ip dhcp snooping information option self-defined remote-id

Function: Set creation method for option82, users can define the parameters of remote-id suboption by themselves.

Parameters: WORD the defined character string of remote-id by themselves, the maximum length is 64.

Command Mode: Global Mode

Default: Using standard method.

Usage Guide: After configure this command, if users do not configure ip dhcp snooping information option remote-id globally, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii format, but hex format occpies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp snooping information option delimiter** configuration).

Example: Set self-defined method and character string of remote-id suboption are mac and abc respectively for option82.

Switch(config)# ip dhcp snooping information option self-defined remote-id mac string abc

3.11.21 ip dhcp snooping information option self-defined remote-id format

Command: ip dhcp snooping information option self-defined remote-id format [ascii | hex]

Function: Set self-defined format of remote-id for snooping option82.

Parameters: None.

Command Mode: Global Mode

Default: ascii.

Usage Guide: self-defined format use ip dhcp snooping information option type self-defined remote-id to create remote-id format.

Example: Set self-defined format of remote-id as hex for snooping option82.

Switch(config)# ip dhcp snooping information option self-defined remote-id format hex

3.11.22 ip dhcp snooping information option self-defined subscriber-id

Command: ip dhcp snooping information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac) | string WORD}

no ip dhcp snooping information option type self-defined subscriber-id

Function: Set creation method for option82, users can define the parameters of circute-id suboption by themselves.

Parameters: WORD the defined character string of circuit-id by themselves, the maximum length is 64.

Command Mode: Global Mode

Default: Using standard method.

Usage Guide: After configure this command, if users do not configure circuit-id on port, it will create circuit-id suboption for option82 according to self-defined method. Self-defined format of circuit-id: if self-defined subscriber-id format is ascii, the filled format of vlan such as “Vlan2”, the format of port such as “Ethernet1/0/1”, the format of mac and remote-mac such as “00-02-d1-2e-3a-0d”. If self-defined format is hex, the filled format of vlan occupies 2 bytes, port occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp snooping information option delimiter** configuration).

Example: Set self-defined method of circuit-id suboption as vlan, port, mac and remote-mac for option82.

Switch(config)#ip dhcp snooping information option self-defined subscriber-id vlan port id remote-mac

3.11.23 ip dhcp snooping information option self-defined subscriber-id format

Command: ip dhcp snooping information option self-defined subscriber-id format [ascii | hex]

Function: Set self-defined format of circuit-id for snooping option82.

Parameters: None.

Command Mode: Global Mode

Default: ascii.

Usage Guide: self-defined format uses ip dhcp snooping information option type self-defined subscriber-id to create circuit-id format.

Example: Set self-defined format of circuit-id as hex for snooping option82.

Switch(config)#ip dhcp snooping information option self-defined subscriber-id format hex

3.11.24 ip dhcp snooping information option subscriber-id

Command: ip dhcp snooping information option subscriber-id {standard | *<circuit-id>*}

no ip dhcp snooping information option subscriber-id

Function: Set the suboption1 (circuit ID option) content of option 82 added by DHCP request packets (they are received by the port). The no command sets the additive suboption1 (circuit ID option) format of option 82 as standard.

Parameters: standard means the standard format of VLAN name and physical port name, such as Vlan2+Ethernet1/0/12. ***<circuit-id>*** means the circuit-id content of option 82 specified by users, its length can not exceed 64 characters.

Command Mode: Port Mode

Default: Use standard format to set circuit-id.

Usage Guide: The additive option 82 needs to associate with third-party DHCP server, it is used to specify the circuit-id content by user when the standard circuit-id format can not satisfy server's request.

Example: Set the suboption circuit-id of DHCP option82 as P2.

Switch(config)#ip dhcp snooping information option subscriber-id P2

3.11.25 ip dhcp snooping information option subscriber-id format

Command: ip dhcp snooping information option subscriber-id format {hex | acsii | vs-hp}

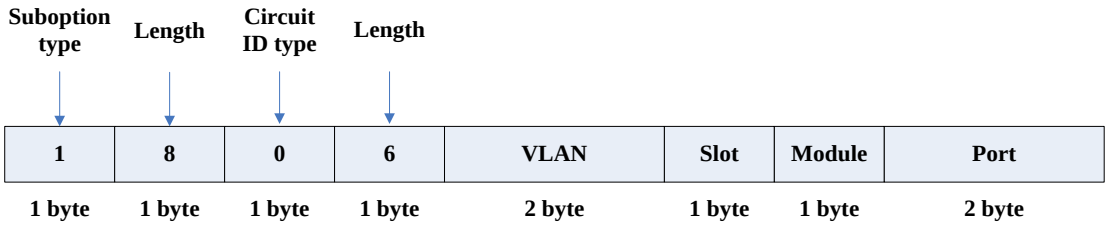
Function: This command is used to set subscriber-id format of DHCP snooping option82.

Parameters: hex means that subscriber-id is VLAN and port information with hexadecimal format, acsii means that subscriber-id is VLAN and port information with ACSII format. vs-hp means that subscriber-id is compatible with the format of HP manufacturer.

Command Mode: Global mode

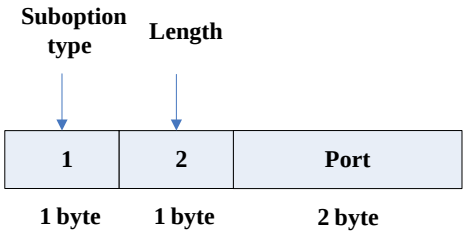
Default: ascii.

User Guide : VLAN and port information with ASCII format, such as Vlan1+Ethernet1/0/11, VLAN and port information with hexadecimal format defined as below:



VLAN field fill in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.

The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.

Example: Set subscriber-id format of DHCP snooping option82 as hexadecimal format.

Switch(config)#ip dhcp snooping information option subscriber-id format hex

3.11.26 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

3.11.27 ip dhcp snooping timeout detection

Command: ip dhcp snooping timeout detection <0-7200>

no ip dhcp snooping timeout detection

Function: Configure the traffic detection timeout of the bound entry.

Parameters: The range of the traffic detection timeout is from 0 to 7200, the default value is 3 and the unit is second.

Command Mode: Global Mode.

Usage Guide: When the bound entry is protected, it can check if there is traffic of the source mac every once in a while. If there is traffic, the entry will keep being protected, otherwise, the quiet-period will be enabled and the entry will be protected in this while. If there is still no traffic after the quiet time, the protection mode of entry will be deleted.

Example: (Config)#ip dhcp snooping timeout detection 100

3.11.28 ip dhcp snooping timeout quiet

Command: ip dhcp snooping timeout quiet <0-4294967295>

no ip dhcp snooping timeout quiet

Function: Configure the traffic detection quiet time of the bound entry.

Parameters: The range of the traffic detection quiet time is from 0 to 4294967295, the default value is 0 and the unit is second.

Command Mode: Global Mode.

Usage Guide: When the bound entry is protected, it can check if there is traffic of the source mac every once in a while. If there is traffic, the entry will keep being protected, otherwise, the quiet-period will be enabled and the entry will be protected in this while. If there is still no traffic after the quiet time, the protection mode of entry will be deleted.

Example: (Config)#ip dhcp snooping timeout quiet 1000

3.11.29 ip dhcp snooping trust

Command: ip dhcp snooping trust

no ip dhcp snooping trust

Function: Set or delete the DHCP Snooping trust attributes of a port.

Parameters: None

Command Mode: Port mode

Default Settings: By default, all ports are non-trusted ports

Usage Guide: Only when DHCP Snooping is globally enabled, can this command be set. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted; all the security history records will be cleared (except the information in system log).

Example: Set port ethernet1/0/1 as a DHCP Snooping trusted port

switch(config)#interface ethernet 1/0/1

switch(Config- Ethernet 1/0/1)#ip dhcp snooping trust

3.11.30 ip dhcp snooping vlan

Command: ip dhcp snooping vlan (WORD |)

no ip dhcp snooping vlan (WORD |)

Function: Enable the dhcp snooping in vlan.

Parameters: None. Enable the dhcp snooping on all vlan as default, otherwise, enable it on the vlan that the parameter appoints.

Command Mode: Global Mode.

Default: Disable.

Usage Guide: no ip dhcp snooping vlan <vlan-id> means to disable the dhcp snooping function on the appointed vlan.

Example: Enable DHCP snooping function.

switch(config)#ip dhcp snooping vlan 10

switch(config)#no ip dhcp snooping vlan 10

3.11.31 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 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 DCBI 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

3.11.32 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.

Parameter: None.

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

3.11.33 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 Global Configuration Mode.

Default Settings: None.

Usage Guide: If there is no specific port, then display the current cofiguration information of dhcp snooping, otherwise, display the records of defense actions of the specific port.

Example:

switch#show ip dhcp snooping

DHCP Snooping is enabled

DHCP Snooping binding arp: disabled

DHCP Snooping maxnum of action info:10

DHCP Snooping limit rate: 100(pps), switch ID: 0003.0F12.3456

DHCP Snooping droped packets: 0, discarded packets: 0

DHCP Snooping alarm count: 0, binding count: 0,

expired binding: 0, request binding: 0

interface	trust	action	recovery	alarm num	bind num
Ethernet1/0/1	trust	none	0second	0	0
Ethernet1/0/2	untrust	none	0second	0	0
Ethernet1/0/3	untrust	none	0second	0	0
Ethernet1/0/4	untrust	none	0second	0	1
Ethernet1/0/5	untrust	none	0second	2	0
Ethernet1/0/6	untrust	none	0second	0	0
Ethernet1/0/7	untrust	none	0second	0	0

Ethernet1/0/8	untrust	none	0second	0	1
Ethernet1/0/9	untrust	none	0second	0	0
Ethernet1/0/10	untrust	none	0second	0	0
Ethernet1/0/11	untrust	none	0second	0	0
Ethernet1/0/12	untrust	none	0second	0	0
Ethernet1/0/13	untrust	none	0second	0	0
Ethernet1/0/14	untrust	none	0second	0	0
Ethernet1/0/15	untrust	none	0second	0	0
Ethernet1/0/16	untrust	none	0second	0	0
Ethernet1/0/17	untrust	none	0second	0	0
Ethernet1/0/18	untrust	none	0second	0	0
Ethernet1/0/19	untrust	none	0second	0	0
Ethernet1/0/20	untrust	none	0second	0	0
Ethernet1/0/21	untrust	none	0second	0	0
Ethernet1/0/22	untrust	none	0second	0	0
Ethernet1/0/23	untrust	none	0second	0	0
Ethernet1/0/24	untrust	none	0second	0	0
Ethernet1/0/25	untrust	none	0second	0	0
Ethernet1/0/26	untrust	none	0second	0	0
Ethernet1/0/27	untrust	none	0second	0	0
Ethernet1/0/28	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 Ethernet1/0/1
interface Ethernet1/0/1 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

3.11.34 show ip dhcp snooping binding all

Command: show ip dhcp snooping binding all

Function: Display the current global binding information of DHCP snooping.

Parameters: None.

Command Mode: Admin and Global Configuration Mode.

Default Settings: None.

Usage Guide: This 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. Besides, DHCP Snooping must be enabled globally, this command can be configured.

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	Ethernet1/0/1	1	S
00-00-00-00-00-10	192.168.40.10	Ethernet1/0/2	1	D
00-00-00-00-00-11	192.168.40.11	Ethernet1/0/4	1	D
00-00-00-00-00-12	192.168.40.12	Ethernet1/0/4	1	D
00-00-00-00-00-13	192.168.40.13	Ethernet1/0/4	1	SU
00-00-00-00-00-14	192.168.40.14	Ethernet1/0/4	1	SU
00-00-00-00-00-15	192.168.40.15	Ethernet1/0/5	1	SL
00-00-00-00-00-16	192.168.40.16	Ethernet1/0/5	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

3.11.35 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).

Parameter: None.

Command Mode: Admin and Global Configuration Mode.

Default: None.

Usage Guide: This command can be used for debugging the communication messages between the switch and the TrustView server, messages such as protocol version notification, encryption negotiation, free resource and web URL redirection, and the number of forced log-off messages, as well as the number of forced accounting update messages, can be displayed.

Example:

Switch#show trustview status
Primary TrustView Server 200.101.0.9:9119
    TrustView version2 message inform successed
    TrustView inform free resource successed
    TrustView inform web redirect address successed
    TrustView inform user binding data successed
TrustView version2 message encrypt/digest enabled
Key: 08:02:33:34:35:36:37:38
Rcvd 106 encrypted messages, in which MD5-error 0 messages, DES-error 0 messages
Sent 106 encrypted messages
Free resource is 200.101.0.9/255.255.255.255
Web redirect address for unauthencated users is <http://200.101.0.9:8080>
Rcvd 0 force log-off packets
Rcvd 19 force accounting update packets
Using version two private packet

3.12 DHCP Snooping option 82

3.12.1 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.

Parameters: None.

Default Settings: Option 82 function is disabled in DHCP Snooping by default.

Command Mode: Global Configuration Mode.

Usage Guide: Only by implementing this command, can DHCP Snooping add standard option 82 to DHCP request messages and forward the message. The format of option1 in option 82 (Circuit ID option) is standard vlan name plus physical port name, like “vlan1+ethernet1/0/12”. 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.

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

3.13 DHCP option 60 and option 43

3.13.1 option 43 ascii LINE

Command: option 43 ascii LINE

no option 43

Function: Configure option 43 character string with ascii format in ip dhcp pool mode. The no command deletes the configured option 43.

Parameter: LINE: The configured option 43 character string with ascii format, its length range between 1 and 255.

Default: No option 43 character string is configured.

Command Mode: ip dhcp pool mode

Usage Guide: None.

Example: Configure option 43 with ascii format to be "AP 1000".

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 43 ascii AP 1000

3.13.2 option 43 hex WORD

Command: option 43 hex WORD

no option 43

Function: Configure option 43 character string with hex format in ip dhcp pool mode. The no command deletes the configured option 43.

Parameter: WORD: The configured option 43 character string with hex format, such as a1241b.

Default: No option 43 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: When using hex method to configure option 43, the string needs to be written according to TLV (Type-Length-Value) format. For example, issue ip address of 10.1.1.1 through option 43, then the hex string here should be 01040A010101; Type=0x01, it means IP address; Length=0x04, it means the length of IP address is 4 Bytes; Value=0x0A010101, it means the hexadecimal format of 10.1.1.1.

Example: Configure option 43 with hex format to be "01040a010101".

switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 43 hex 01040a010101

3.13.3 option 43 ip A.B.C.D

Command: option 43 ip A.B.C.D
no option 43

Function: Configure option 43 character string with IP format in ip dhcp pool mode. The no command deletes the configured option 43.

Parameter: A.B.C.D: The configured option 43 with IP format, such as 192.168.1.1.

Default: No option 43 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: Using this command to configure option 43, such as "192.168.1.1", then option 43 filled in packets is "C0A80101".

Example: Configure option 43 with IP format to be "192.168.1.1".

switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 43 ip 192.168.1.1

3.13.4 option 60 ascii LINE

Command: option 60 ascii LINE
no option 60

Function: Configure option 60 character string with ascii format in ip dhcp pool mode. The no command deletes the configured option 60.

Parameter: LINE: The configured option 60 character string with ascii format, its length range between 1 and 255.

Default: No option 60 character string is configured.

Command Mode: ip dhcp pool mode

Usage Guide: None.

Example: Configure option 60 with ascii format to be "AP 1000".

switch(config)#ip dhcp pool a
switch (dhcp-a-config)#option 60 ascii AP 1000

3.13.5 option 60 hex WORD

Command: option 60 hex WORD
no option 60

Function: Configure option 60 character string with hex format in ip dhcp pool mode. The no command deletes the configured option 60.

Parameter: WORD: The configured option 60 character string with hex format, such as a1241b.

Default: No option 60 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: None.

Example: Configure option 60 with hex format to be "41502031303030".

switch(config)#ip dhcp pool a

switch(dhcp-a-config)#option 60 hex 41502031303030

3.13.6 option 60 ip A.B.C.D

Command: option 60 ip A.B.C.D

no option 60

Function: Configure option 60 character string with IP format in ip dhcp pool mode. The no command deletes the configured option 60.

Parameter: A.B.C.D: The configured option 60 with IP format, such as 192.168.1.1.

Default: No option 60 is configured.

Command Mode: ip dhcp pool mode

Usage Guide: Using this command to configure option 60, such as "192.168.1.1", option 60 of packets matched with the configured option 60 is "C0A80101".

Example: Configure option 60 with IP format to be "192.168.1.1".

switch(config)#ip dhcp pool a

switch (dhcp-a-config)#option 60 ip 192.168.1.1

Chapter 4 Commands for Multicast Protocol

4.1 DCSCM

4.1.1 access-list (Multicast Destination Control)

Command: **access-list <6000-7999> {{{add | delete} profile-id WORD} | {{deny|permit} (ip) {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}}**

no access-list <6000-7999> {deny|permit} ip {{<source> <source-wildcard>}|{host-source <source-host-ip> {range <2-65535>|}}|any-source} {{<destination> <destination-wildcard>}|{host-destination <destination-host-ip> {range <2-255>|}}|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.

{add | delete}: add or delete the profile.

{deny|permit}: deny or permit.

<source/M>: multicast source address and mask length.

<source-host-ip>: multicast source host address.

<2-65535>: the range of multicast source host.

<destination/M>: multicast destination address and mask length.

<destination-host-ip>: multicast destination host address.

<2-255>: the range of multicast destination host.

Default: None

Command Mode: Global Mode

Usage Guide: ACL of Multicast destination control list item is controlled by specifical ACL number from 6000 to 7999, the command applies to configure this ACL. ACL of ip 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 mask length 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. And adding or deleting the profile-id can be used to change the multicast destination control ACL.

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)#access-list 6000 add profile-id 1
Switch(config)#

4.1.2 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.

Default: None

Command Mode: Global Mode

Usage Guide: ACL of Multicast source control list item is controlled by specifical ACL number from 5000 to 5099, the command applies to configure this ACL. ACL of Multicast source control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use wildcard character to configure address range, and also specify a host address or all address. Remarkable, "all address" is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.

Example: Switch(config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

4.1.3 ip multicast destination-control

This command is not supported by the switch.

4.1.4 ip multicast destination-control access-group

Command: ip multicast destination-control access-group <6000-7999>
no ip multicast destination-control access-group <6000-7999>

Function: Configure multicast destination-control access-list used on interface, the "**no ip multicast destination-control access-group <6000-7999>**" command deletes the configuration.
Parameter: <6000-7999>: destination-control access-list number.
Default: None
Command Mode: Interface Configuration Mode
Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the interface to multicast group, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.
Example:
Switch(config)#inter e 1/0/4
Switch(Config-If-Ethernet 1/0/4)#ip multicast destination-control access-group 6000
Switch (Config-If-Ethernet1/0/4)#

4.1.5 ip multicast destination-control access-group (sip)

Command: ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>
no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>
Function: Configure multicast destination-control access-list used on specified net segment, the "**no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>**" command deletes this configuration.
Parameter: <IPADDRESS/M>: IP address and mask length;
<6000-7999>: Destination control access-list number.
Default: None
Command Mode: Global Mode
Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING or IGMP is enabled, for adding the members to multicast group. If configuring multicast destination-control on specified net segment of transmitted igmp-report, and match configured access-list, such as matching permit, the interface can be added, otherwise do not be added. If relevant group or source in show ip igmp groups detail has been established before executing the command, it needs to execute clear ip igmp groups command to clear relevant groups in Admin mode.
Example:
Switch(config)#ip multicast destination-control 10.1.1.0/24 access-group 6000

4.1.6 ip multicast destination-control access-group (vmac)

Command: ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>
no ip multicast destination-control <1-4094> <macaddr >access-group

<6000-7999>

Function: Configure multicast destination-control access-list used on specified vlan-mac, the "**no ip multicast destination-control <1-4094> <macaddr >access-group <6000-7999>**" command deletes this configuration.

Parameter: <1-4094>: VLAN-ID;

<macaddr>: Transmitting source MAC address of IGMP-REPORT, the format is "xx-xx-xx-xx-xx-xx";

<6000-7999>: Destination-control access-list number.

Default: None

Command Mode: Global Mode

Usage Guide: The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the members to multicast group. If configuring multicast destination-control to source MAC address of transmitted igmp-report, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.

Example:

Switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000

4.1.7 ip multicast policy

Command: ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority>

no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos

Function: Configure multicast policy, the "**no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos**" command deletes it.

Parameter:

<IPADDRESS/M>: are multicast source address, mask length, destination address, and mask length separately.

<priority>: specified priority, range from 0 to 7

Default: None

Command Mode: Global Mode

Usage Guide: The command configuration modifies to a specified value through the switch matching priority of specified range multicast data packet, and the TOS is specified to the same value simultaneously.Carefully, the packet transmitted in UNTAG mode does not modify its priority.

Example: Switch(config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7

4.1.8 ip multicast source-control

Command: ip multicast source-control

no ip multicast source-control

Function: Configure to globally enable multicast source control, the "**no ip multicast source-control**" command restores global multicast source control disabled.

Parameter: None

Default: Disabled

Command Mode: Global Mode

Usage Guide: The source control access-list applies to interface with only enabling global multicast source control, and configure to disabled global multicast source control without configuring source control access-list on every interface. After configuring the command, multicast data received from every interface does not have matching multicast source control list item, and then they will be thrown away by switches, namely only multicast data matching to PERMIT can be received and forwarded.

Example: Switch(config)#ip multicast source-control

4.1.9 ip multicast source-control access-group

Command: ip multicast source-control access-group <5000-5099>

no ip multicast source-control access-group <5000-5099>

Function: Configure multicast source control access-list used on interface, the "no ip multicast source-control access-group <5000-5099>" command deletes the configuration.

Parameter: <5000-5099>: Source control access-list number**.**

Default: None

Command Mode: Interface Configuration Mode

Usage Guide: The command configures with only enabling global multicast source control. After that, it will match multicast data message imported from the interface according to configured access-list, such as matching: permit, the message will be received and forwarded; otherwise the message will be thrown away.

Example:

Switch (config)#interface ethernet1/0/4

Switch (Config-If-Ethernet1/0/4)#ip multicast source-control access-group 5000

Switch (Config-If-Ethernet1/0/4)#

Switch(router-msdp)#default-rpf-peer 10.0.0.1 rp-policy 10

4.1.10 multicast destination-control

Command: multicast destination-control

no multicast destination-control

Function: Configure to globally enable multicast destination control, the NO command is to recover and disable the multicast destination control globally.

Parameters: None.

Default: Disabled.

Command Mode: Global Configuration Mode.

Usage Guide: Only after globally enabling the multicast destination control, the other destination control configuration can take effect; the destination access list can be applied to ports, VLAN-MAC and SIP. After configuring this command, IGMP-SNOOPING and IGMP will match according to the rules mentioned above when they try to add ports after receiving IGMP-REPORT.

Example:

Protocol switch(config)# multicast destination-control

4.1.11 profile-id (Multicast Destination Control Rule List)

Command: profile-id <1-50> {deny|permit} {{<source/M> }|{host-source <source-host-ip> (range <2-65535>|)}|any-source} {{<destination/M>}|{host-destination <destination-host-ip> (range <2-255>|)}|any-destination}

no profile-id <1-50>

Function: Configure the destination control profile rule. The no command deletes the profile rule.

Parameters: <1-50>: profile-id.

{deny|permit}: deny or permit.

<source/M>: multicast source address and mask length.

<source-host-ip>: multicast source host address.

<2-65535>: range of multicast source host.

<destination/M>: multicast destination address and mask length.

<destination-host-ip>: multicast destination host address.

<2-255>: range of multicast destination host.

Default: None.

Command Mode: Global Mode.

Usage Guide: Profile-list of Multicast destination control list item is controlled by specifical profile-id number from 1 to 50, the command applies to configure this profile to add it into the ACL for using. 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 ACLs, and use mask length 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)# profile-id 1 deny ip any-source host-destination 224.1.1.2

4.1.12 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 Ethernet1/0/1, port-channel 1 or ethernet1/0/1.

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays multicast destination control rules of configuration, including detail option, and access-list information applied in detail.

Example:

Switch (config)#show ip multicast destination-control
ip multicast destination-control is enabled
ip multicast destination-control 11.0.0.0/8 access-group 6003
ip multicast destination-control 1 00-03-05-07-09-11 access-group 6001
multicast destination-control access-group 6000 used on interface Ethernet1/0/13
switch(config)#

4.1.13 show ip multicast destination-control access-list

Command: show ip multicast destination-control access-list
show ip multicast destination-control access-list <6000-7999>

Function: Display destination control multicast access-list of configuration.

Parameter: <6000-7999>: access-list number.

Default: None

Command Mode: Admin Mode and Global Mode

Usage Guide: The command displays destination control multicast access-list of configuration.

Example:

Switch# sh ip multicast destination-control acc
access-list 6000 deny ip any any-destination
access-list 6000 deny ip any host-destination 224.1.1.1
access-list 6000 deny ip host 2.1.1.1 any-destination
access-list 6001 deny ip host 2.1.1.1 225.0.0.0 0.255.255.255
access-list 6002 permit ip host 2.1.1.1 225.0.0.0 0.255.255.255
access-list 6003 permit ip 2.1.1.0 0.0.0.255 225.0.0.0 0.255.255.255

4.1.14 show ip multicast destination-control filter-profile-list

Command: show ip multicast destination-control filter-profile-list
show ip multicast destination-control filter-profile-list <1-50>

Function: Show the configured destination control profile rule list.

Parameters: <1-50>: profile-id.

Default: None.

Command Mode: Admin and configuration mode.

Usage Guide: This command can show the configured destination control profile rule list.

Example:

Switch#show ip multicast destination-control filter-profile-list

profile-id 1 deny ip any-source any-destination
profile-id 2 deny ip any-source host-destination 224.1.1.1
profile-id 3 deny ip host-source 2.1.1.1 any-destination

4.1.15 show ip multicast policy

Command: show ip multicast policy
Function: Display multicast policy of configuration
Parameter: None
Default: None
Command Mode: Admin Mode and Global Mode
Usage Guide: The command displays multicast policy of configuration
Example:
Switch#show ip multicast policy
ip multicast-policy 10.1.1.0/24 225.0.0.0/8 cos 5

4.1.16 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 1/0/1 or ethernet1/0/1.
Default: None
Command Mode: Admin Mode and Global Mode
Usage Guide: The command displays multicast source control rules of configuration, including detail option, and access-list information applied in detail.
Example:
Switch#show ip multicast source-control detail
ip multicast source-control is enabled
Interface Ethernet1/0/13 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

4.1.17 show ip multicast source-control access-list

Command: show ip multicast source-control access-list
show ip multicast source-control access-list <5000-5099>
Function: Display source control multicast access-list of configuration
Parameter: <5000-5099>: access-list number
Default: None
Command Mode: Admin Mode and Global Mode
Usage Guide: The command displays source control multicast access-list of configuration

Example:

Switch#sh ip multicast source-control access-list

access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255

access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255

4.2 IGMP Snooping

4.2.1 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.

Parameters: <1-4094> the specific VLAN ID; A.B.C.D the specific group address.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.

Switch#clear ip igmp snooping vlan 1 groups

Relative Command: show ip igmp snooping vlan <1-4094>

4.2.2 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.

Parameters: <1-4094> the specific VLAN ID; ethernet the Ethernet port name; IFNAME the port name.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted mrouter port of the specific VLAN.

Example: Delete mrouter port in vlan 1.

Switch# clear ip igmp snooping vlan 1 mrouter-port

Relative Command: show ip igmp snooping mrouter-port

4.2.3 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".

4.2.4 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

Default: IGMP Snooping is disabled by default.

Usage Guide: Use this command to enable IGMP Snooping, that is permission every VLAN config the function of IGMP snooping. The "**no ip igmp snooping**" command disables this function.

Example: Enable IGMP Snooping.

Switch(config)#ip igmp snooping

4.2.5 ip igmp snooping proxy

Command: ip igmp snooping proxy

no ip igmp snooping proxy

Function: Enable IGMP Snooping proxy function, the no command disables the function.

Parameter: None.

Command Mode: Global Mode

Default: Enable.

Example:

Switch(config)#no ip igmp snooping proxy

4.2.6 ip igmp snooping vlan

Command: ip igmp snooping vlan *<vlan-id>*

no ip igmp snooping vlan *<vlan-id>*

Function: Enable the IGMP Snooping function for the specified VLAN; the "**no ip igmp snooping vlan <vlan-id>**" command disables the IGMP Snooping function for the specified VLAN.

Parameter: *<vlan-id>* is the VLAN number.

Command mode: Global Mode
Default: IGMP Snooping is disabled by default.
Usage Guide: To configure IGMP Snooping on specified VLAN, the global IGMP Snooping should be first enabled. Disable IGMP Snooping on specified VLAN with the "**no ip igmp snooping vlan <vlan-id>**" command.
Example: Enable IGMP Snooping for VLAN 100 in Global Mode.
Switch(config)#ip igmp snooping vlan 100

4.2.7 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 Snooping fast leave function for the specified VLAN; the "**no ip igmp snooping vlan *<vlan-id>* immediate-leave**" command disables the IGMP Snooping 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 Snooping fast leave function for VLAN 100.
Switch(config)#ip igmp snooping vlan 100 immediate-leave

4.2.8 ip igmp snooping vlan <id> immediately-leave mac-based

Command: ip igmp snooping vlan <id> immediately-leave **mac-based**
no ip igmp snooping vlan <id> immediately-leave mac-based
Function: Configure this command to delete the existed igmp snooping table entries according to the source mac in leave packet when the switch which is enabled the igmp snooping function receives the leave packet. Only when the received the port, source mac and multicast group of the leave packet are the same as the port, host mac and multicast group of the existed igmp snooping table entry, the snooping table entry can be deleted. If this command is not configured, delete the existed igmp snooping table entry according to the port and multicast group of the leave packet.
Command mode: Global Mode
Default: This function is disabled by default.
Usage Guide: Configure the immediately-leave under the same vlan at the same time to make this command effective. In this time, deal with it according to the host mac of the port.
Example: Use the following configuration when delete the table entry according to the host mac of the port.

switch(config)#ip igmp snooping vlan 12 immediately-leave
switch(config)#ip igmp snooping vlan 12 immediately-leave mac-based

4.2.9 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 is <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

4.2.10 ip igmp snooping vlan l2-general-querier-source

Command: ip igmp snooping vlan <vlanid> L2-general-query-source <A.B.C.D>
no ip igmp snooping vlan <vlanid> L2-general-query-source
Function: Configure source address of query of igmp snooping
Parameters: <vlanid>: the id of the VLAN, with limitation to <1-4094>. **<A.B.C.D>** is the source address of the query operation.
Command Mode: Global mode.
Default: 0.0.0.0
Usage Guide: It is not supported on Windows 2000/XP to query with the source address as 0.0.0.0. So the layer 2 query source address configuration does not function. The client will stop sending requesting datagrams after one is sent. And after a while, it can not receive multicast datagrams.
Example:
Switch(config)#ip igmp snooping vlan 2 L2-general-query-source 192.168.1.2

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

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

Function: Configure igmp snooping.
Parameters: vlan-id is the id of the VLAN, limited to <1-4094>. **version** is the version number, limited to <1-3>.
Command Mode: Global mode.
Default: version 3.
Usage Guide: When the switch is connected to V1 and V2 capable environment, and for VLAN which has source of layer 2 query configuration, the VLAN can be queried only if the version number has been specified. This command is used to query the layer 2 version number.
Example:
Switch(config)#ip igmp snooping vlan 2 L2-general-query-version 2

4.2.12 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

4.2.13 ip igmp snooping vlan interface (ethernet | port-channel|) IFNAME limit

Command：ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit {group <1-65535>| source <1-65535>} strategy (replace | drop)
no ip igmp snooping vlan <1-4094> interface (ethernet | port-channel|) IFNAME limit group source strategy
Function： Configure the number of groups which are allowed joining and the maximum of the source in each group under the IGMP Snooping port. Configure the strategy when it is up to the upper limit, including "replace" and "drop".

Parameters：*vlan-id*: VLAN ID range is <1-4094>

ehternet：Ethernet port name

ifname：Interface name

port-channel: ports aggregation

<1-65535>：The maximum number of groups allowed joining

<1-65535>：The maximum number of source table entries in each group, including include source and exclude source.

replace：Replace the group and source information

drop：Drop the new group and source information

Command mode: Global Mode.

Default: There is no limitation as default.

Usage Guide: When the number of the groups joined under the port or the number of sources in this group exceeds the limit, it will be dealt according to the configured strategy. If it is drop, drop the new group and source information; if it is replace, find a dynamic group and source from the port to conduct deleting and replacing, and then add the new group and source information. The premise of using this command is that this VLAN is enabled IGMP Snooping function. No command configures as “no limitation”.

Example：

Switch(config)#ip igmp snooping vlan 2 interface ethernet 1/0/11 limit group 300 source 200 strategy replace

Switch(config)#

4.2.14 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 ethernet1/0/13

4.2.15 ip igmp snooping vlan mrouter-port learnpim

Command: ip igmp snooping vlan <*vlan-id*> mrouter-port learnpim

no ip igmp snooping vlan <*vlan-id*> mrouter-port learnpim

Function: Enable the function that the specified VLAN learns mrouter-port (according to pim packets), the no command will disable the function.

Parameter: <*vlan-id*>: The specified VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode

Default: Enable

Usage Guide: Enable the function that the specified VLAN learns mrouter-port (according to pim packets). After a port received pim packets, it will be set to mrouter port for implementing the automatic learning.

Example: Disable the function that vlan 100 learns mrouter-port (according to pim packets).

Switch(config)#no ip igmp snooping vlan 100 mrouter-port learnpim

4.2.16 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

4.2.17 ip igmp snooping vlan query-interval

Command: ip igmp snooping vlan <*vlan-id*> query-interval <*value*>

no ip igmp snooping vlan <*vlan-id*> query-interval

Function: Configure this query interval.

Parameter: *vlan-id*: VLAN ID, ranging between <1-4094>

value: query interval, ranging between <1-65535>seconds

Command Mode: Global mode

Default: 125s

Usage Guide: It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.

Example: Switch(config)#ip igmp snooping vlan 2 query-interval 130

4.2.18 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

4.2.19 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

4.2.20 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:

Protocol Switch (config)#ip igmp snooping vlan 2 report source-address 10.1.1.1

4.2.21 ip igmp snooping vlan specific-query-mrsp

Command: ip igmp snooping vlan <vlan-id> specific-query-mrsp <value>

no ip igmp snooping vlan <vlan-id> specific-query-mrspt

Function: Configure the maximum query response time of the specific group or source, the no command restores the default value.

Parameters: <vlan-id>: the specific VLAN ID, the range from 1 to 4094.

<value>: the maximum query response time, unit is second, the range from 1 to 25, default value is 1.

Command Mode: Global mode

Default: Enable the function.

Usage Guide: After enable vlan snooping in global mode, input this command to configure the maximum query response time of the specific group.

Example: Configure/cancel the specific-query-mrsp of vlan3 as 2s.

Swith(config)#ip igmp snooping vlan 3 specific-query-mrsp 2

Swith(config)#no ip igmp snooping vlan 3 specific-query-mrspt

4.2.22 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 1/0/1

4.2.23 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

4.2.24 show ip igmp snooping

Command: show ip igmp snooping [vlan <*vlan-id*>]
Parameter: <*vlan-id*> is the VLAN number specified for displaying IGMP Snooping messages.
Command Mode: Admin Mode
Usage Guide: If no VLAN number is specified, it will show whether global IGMP Snooping switch is on, which VLAN is configured with l2-general-querier function, and if a VLAN number is specified, detailed IGMP messages for this VLAN will be shown.
Example:
1. Show IGMP Snooping summary messages of the switch
Switch(config)#show ip igmp snooping
Global igmp snooping status: Enabled
L3 multicasting: running
Igmp snooping is turned on for vlan 1(querier)
Igmp snooping is turned on for vlan 2

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-**Protocol** 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)	Ethernet1/0/8	00:04:14	V2
	(192.168.0.2)	Ethernet1/0/8	00:04:14	V2

Igmp snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/0/2

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

4.3 IGMP Snooping Authentication

4.3.1 igmp snooping authentication enable

Command: igmp snooping authentication enable
no igmp snooping authentication enable

Function: Configure the port of the switch as the igmp authentication port. After the successful configuration, the switch has the igmp authentication function in this port. The no command disables this function.

Command Mode: Port Mode.
Default: Disable.
Usage Guide: If the switch should conduct authentication for the multicast group of client demanding, use this command to configure the port. The ports without configuring this command will not conduct authentication for the demanded packet.
Example: Enable the IGMP authentication function on the port.
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#igmp snooping authentication enable

4.3.2 igmp snooping authentication free-rule access-list <6000-7999>

Command: igmp snooping authentication free-rule access-list <6000-7999>
no igmp snooping authentication free-rule access-list <6000-7999>
Function: Configure the authentication free-rule access list of the multicast group. The no command deletes it.
Parameters: <6000-7999>: number of access list.
Command Mode: Port Mode.
Default: Do not configure.
Usage Guide: This command can be effective only after the port authentication function is enabled. After configured this command, the multicast group of client demanding that the port received will be matched according to the configured access list. If it is permit, this multicast group is free for authentication and the table entry will be issued directly. Otherwise, it needs to conduct authentication.
Example: Configure the authentication free-rule access list of the multicast group.
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#igmp snooping authentication free-rule access-list 6000

4.3.3 ip igmp snooping authentication radius none

Command: ip igmp snooping authentication radius none
no ip igmp snooping authentication radius none
Function: Configure the switch to work with successful authentication when the radius server has no response. The no command recovers the default authentication method, the switch works with failed authentication.
Command Mode: Global Mode.
Default: Adopt radius authentication, the server has no response, the switch works with failed authentication.
Example:
Switch(config)#ip igmp snooping authentication radius none

4.3.4 ip igmp snooping authentication forwarding-first

Command: ip igmp snooping authentication forwarding-first

no ip igmp snooping authentication forwarding-first

Function: Configure the process procedure of igmp authentication: issue the multicast table entry to the multicast group of client demanding and then conduct authentication. After the authentication is successful, there is no action, if the authentication failed, the issued table entry will be deleted. The no command recovers to be the default method: conducts the authentication first, and issues the table entry after the authentication result is back.

Command Mode: Global Mode.

Default: Conducts the authentication first, and issues the table entry after the authentication result is back.

Example:

Switch(config)#ip igmp snooping authentication forwarding-first

4.3.5 ip igmp snooping authentication timeout <30-30000>

Command: ip igmp snooping authentication timeout <30-30000>

no ip igmp snooping authentication timeout

Function: Configure the timeout of the table entry in igmp authentication, including permit and deny. When the timer is timeout, deletes all the authenticated entries of permit and deny. The no command recovers to be the default value.

Parameters: <30-30000>: timeout, unit is second.

Command Mode: Global Mode.

Default: 600 seconds.

Usage Guide: The switch records the authentication result for multicast group of client demanding into the table entry, including permit and deny rules. Before each authentication, checks the rule in the entry first. If the rule is found, there is no need for authentication and the authentication result can be used directly. Otherwise, sends authentication. It can reduce the times of authentication. But the configuration on radius server may be changed. The recorded authentication table entry results may be timeout, so they should be cleared. This command configures the global timeout.

Example: Configure the authenticationtable entry timeout.

Switch(config)#ip igmp snooping authentication timeout 30000

4.3.6 clear ip igmp snooping vlan <1-4094> groups (A.B.C.D|) ((authentication-port (ethernet IFNAME | IFNAME)) |)

Command: clear ip igmp snooping vlan <1-4094> groups (A.B.C.D|) ((authentication-port (ethernet IFNAME | IFNAME)) |)

Function: Force the user to get off the line, and clear the corresponding authentication record and issued table entry.

Parameters: <1-4094> is the appointed VLAN ID; A.B.C.D is the appointed group address; ethernet is the Ethernet name; IFNAME is the port name.

Command Mode: Admin Mode.

Usage Guide: Delete the group authentication record and the issued table entry quickly. The show command can be used to view the group record and authentication record.

Example:

Switch#clear ip igmp snooping vlan 1 groups 225.2.2.2 authentication-port ethernet 1/0/1

Related Command: show ip igmp snooping vlan <1-4094> groups (A.B.C.D|) (authentication-table |)

4.3.7 show ip igmp snooping vlan <1-4094> groups (A.B.C.D|) authentication-table

Command: show ip igmp snooping vlan <1-4094> groups (A.B.C.D|) authentication-table

Function: Show the authentication table entry record.

Parameters: <1-4094> is the appointed VLAN ID; A.B.C.D is the appointed group address.

Command Mode: Admin Mode.

Example:

Switch# config

Switch(config)# show ip igmp snooping vlan 1 groups 225.1.1.1 authentication-table

Igmp snooping authentication permit information for vlan 1：

Igmp snooping authentication-table expire 00:09:56, 600

Vlan	Ports	Groups	Mac	AuthState
1	Ethernet1/0/11	225.1.1.1	F0-7D-68-FA-7E-F3	permit
1	Ethernet1/0/11	225.1.1.1	04-0A-EB-6A-7F-88	permit
1	Ethernet1/0/11	225.1.1.1	03-0A-EB-6A-7F-88	permit

4.3.8 show ip igmp snooping authentication free-rule ((interface (ethernet IFNAME|IFNAME))|)

Command: show ip igmp snooping authentication free-rule ((interface (ethernet IFNAME|IFNAME))|)

Function: Show the igmp free authentication rule configured on the port.

Parameters: ethernet is the Ethernet name; IFNAME is the port name.

Command Mode: Admin Mode.

Example:

Switch(config)#show ip igmp snooping authentication free-rule

access-list 6001 used on interface Ethernet1/0/1

access-list 6001 permit ip any-source 224.0.0.0 0.0.0.255

4.3.9 debug igmp snooping authentication (event|timer|all)

Command: debug igmp snooping authentication (event|timer|all)

no debug igmp snooping authentication (event|timer|all)

Function: Enable the debugging on-off of the IGMP Snooping authentication on the switch. The no command disables it.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: It is used to enable the debugging on-off of the IGMP Snooping authentication on the switch. It can show the information of event, timer and all (all the debugs) that the switch deals with the IGMP authentication.

4.4 Multicast VLAN

4.4.1 multicast-vlan

Command: multicast-vlan

no multicast-vlan

Function: Enable multicast VLAN function on a VLAN; the “no” form of this command disables the multicast VLAN function.

Parameter: None.

Command Mode: VLAN Configuration Mode.

Default: Multicast VLAN function not enabled by default.

Usage Guide: The multicast VLAN function can not be enabled on Private VLAN. To disabling the multicast VLAN function of the VLAN, configuration of VLANs associated with the multicast VLAN should be deleted. Note that the default VLAN can not be configured with this command and only one multicast VLAN is allowed on a switch.

Examples:

Switch(config)#vlan 2

Switch(Config-Vlan2)# multicast-vlan

4.4.2 multicast-vlan association

Command: multicast-vlan association *<vlan-list>*

no multicast-vlan association *<vlan-list>*

Function: Associate several VLANs with a multicast VLAN; the “no” form of this command cancels the association relations.

Parameter: *<vlan-list>* the VLAN ID list associated with multicast VLAN. Each VLAN can only be

associated with one multicast VLAN and the association will only succeed when every VLAN listed in the VLAN ID table exists.

Command Mode: VLAN Mode.

Default: The multicast VLAN is not associated with any VLAN by default.

Usage Guide: After a VLAN is associated with the multicast VLAN, when there comes the multicast order in the port of this VLAN, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. The VLAN associated with the multicast VLAN should not be a Private VLAN. A VLAN can only be associated with another VLAN after the multicast VLAN is enabled. Only one multicast VLAN can be enabled on a switch.

Examples:

Switch(config)#vlan 2

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

4.4.3 multicast-vlan association interface

Command: multicast-vlan association interface (ethernet | port-channel|) IFNAME out-tag *<tag-id>*

no multicast-vlan association interface (ethernet | port-channel|) IFNAME

Function: Associate the specified port with the multicast VLAN, so the associated ports are able to receive the multicast flow. The no command cancels the association between the ports and the multicast VLAN.

Parameter: IFNAME: The name of the ethernet port or port-channel port

tag-id: Specify vlan tag of the multicast data forwarded by the associated port, only the tag of the associated port allows the multicast VLAN, the tag-id takes effect. Its range from 1 to 4094.

Command Mode: VLAN configuration mode

Default: None.

Usage Guide:

1. 'associated VLAN' and 'associated port' of the multicast VLAN are absolute, they do not affect each other when happening the cross.
2. The port of the aggregation member cannot be associated, but the associated port is able to be added to port-group and cancelling the association.
3. The configured port type includes port-channel port or ethernet port and the port is only configured as ACCESS mode.
4. The port (it will be associated) cannot belong to the multicast VLAN, in the same way, the associated port cannot be divided in multicast VLAN.
5. When the associated port mode is set as non ACCESS mode, the mode cannot be changed.

Example: Suppose vlan2 is multicast VLAN.

Switch(config-vlan2)#multicast-vlan association interface ethernet 1/2

Switch(config-vlan2)#multicast-vlan association interface port-channel 2

Switch(config-vlan2)#no multicast-vlan association interface ethernet 1/2

Switch(config-vlan2)#no multicast-vlan association interface port-channel 2

4.4.4 multicast-vlan mode

Command: multicast-vlan mode {dynamic| compatible}

no multicast-vlan mode {dynamic| compatible}

Function: This command is used to configure the two modes of the multicast vlan; the no command cancels this configuration.

Parameters: dynamic: dynamic mode;

compatible: compatible mode.

Command mode: VLAN configuration mode.

Default: Neither of the two modes.

Usage Guide: When configured as dynamic mode, the mrouter port will not be added automatically any mort when issuing the multicast entries; when configured as compatible mode, the report packet will be not transmitted to the mrouter port any more. When it is not configured as default, the mrouter port will be added when issuing the multicast entries and the report packet will be transmitted to the mrouter port when it is received.

Example:

Switch(Config-Vlan2)#multicast vlan mode dynamic

Switch(Config-Vlan2)#

4.4.5 switchport association multicast-vlan

Command: switchport association multicast-vlan <*vlan-id*> out-tag <*tag-id*>

no switchport association multicast-vlan <*vlan-id*>

Function: Associate a port with the specified multicast VLAN; the no command cancels the association.

Parameter: ***<vlan-id>***: The multicast VLAN associates with the port. Each port can only be associated with one multicast VLAN, and the association will be successful only when the multicast VLAN is existent.

<tag-id>: Specify vlan tag of the multicast data forwarded by the associated port, only the tag of the associated port allows the multicast VLAN, the tag-id takes effect. Its range from 1 to 4094.

Command Mode: Port mode.

Default: The port is not associated with any multicast VLAN by default.

Usage Guide: After a port is associated with the multicast VLAN, when there comes the multicast order in the port, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. If the associated port is set as trunk port and allows the multicast VLAN, the multicast traffic with the specified vlan tag will be forwarded. The port can only be associated with the multicast VLAN after the multicast VLAN is enabled.

Example:

Switch(config)#vlan 2

Switch(Config-Vlan2)#multicast-vlan

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#switchport mode trunk

Protocol Switch(config-if-ethernet1/0/1)#switchport association multicast-vlan 2 out-tag 5

Chapter 5 Commands for Security Function

5.1 ACL

5.1.1 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 admin_timer

Switch(Config-Time-Range-admin_timer)#absolute-periodic Tuesday 9:15:30 to Saturday

12:30:00

Make configurations effective within the period from 14:30:00 to 16:45:00 on Monday, Wednesday, Friday and Sunday.

Switch(Config-Time-Range-admin_timer)#periodic Monday Wednesday Friday Sunday 14:30:00 to 16:45:00

5.1.2 absolute start

Command: [no] absolute start *<start_time> <start_data>* [end *<end_time> <end_data>*]

Functions: Define an absolute time-range, this time-range operates subject to the clock of this equipment.

Parameters: *start_time* : start time, HH:MM:SS (hour: minute: second)

***end_time* :** end time, HH:MM:SS (hour: minute: second)

***start_data* :** start data, the format is, YYYY.MM.DD （ year.month.day ）

***end_data* :** end data, the format is, YYYY.MM.DD（year.month.day）

Remark: time-range is one minute per time, so the time error shall be <= one minute.

Command Mode: Time-range mode

Default: No time-range configuration.

Usage Guide: Absolute time and date, assign specific year, month, day, hour, minute of the start, shall not configure multiple absolute time and date, when in repeated configuration, the latter configuration covers the absolute time and date of the former configuration.

Examples: Make configurations effective from 6:00:00 to 13:30:00 from Oct. 1, 2004 to Jan. 26, 2005.

Switch(config)#Time-range admin_timer

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

5.1.3 access-list deny-preemption

This command is not supported by the switch.

5.1.4 access-list (ip extended)

Command: access-list *<num>* {deny | permit} icmp {{*<slpAddr> <sMask>*} | any-source | {host-source *<slpAddr>*}} {{*<dlpAddr> <dMask>*} | any-destination | {host-destination *<dlpAddr>*}} [*<icmp-type>* [*<icmp-code>*]] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]

access-list *<num>* {deny | permit} igmp {{*<slpAddr> <sMask>*} | any-source | {host-source *<slpAddr>*}} {{*<dlpAddr> <dMask>*} | any-destination | {host-destination *<dlpAddr>*}} [*<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, 0-255; ***<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

5.1.5 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

5.1.6 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 an extended *numeric* MAC *ACL* rule, 'no access-list <num>' command deletes an extended numeric *MAC access-list rule.

Parameters:* <num> is the** access-list No. which is a decimal's No. from 1100-1199; **deny** if rules are matching, deny access; **permit** if rules are matching, permit access; ***<any-source-mac> any source address; ***<any-destination-mac>*** any destination address; ***<host_smac>, <smac>*** source MAC address; ***<smac-mask>*** mask (reverse mask) of source MAC address; ***<host_dmac> , <dmac>***

destination MAC address; ***<dmac-mask>*** mask (reverse mask) of destination MAC address; **untagged-eth2** format of untagged ethernet II packet; **tagged-eth2** format of tagged ethernet II packet; **untagged-802-3** format of untagged ethernet 802.3 packet; **tagged-802-3** format of tagged ethernet 802.3 packet.

Command Mode: *Global* mode

Default Configuration: No access-list configured

Usage Guide: When the **user *assign specific*** <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL.

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

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

5.1.7 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 an 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

5.1.8 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 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

5.1.9 clear access-group

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

Functions: *Empty packet* statistics *information of* the specified interface.

Parameters: <interface-name>: Interface name.

Command Mode: Admin mode

Default: *None*

***Examples*:** Empty packet statistics information of interface.

Switch#clear access-group statistic

5.1.10 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

5.1.11 ip access extended

Command: ip access extended <*name*>

no ip access extended <*name*>

Function: Create a named extended IP access list. The no prefix will remove the named extended IP access list including all the rules.

Parameters: <name> is the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32.

Command Mode: Global Mode.

Default: No access list is configured by default.

Usage Guide: When this command is issued for the first time, an empty access list will be created.

Example: To create a extended IP access list name tcpFlow.

Switch(config)#ip access-list extended tcpFlow

5.1.12 ip access standard

Command: ip access standard <*name*>

no ip access standard <*name*>

Function: Create a named standard access list. The no prefix will remove the named standard access list including all the rules in the list.

Parameters: <*name*> is the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32.

Command Mode: Global Mode.

Default: No access list is configured by default.

Usage Guide: When this command is issued for the first time, an empty access list will be created.

Example: To create a standard IP access list name ipFlow.

Switch(config)#ip access-list standard ipFlow

5.1.13 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*

5.1.14 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 to 32.

Command Mode: Global Mode.

Default: No access list is configured by default.

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.

Example: Create a standard IPv6 access list named ip6Flow.

Switch(config)#ipv6 access-list standard ip6Flow

5.1.15 ipv6 access extended

Command: ipv6 access-list extended *<name>*

no ipv6 access-list extended *<name>*

Function: Create a name-based extended IPv6 access list; the no command delete the name-based extended IPv6 access list.

Parameter: *<name>* is the name for access list, the character string length is from 1 to 32.

Command Mode: Global Mode.

Default: No IP address is configured by default.

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.

Example: Create an extensive IPv6 access list named tcpFlow.
Switch (config)#ipv6 access-list extended tcpFlow

5.1.16 {ip|ipv6|mac|mac-ip} access-group

Command: {ip|ipv6|mac|mac-ip} access-group *<name>* {in} [traffic-statistic]
no {ip|ipv6|mac|mac-ip} 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 to 32.
Command Mode: Port Mode
Default: The entry of port is not bound ACL.
Usage *Guide: One* port can bind ingress rules
Note: when a ACL has multiple rules, traffic-statistic can't configure.
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-Ethernet1/0/5)#ip access-group aaa in

5.1.17 {ip|ipv6|mac|mac-ip} access-group (Interface Mode)

This command is not supported by switch.

5.1.18 mac access extended

Command: mac-access-list extended *<name>*

no mac-access-list extended <*name*>

Functions: Define a name-manner MAC ACL or enter access-list configuration mode, "**no**

mac-access-list extended *<name>*" command deletes this ACL.

Parameters: *<name>* name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32. (remark: sensitivity on capital or small letter.)

Command Mode: Global mode

Default Configuration: No access-lists configured.

Usage Guide: After assigning this command 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)#

5.1.19 mac-ip access extended

Command: mac-ip-access-list extended *<name>*

no mac-ip-access-list extended *<name>*

Functions: Define a name-manner MAC-IP ACL or enter access-list configuration mode, "**no mac-ip-access-list extended *<name>***" command deletes this ACL.

Parameters: *<name>*: name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32 (remark: sensitivity on capital or small letter).

Command Mode: Global Mode.

Default: No named MAC-IP access-list.

Usage Guide: After assigning this command 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)#

5.1.20 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, 0-255; ***<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

5.1.21 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

5.1.22 permit | deny(ipv6 extended)

Command: [no] {deny | permit} icmp {{*<sIPv6Prefix/sPrefixlen>*} | any-source | {host-source

<*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [<*icmp-type*> [<*icmp-code*>]] [dscp <*dscp*>] [flow-label <*fl*>][time-range <*time-range-name*>]

[no] {deny | permit} tcp { <*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*> }} [s-port { <*sPort*> | range <*sPortMin*> <sPortMax> }] { <*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <dIPv6Addr> }} [d-port { <*dPort*> | range <*dPortMin*> <*dPortMax*> }] [syn | ack | urg | rst | fin | psh] [dscp <*dscp*>] [flow-label <*fl*>][time-range <*time-range-name*>]

[no] {deny / *permit}* udp { <*sIPv6Prefix/sPrefixlen*> | *any-source* / {host-source <*sIPv6Addr*> }} [s-port *{* <*sPort*> | *range* <*sPortMin*> <sPortMax> }] { <*dIPv6Prefix/dPrefixlen*> | any-destination / *{host-destination* <dIPv6Addr> *}}* [d-port { <*dPort*> | range <*dPortMin*> <dPortMax> }] [dscp <*dscp*>] [flow-label <*fl*>][time-range <*time-range-name*>]

[no] {deny / permit} <next-header> *{<sIPv6Prefix/*sPrefixlen> | *any-source* / {host-source <*sIPv6Addr*>}} {<dIPv6Prefix/*dPrefixlen*> | any-destination | *{host-destination* <*dIPv6Addr*>}} [dscp <*dscp>]* [flow-label <fl>*][*time-range <*time-range-name>]*

[no*]* {deny | *permit}* {<sIPv6Prefix/*sPrefixlen*> / *any-source* / {host-source <sIPv6Addr>*}}* {<dIPv6Prefix/dPrefixlen> / any-destination | *{host-destination* <dIPv6Addr>}} [dscp <*dscp*>] [flow-label <*fl*>] [time-range<*time-range-name*>]

Function: Create an *extended* nomenclature IPv6 access control *rule for* specific IPv6 protocol.

Parameter: <*sIPv6Addr*> is the source IPv6 address; **<sPrefixlen>** is the length of the IPv6 address prefix, the range is 1～128; **<dIPv6Addr>** is the destination IPv6 address; **<*dPrefixlen*>** is the length of the IPv6 address prefix, the range is 1～128; ***<igmp-type>***, type of the IGMP; ***<icmp-type>***, icmp type; ***<icmp-code>***, icmp protocol number; ***<dscp>***, IPv6 priority ,the range is 0～63; ***<flowlabel>***, value of the flow label, the range is 0～1048575; **syn**,**ack**,**urg**,**rst**,**fin**,**psh**,**tcp** label position; ***<sPort>***, source port number, the range is 0～65535; ***<sPortMin>***, the down boundary of source port; <sPortMax>***, the** *up* boundary of source ***port;*** <dPort>, destination port number, the range is 0～65535; ***<dPortMin>***, the down boundary of destination port; ***<dPortMax>***, the up boundary of destination port. ***<next-header>,*** the IPv6 next-header. ***<time-range-name>***, time range name.

Command Mode: IPv6 nomenclature extended access control list mode

Default: No access control list configured.

Example: Create an extended access control list named udpFlow, denying the igmp packets while allowing udp packets with destination address 2001:1:2:3::1 and destination port 32.

Switch(config)#ipv6 access-list extended udpFlow

Switch(Config-IPv6-Ext-Nacl-udpFlow)#deny igmp any any-destination

Switch(Config-IPv6-Ext-Nacl-udpFlow)#permit udp any-source host-destination 2001:1:2:3::1 dPort 32

5.1.23 permit | deny(ipv6 standard)

Command: [no] {deny | permit} {{<*sIPv6Prefix/sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}}

Function: Create a standard nomenclature IPv6 access control rule; the no form of this command deletes the nomenclature standard IPv6 access control rule.

Parameter: ***<sIPv6Prefix>*** is the prefix of the source IPv6 address, ***<sPrefixlen>*** is the length of the IPv6 address prefix, the valid range is 1~128. ***<sIPv6Addr>*** is the source IPv6 address.

Command Mode: Standard IPv6 nomenclature access list mode

Default: No access list configured by default.

Usage Guide:

Example: Permit packets with source address of 2001:1:2:3::1/64 while denying those with source address of 2001:1:2:3::1/48.

Switch(config)#ipv6 access-list standard ipv6Flow

Switch(Config-IPv6-Std-Nacl-ipv6Flow)# permit 2001:1:2:3::1/64

Switch(Config-IPv6-Std-Nacl-ipv6Flow)# deny 2001:1:2:3::1/48

5.1.24 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

5.1.25 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

5.1.26 show access-lists

Command: show access-lists [*<num>*|*<acl-name>*]

Functions: Reveal ACL of configuration.

Parameters: ***<acl-name>***, specific ACL name character string; ***<num>,*** specific ACL No.

Default: None.

Command Mode: Admin 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 ACL100, 1 time to be used
access-list 100 deny ip any-source any-destination	Deny IP packet of any source IP address and destination address to pass
access-list 100 deny tcp any-source	Deny TCP packet of any source IP address and

any-destination	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.

5.1.27 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.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: When not assigning interface names, all ACL tied to port will be revealed.

Examples:

Switch#show access-group

interface name: Ethernet 1/0/1

IP Ingress access-list used is 100, traffic-statistics Disable.

interface name: Ethernet1/0/2

IP Ingress access-list used is 1, packet(s) number is 11110.

Displayed information	Explanation
interface name: Ethernet 1/0/1	Tying situation on port Ethernet1/0/1
IP Ingress access-list used is 100	No. 100 numeric expansion ACL tied to entrance of port Ethernet1/0/1
packet(s) number is 11110	Number of packets matching this ACL rule

5.1.28 show firewall

Command: show firewall

Functions: Reveal configuration information of packet filtering functions.

Parameters: None.

Default: None.

Command Mode: Admin and Configuration Mode.

Examples:

Switch#show firewall

Firewall status: Enable.

5.1.29 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 1～32.
Default: None.
Command Mode: Admin and Configuration Mode.
Usage Guide: When no access control list is specified, all the access control lists will be displayed; in used x time（s） is shown the times the ACL had been quoted.
Example:
Switch #show ipv6 access-lists
ipv6 access-list 500(used 1 time(s))
ipv6 access-list 500 deny any-source

ipv6 access-list 510(used 1 time(s))
ipv6 access-list 510 deny ip any-source any-destination
ipv6 access-list 510 deny tcp any-source any-destination

ipv6 access-list 520(used 1 time(s))
ipv6 access-list 520 permit ip any-source any-destination

5.1.30 show time-range

Command: show time-range *<word>*
Functions: Reveal configuration information of time range functions.
Parameters: ***word*** assign name of time-range needed to be revealed.
Default: None.
Command Mode: Admin 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

5.1.31 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 or number, and the

length cannot exceed 32 characters long.
Command Mode: Global mode
Default: No time-range configuration.
Usage Guide: None
Examples: Create a time-range named admin_timer.
Switch(config)#Time-range admin_timer

5.2 Self-defined ACL

5.2.1 permit | deny

This command is not supported by the switch.

5.2.2 udf-access-list standard

This command is not supported by the switch.

5.2.3 userdefined-access-list standard offset

Command: userdefined-access-list standard offset [window1 { l3start | l4start} <*offset*>] [window2 { l3start | l4start } <*offset*>] [window3 { l3start | l4start } <*offset*>] [window4 { l3start | l4start } <*offset*>] [window5 { l3start | l4start } <*offset*>] [window6 { l3start | l4start } <*offset*>] [window7 { l3start | l4start } <*offset*>] [window8 { l3start | l4start } <*offset*>] [window9 { l3start | l4start } <*offset*>] [window10 { l3start | l4start } <*offset*>] [window11 { l3start | l4start } <*offset*>] [window12 { l3start | l4start } <*offset*>]

no userdefined-access-list standard offset [window1] [window2] [window3] [window4] [window5] [window6] [*window7*] [window8] [window9] [window10] [window11] [window12]
Function: Create a standard self-defined ACL *template*. If the template exists, the corresponding window of the template can be modified; the no command deletes the window of the standard self-defined ACL template. If the window is not specified, the standard self-defined ACL template will be deleted.
Parameter:
window1-window12 self-defined window 1 to 12
l3start **The** start offset position is start of layer3 (It can be effective only when the start of layer3 exists)
l4start The start offset position is start of layer4 (It can be effective only when the start of layer4 exists**)**
offset **The** configured offset is from 0 to 178 (unit is 2Bytes)
Command Mode: Global Mode
Default: No Configuration Template
Usage Guide: {l2endoftag | l3start | l4start}: used to configure the start offset position of a

window, <*offset*>: used to the offset of a window, the range is <*0-178*>, unit is 2Bytes, namely, 0 means 0Bytes offset and 1 means 2Bytes offset. Standard self-defined ACL template can configure the start offset position and offset for 12 window at most. One standard self-defined ACL template can be shared in global mode. The window cannot be modified if the standard self-defined ACL rule is configured with this window. But if the standard self-defined ACL rule is not configured, the window configuration can be modified with this command.

The no command can delete one or more offset configuration of the window in the template or delete the whole template. The window in the template can be deleted successfully when it is not used by the self-defined ACL rule.

Ipv6 only supports window1-6, the biggest offset of l3start includes the head of L2, the biggest offset of l4start includes the head of L2 and L3.

Example: Create a global template with 7 windows (3-9) to configure the start offset position and the offset:

Switch(config)#userdefined-access-list standard offset window3 l2 0 window4 l2 2 window5 l3 0 window6 l3 1 window7 l3 2 window8 l4 1 window9 l4 2

5.2.4 userdefined-access-list extended offset

This command is not supported by switch.

5.2.5 userdefined-access-list standard

Command: userdefined-access-list standard *<1200-1299>* {permit|deny} {window1|window2|window3|window4|window5|window6|window7|window8|window9|window10|window11|window12}

no userdefined-access-list standard *<1200-1299> {permit*|deny} {window1*|window2|window3|window4*|window5|window6|window7*|window8|window9|window10*|window11|window12}

Function: Create a* numbered standard self-defined *ACL. If the* standard self-defined *ACL exists, then* a rule will *be added to* the ACL. *The no command deletes* a numbered *standard self-defined ACL.

Parameter: <num> ***is the access-list*** **No. from *1200 to 1299* in decimal notation*; deny if rules* are matching, *deny access; permit* if rules *are matching, permit* access; <value>** ***and <mask>*** **of each *window is a 2* bits** Hexadecimal number.

Command Mode: *Global Mode*

Default: No any access-list configured

Usage Guide: When users specify the specified <num> for the first time, create the ACL with this serial number, then add the entry into this **ACL.**

Example: *Permit the* second bytes of the start of l3 is 0x4501. Permit the packets **that** the forth byte of the start of **l4** is 0xFF.

Switch(config)#userdefined-access-list standard offset window1 l3 0 window2 l4 1

Switch(config*)#userdefined-access-list* standard *1200 permit* window1 4501 FFFF window2 00FF

00FF. Configure a rule in the same list to deny the packets that the fifth and the sixth bytes of the start of l3 is 0xFFAA.
Switch(config)#userdefined-access-list standard offset window3 l3 2
Switch(config)#userdefined-access-list standard 1200 deny any-source-mac any-destination-mac untagged-eth2 window3 FFAA FFFF

5.2.6 userdefined-access-list extended

This command is not supported by switch.

5.2.7 userdefined access-group

Command: userdefined access-group <*name*> *{in}* [*traffic-statistic*]
no userdefined access-group <*name*> {in}
Function: Apply userdefined-access-list *to one direction of the* port. Decide whether the statistical counter should be added to the ACL according to the options. The no command deletes the configuration bound to the port.
Parameter: <name> is the access-list name from 1200-1399 in decimal notation.
Command Mode: Physical Port Configuration Mode.
Default: userdefined-access-list is not bound to the port
Usage Guide: A self-defined access-list can be bound to the ingress of a port and can be configured at the ingress of the same port with other access-lists at the same time. The deny rule is precedent when different access-lists are matching, that means if there is a access-lists match the deny rule, the deny rule must be executed, the permit rule will be executed oppositely.
Example: The *configured* self-defined access-list is shown in the following:
Switch(config)#userdefined-access-list standard offset window1 l3 0 window2 l4 1 window3 l3 1
Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF window2 00FF 00FF
Switch(config)#userdefined-access-list standard 1300 deny **window1** FFAA0000 FFFF0000
Bind the self-defined access-list to Ethernet1/1:
Switch(config)#interface ethernet1/1
Switch(config-if-ethernet1/1)#userdefined access-group 1300 in

5.2.8 vacl userdefined access-group

Command: vacl userdefined access-group <name> {in} **vlan <*vlanId*> [traffic-statistic]**
no vacl userdefined access-group <*name*> {in} vlan <*vlanId*>
Function: Apply userdefined-access-list to one direction of the specified VLAN, decide whether the statistical counter should be added to the ACL according to the options or. Theno command deletes the configuration bound to the specified VLAN.
Parameter: *<name>* is the access-list name from 1200 to 1399 in decimal notation; *<vlanId>* the

bound VLAN， the range is 1-4095.
Command Mode: Global Mode
Default: userdefined-access-list is not bound to any VLAN
Usage Guide: A self-defined access-list can be bound to the ingress of a VLAN and can be configured at the ingress of the same VLAN with other access-lists at the same time. The deny rule is precedent when different access-lists are matching, that means if there is a access-lists match the deny rule, the deny rule must be executed, the permit rule will be executed oppositely.
Example: The configured self-defined access-list is shown in the following:
Switch(config)#userdefined-access-list standard offset window1 l3 0 window2 l4 1 window3 l3 1
Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF window2 00FF 00FF
Switch(config)#userdefined-access-list standard 1300 deny window1 FFAA0000 FFFF0000
Bind the self-defined access-list to VLAN1:
Switch(config)#vacl userdefined access-group 1300 in vlan 1.

5.3 802.1x

5.3.1 authentication dot1x radius none

This command is not supported by the switch.

5.3.2 debug dot1x detail

Command: debug dot1x detail {pkt-send | pkt-receive | internal | all | userbased} interface [ethernet] <*interface-name*>
no debug dot1x detail { pkt-send | pkt-receive | internal | all | userbased} 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 interface1/0/1.

Switch#debug dot1x detail all interface ethernet1/0/1

5.3.3 debug dot1x error

Command: debug dot1x error

no debug dot1x error

Function: Enable the debug information of dot1x about errors; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of dot1x about errors, users can check the information of errors that occur in the processes of the Radius protocol operation, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of dot1x about errors.

Switch#debug dot1x error

5.3.4 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 ethernet1/0/1

5.3.5 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 ethernet1/0/1

5.3.6 dot1x accept-mac

Command: dot1x accept-mac <mac-address> [interface <interface-name>]
no dot1x accept-mac <mac-address> [interface <interface-name>]
Function: Add a MAC address entry to the dot1x address filter table. If a port is specified, the entry added applies to the specified port only. If no port is specified, the entry added applies to all the ports. The 'no dot1x accept-mac <mac-address> [interface <interface-name>]' command deletes the entry from dot1x address filter table.
Parameters: <mac-address> stands for MAC address;
<interface-name> for interface name and port number.
Command mode: Global Mode.
Default: N/A.
Usage Guide: The dot1x address filter function is implemented according to the MAC address filter table, dot1x address filter table is manually added or deleted by the user. When a port is specified in adding a dot1x address filter table entry, that entry applies to the port only; when no port is specified, the entry applies to all ports in the switch. When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted, the rest will be rejected.
Example: Adding MAC address 00-01-34-34-2e-0a to the filter table of Ethernet 1/0/5.
Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/0/5

5.3.7 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

5.3.8 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 port1/0/12.

Switch(config)#dot1x enable

Switch(config)#interface ethernet 1/0/12

Switch(Config-If-Ethernet1/0/12)#dot1x enable

5.3.9 dot1x ipv6 passthrough

This command is not supported by the switch.

5.3.10 dot1x guest-vlan

Command: dot1x guest-vlan <*vlanid*>

no dot1x guest-vlan

Function: Set the guest-vlan of the specified port; the "**no dot1x guest-vlan**" command is used to delete the guest-vlan.

Parameters: *<vlanid>* the specified VLAN id, ranging from 1 to 4094.

Command Mode: Port Mode.

Default Settings: There is no 802.1x guest-vlan function on the port.

User Guide: The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being too low.

In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or

update some other applications (such as anti-virus software, the patches of operating system). When a user of a port within Guest VLAN starts an authentication, the port will remain in Guest VLAN in the case of a failed authentication. If the authentication finishes successfully, there are two possible results:

- The authentication server assigns an Auto VLAN, causing the port to leave Guest VLAN to join the assigned Auto VLAN. After the user gets offline, the port will be allocated back into the specified Guest VLAN.
- The authentication server assigns an Auto VLAN, then the port leaves Guest VLAN and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.

Attention:

- There can be different Guest VLAN set on different ports, while only one Guest VLAN is allowed on one port.
- Only when the access control mode is portbased, the Guest VLAN can take effect. If the access control mode of the port is macbased or userbased, the Guest VLAN can be successfully set without taking effect.
- If both 802.1x and MAB authentication functions are enabled on the port at the same time, the guest VLAN function of 802.1x cannot be enabled, but the guest VLAN function of MAB can be configured.

Examples： Set Guest-VLAN of port Ethernet1/0/3 as VLAN 10.

Switch(Config-If-Ethernet1/0/3)#dot1xguest-vlan 10

5.3.11 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

5.3.12 dot1x macbased guest-vlan

Command: dot1x macbased guest-vlan <vlanid>

no dot1x macbased guest-vlan

Function: Configure to appoint the port's guest-vlan based on the mac authentication; the no

command deletes this guest-vlan.
Parameters: <vlanid>: the configured vlan id, the range is from 1 to 4094.
Command mode: Port Mode.
Default: Do not configure 802.1x macbased guest-vlan.
Usage Guide: If there is no dedicated authentication client or the client version was too low, and it makes no clients authenticate successfully on the port in some time, then the access device will make this user join to the guest VLAN. User can get the 802.1x client software in guest VLAN, update the client or do other updating things (such as anti-virus software, system patches and etc.) When the user under the port in Guest VLAN issues the authentication, this port will be stay in guest VLAN if the authentication failed; if it was successful, there are two situations as below:
1. The authentication server issues an auto VLAN, in this time, the user left the guest VLAN and joined to the auto VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again.
2. The authentication server did not issue the VLAN, in this time, the user left the guest VLAN and joined to the configured native VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again.
Notice:
1. dot1x macbased guest-vlan can be configured only on the port based on mac authentication and in HYBRID mode.
2. Different macbased guestVLAN can be configured on different ports, but only one macbased guestVLAN can be configured on one port.
Example: Configure the guest-vlan of Ethernet1/0/3 as Vlan 10.
Switch(Config-If-Ethernet1/0/3)#dot1x macbased guest-vlan 10

5.3.13 dot1x macbased port-down-flush

Command: dot1x macbased port-down-flush
no dot1x macbased port-down-flush
Function: Enables this command, when the dot1x certification according to mac is down, delete the user who passed the certification of the port; The no command does not make the down operation.
Command mode: Global Mode
Default: The command is not enabled by default.
Usage Guide: When users who passed the certification according to mac changed among different ports, delete the user for the new certification. The command should be enable to delete the user.
Example: When the dot1x certification according to mac is down, delete the user who passed the certification of the port.
Switch(config)#dot1x macbased port-down-flush

5.3.14 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

5.3.15 dot1x user allow-movement

Command: dot1x user allow-movement

no dot1x user allow-movement

Function: Enable the authentication function after the user moves the port, the no command disables the function.

Command Mode: Global mode

Default: Disable the authentication function after the user moves the port.

Usage Guide: Enable the authentication function after the user moves the port, so the switch allows user to process this authentication. In the condition that the switch connects with hub, when the user will be moved to other port, dot1x user allow-movement command should be enabled.

Example: Enable the authentication function after the user moves the port.

Switch(config)#dot1x user allow-movement

5.3.16 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

5.3.17 free-resource destination

This command is not supported by the switch.

5.3.18 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 1/0/3 to allow 5 users.
Switch(Config-If-Ethernet1/0/3)#dot1x max-user macbased 5

5.3.19 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 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 1/0/3 to allow 5 users.
Switch(Config-If-Ethernet1/0/3)#dot1x max-user userbased 5

5.3.20 dot1x portbased mode single-mode

Command: dot1x portbased mode single-mode
no dot1x portbased mode single-mode

Function: Set the single-mode based on portbase authentication mode; the no command disables this function.
Parameters: None.
Command mode: Port Mode
Default: Disable the single-mode.
Usage Guide: This command takes effect when the access mode of the port is set as portbase only. Before configuring the single-mode, if the port has enabled dot1x port-method portbased command and exist online users, the switch will enforce all users of this port are offline. After that, this port only allows a user to pass the authentication, the user can access the specified network resource, but other authentication users of this port will be denied and can not access the network. After disabling the single-mode, the switch also enforce the authenticated user is offline.
Example:
Switch(Config-If-Ethernet1/0/1)#dot1x portbased mode single-mode

5.3.21 dot1x port-control

This command is not supported by the switch.

5.3.22 dot1x port-method

Command: dot1x port-method {macbased | portbased | userbased {standard | 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
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.
Notes: For standard control method based on user, the 802.1x free resource must be configured first, and it needs to be used with dot1x privateclient enable.
Example: To configure the access control method based on port for Etherent1/0/4.
Switch(Config-If-Ethernet1/0/4)#dot1x port-method portbased

5.3.23 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 Mode: 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. For detailed information, please refer to DCBI integrated solution. 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

5.3.24 dot1x privateclient protect enable

Command: dot1x privateclient protect enable
no dot1x privateclient protect enable
Function: Enable the privateclient protect function of the switch, the no command disables the protect function.
Parameter: None.
Command mode: Global Mode
Default: Disable the privateclient protect function.
Usage Guide: Support the partial encryption of the privateclient protocol to advance the security of the privateclient.
Example: Enable the privateclient protect function of the switch.
Switch(config)#dot1x privateclient protect enable

5.3.25 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 a 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 port1/0/8.
Switch(config)#dot1x re-authenticate interface ethernet 1/0/8

5.3.26 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

5.3.27 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

5.3.28 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

5.3.29 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

5.3.30 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 1/0/1.
Switch(config)#dot1x enable
Switch(config)# dot1x unicast enable
Switch(config)#interface ethernet1/0/1
Switch(Config-If-Ethernet1/0/1)#dot1x enable

5.3.31 dot1x web authentication enable

This command is not supported by switch.

5.3.32 dot1x web authentication ipv6 passthrough

Function This command is not supported by switch.

5.3.33 dot1x web redirect

This command is not supported by switch.

5.3.34 dot1x web redirect enable

This command is not supported by switch.

5.3.35 free-mac

This command is not supported by the switch.

5.3.36 show dot1x

Command**: show dot1x [interface <*interface-list*>]**

Function: Displays dot1x parameter related information, if parameter information is added, corresponding dot1x status for corresponding port is displayed.

Parameters: ***<interface-list>*** is the port list. If no parameter is specified, information for all ports is displayed.

Command mode: Admin and Configuration Mode.

Usage Guide: The dot1x related parameter and dot1x information can be displayed with 'show dot1x' command.

Example:

1. Display information about dot1x global parameter for the switch.

```
Switch#show dot1x
Global 802.1x Parameters
   reauth-enabled          no
   reauth-period           3600
   quiet-period            10
   tx-period               30
   max-req                 2
   authenticator mode      passive

Mac Filter Disable
MacAccessList :
dot1x-EAPoR Enable
dot1x-privateclient Disable
dot1x-unicast Disable


802.1x is enabled on ethernet Ethernet1/0/1
```

Authentication Method:Port based

Max User Number:1

Status	Authorized
Port-control	Auto
Supplicant	00-03-0F-FE-2E-D3

Authenticator State Machine

State	Authenticated

Backend State Machine

State	Idle

Reauthentication State Machine

State	Stop

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)
dot1x-privateclient	Whether the switch supports the privateclient
802.1x is enabled on ethernet Ethernet1/0/1	Indicates whether dot1x is enabled for the port
Authentication Method:	Port authentication method (MAC-based, port-based, user-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

5.3.37 show dot1x user

This command is not supported by the switch.

5.3.38 clear dot1x all

This command is not supported by the switch.

5.3.39 user-control limit ipv4

This command is not supported by the switch.

5.3.40 user-control limit ipv6

This command is not supported by the switch.

5.3.41 vlan-pool

This command is not supported by the switch.

5.4 The Number Limitation Function of MAC and IP in Port, VLAN

5.4.1 debug ip arp count

Command: debug ip arp count

no debug ip arp count

Function: When the number limitation function debug of ARP in the VLAN, if the number of dynamic ARP and the number of ARP in the VLAN is larger than the max number allowed, users will see debug information. "**no debug ip arp count**" command is used to disable the number limitation function debug of ARP in the VLAN.

Parameters: None.

Command Mode: Admin Mode.

Default Settings: None.

Usage Guide: Display the debug information of the number of dynamic ARP in the VLAN.

Examples:

Switch#debug vlan mac count

%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in vlan 1!!

%Jun 14 16:04:40 2007Arp learning will be stopped and some arp will be delete !!

5.4.2 debug ipv6 nd count

Command: debug ipv6 nd count

no debug ipv6 nd count

Function: When the number limitation function debug of neighbor in the VLAN, if the number of dynamic neighbor and the number of neighbor in the VLAN is larger than the max number allowed, users will see debug information. "**no debug ip neighbor count**" command is used to disable the number limitation function debug of neighbor in the VLAN.

Parameters: None.

Command Mode: Admin Mode.

Default Settings: None.

Usage Guide: Display the debug information of the number of dynamic neighbor in the VLAN.

Examples:

Switch#debug vlan mac count

%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in vlan 1!!

5.4.3 debug switchport arp count

Command: debug switchport arp count

no debug switchport arp count

Function: When the number limitation function debug of ARP on the port, if the number of dynamic ARP and the number of ARP on the port is larger than the max number allowed, users will see debug information. "**no debug switchport arp count**" command is used to disable the number limitation function debug of ARP on the port.

Parameters: None

Command Mode: Admin Mode

Default Settings: None

Usage Guide: Display the debug information of the number of dynamic ARP on the port.

Examples:

Switch#debug switchport arp count

%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in port Ethernet3/1

!!%Jun 14 16:04:40 2007 Arp learning will be stopped and some mac will be delete !!

5.4.4 debug switchport mac count

Command: debug switchport mac count

no debug switchport **mac count**

Function: When the number limitation function debug of MAC on the port, if the number of dynamic MAC and the number of MAC on the port is larger than the max number allowed, users will see debug information. 'no **debug switchport mac count'** command is used to disable the number limitation function debug of MAC on the port.

Parameters: None

Command Mode: Admin Mode
Default Settings: None
Usage Guide: Display the debug information of the number of dynamic MAC on the port.
Examples:
Switch#debug switchport mac count
%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maximum limit in port Ethernet3/1
!!%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delete !!

5.4.5 debug switchport nd count

Command: debug switchport nd count
no debug switchport nd count
Function: When the number limitation function debug of ND on the port, if the number of dynamic ND and the number of ND on the port is larger than the max number allowed, users will see debug information. "**no debug switchport nd count**" command is used to disable the number limitation function debug of ND on the port.
Parameters: None
Command Mode: Admin Mode
Default Settings: None
Usage Guide: Display the debug information of the number of dynamic ND on the port
Examples:
Switch#debug switchport arp count
%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in port Ethernet3/1
!!%Jun 14 16:04:40 2007 Neighbor learning will be stopped and some mac will be delete !!

5.4.6 debug vlan mac count

This command is not supported by the switch.

5.4.7 ip arp dynamic maximum

Command: ip arp dynamic maximum *<value>*
no ip arp dynamic maximum
Function: Set the max number of dynamic ARP allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic ARP in the VLAN; "**no ip arp dynamic maximum**" command is used to disable the number limitation function of dynamic ARP in the VLAN.
Parameters: *<value>* upper limit of the number of dynamic ARP in the VLAN, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic ARP in the VLAN is disabled.
Command Mode: Interface Configuration Mode.
Usage Guide: When configuring the max number of dynamic ARP allowed in the VLAN, if the number of dynamically learnt ARP in the VLAN is already larger than the max number to be set, the extra dynamic ARP will be deleted.
Examples:
Enable the number limitation function of dynamic ARP in VLAN 1, the max number to be set is 50.
Switch(config)#interface ethernet
Switch(Config-if-Vlan1)# ip arp dynamic maximum 50
Disable the number limitation function of dynamic ARP in VLAN 1.
Switch(Config-if-Vlan1)#no ip arp dynamic maximum

5.4.8 ipv6 nd dynamic maximum

Command: ipv6 nd dynamic maximum *<value>*
no ipv6 nd dynamic maximum
Function: Set the max number of dynamic NEIGHBOR allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic NEIGHBOR in the VLAN; "**no ipv6 nd dynamic maximum**" command is used to disable the number limitation function of dynamic NEIGHBOR in the VLAN.
Parameters: *<value>* upper limit of the number of dynamic NEIGHBOR in the VLAN, ranging from 1 to 4096.
Default Settings: The number limitation function of dynamic NEIGHBOR in the VLAN is disabled.
Command Mode: Interface Configuration Mode.
Usage Guide: When configuring the max number of dynamic NEIGHBOR allowed in the VLAN, if the number of dynamically learnt NEIGHBOR in the VLAN is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted.
Examples:
Enable the number limitation function of dynamic NEIGHBOR in VLAN 1, the max number to be set is 50.
Switch(config)#interface ethernet
Switch(Config-if-Vlan1)# ipv6 nd dynamic maximum 50
Disable the number limitation function of dynamic NEIGHBOR in VLAN 1.
Switch(Config-if-Vlan1)#no ipv6 nd dynamic maximum

5.4.9 mac-address query timeout

This command is not supported by the switch.

5.4.10 show arp-dynamic count

Command: show arp-dynamic count {(vlan <1-4096>)| interface ethernet *<portName>*}

Function: Display the number of dynamic ARP of corresponding port and VLAN.

Parameters: <*vlan-id*> is the specified vlan ID.

<portName> is the name of layer-2 port.

Command Mode: Admin and Configuration Mode.

Usage Guide: Use this command to display the number of dynamic ARP of corresponding port and VLAN.

Examples: Display the number of dynamic ARP of the port and VLAN which are configured with number limitation function of ARP.

Switch(config)# show arp-dynamic count interface ethernet 1/0/3

Port	MaxCount	CurrentCount
Ethernet1/0/3	5	1

Switch(config)# show arp-dynamic count vlan 1

Vlan	MaxCount	CurrentCount
1	55	15

5.4.11 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 1/0/3

Port	MaxCount	CurrentCount
Ethernet1/0/3	5	1

Switch(config)# show mac-address dynamic count vlan 1

Vlan	MaxCount	CurrentCount
1	55	15

5.4.12 show nd-dynamic count

Command: show nd-dynamic count {(vlan <1-4096>)| interface ethernet *<portName>*}

Function: Display the number of dynamic ND of corresponding port and VLAN.

Parameters: *<vlan-id>* is play the specified vlan ID. ***<portName>*** is the name of layer-2 port.

Command Mode: Admin and Configuration Mode.

Usage Guide: Use this command to display the number of dynamic ND of corresponding port and VLAN.

Examples: Display the number of dynamic ND of the port and VLAN which are configured with number limitation function of ND.

Switch(config)# show nd-dynamic count interface ethernet 1/0/3

Port	MaxCount	CurrentCount
Ethernet1/0/3	5	1

Switch(config)# show nd-dynamic count vlan 1

Vlan	MaxCount	CurrentCount
1	55	15

5.4.13 switchport arp dynamic maximum

Command: switchport arp dynamic maximum *<value>*

no switchport arp dynamic maximum

Function: Set the max number of dynamic ARP allowed by the port, and, at the same time, enable the number limitation function of dynamic ARP on the port; "**no switchport arp dynamic maximum**" command is used to disable the number limitation function of dynamic ARP on the port.

Parameters: *<value>* upper limit of the number of dynamic ARP of the port, ranging from 1 to 4096.

Default Settings: The number limitation function of dynamic ARP on the port is disabled.

Command Mode: Port mode.

Usage Guide: When configuring the max number of dynamic ARP allowed by the port, if the number of dynamically learnt ARP on the port is already larger than the max number to be set, the extra dynamic ARP will be deleted. TRUNK ports do not supports this function.

Examples:

Enable the number limitation function of dynamic ARP in port 1/0/2 mode, the max number to be set is 20

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)# switchport arp dynamic maximum 20

Disable the number limitation function of dynamic ARP in port 1/0/2 mode

Switch(Config-If-Ethernet1/0/2)#no switchport arp dynamic maximum

5.4.14 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 1/0/2 mode, the max number to be set is 20

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)# switchport mac-address dynamic maximum 20

Disable the number limitation function of dynamic MAC address in port 1/0/2 mode

Switch(Config-If-Ethernet1/0/2)#no switchport mac-address dynamic maximum

5.4.15 switchport mac-address violation

Command: switchport mac-address violation {protect | shutdown} [recovery <5-3600>]

no switchport mac-address violation

Function: Set the violation mode of the port, the no command restores the violation mode to protect.

Parameters: protect: protect mode

shutdown: shutdown mode

recovery: Configure the border port to automatically restore after execute shutdown violation mode

<5-3600>: Recovery time, do not restore by default

Command Mode: Port mode

Default: protect mode

Usage Guide: The port sets the violation mode after enable the number limit function of MAC only. If the violation mode is protect, the port only disable the dynamic MAC address learning function when the MAC address number of the port exceeds the upper limit of secure MAC. If

the violation mode is shutdown, the port will be disabled when the MAC address number exceeds the upper limit of secure MAC, and the user can enable the port by configuring no shutdown command manually or the automatic recovery timeout.
Example: Set the violation mode as shutdown, the recovery time as 60s for port1.
Switch(config)#interface Ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#switchport mac-address violation shutdown recovery 60

5.4.16 switchport nd dynamic maximum

Command: switchport nd dynamic maximum *<value>*
no switchport nd dynamic maximum
Function: Set the max number of dynamic NEIGHBOR allowed by the port, and, at the same time, enable the number limitation function of dynamic NEIGHBOR on the port; "**no switchport nd dynamic maximum**" command is used to disable the number limitation function of dynamic NEIGHBOR on the port.
Parameters: *<value>* upper limit of the number of dynamic NEIGHBOR of the port, ranging from 1 to 4096.
Default Settings: The number limitation function of dynamic ARP on the port is disabled.
Command Mode: Port mode.
Usage Guide: When configuring the max number of dynamic NEIGHBOR allowed by the port, if the number of dynamically learnt NEIGHBOR on the port is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted. TRUNK ports do not supports this function.
Examples:
Enable the number limitation function of dynamic NEIGHBOR in port 1/0/2 mode, the max number to be 20.
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)# switchport nd dynamic maximum 20
Disable the number limitation function of dynamic NEIGHBOR in port 1/0/2 mode
Switch(Config-If-Ethernet1/0/2)#no switchport nd dynamic maximum

5.4.17 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

5.5 AM

5.5.1 am enable

Command: am enable

no am enable

Function: Globally enable/disable AM function.

Parameters: None.

Default: AM function is disabled by default.

Command Mode: Global Mode.

Usage Guide: None.

Example: Enable AM function on the switch.

Switch(config)#am enable

Disable AM function on the switch.

Switch(config)#no am enable

5.5.2 am port

Command: am iport

no am port

Function: Enable/disable AM function on port.

Parameters: None.

Default: AM function is disabled on all port.

Command Mode: Port Mode.

Example: Enable AM function on interface 1/0/3 of the switch.

Switch(Config-If-Ethernet 1/0/3)#am port

Disable AM function on interface 1/0/3 of the switch.
Switch(Config-If-Ethernet 1/0/3)#no am port

5.5.3 am ip-pool

Command: am ip-pool <*ip-address*> <*num*>

no am ip-pool <*ip-address*> <*num*>

Function: Set the AM IP segment of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.

Parameters: ***<ip-address>*** the starting address of an address segment in the IP address pool; ***<num>*** is the number of consecutive addresses following ip-address, less than or equal with 32.

Default: IP address pool is empty.

Command Mode: Port Mode.

Usage Guide: None.

Example: Configure that interface 1/0/3 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 1/0/3)#am ip-pool 10.10.10.1 10

5.5.4 am mac-ip-pool

Command: am mac-ip-pool <*mac-address*> <*ip-address*>

no am mac-ip-pool <*mac-address*> <*ip-address*>

Function: Set the AM MAC-IP address of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.

Parameter: ***<mac-address>*** is the source MAC address; ***<ip-address>*** is the source IP address of the packets, which is a 32 bit binary number represented in four decimal numbers.

Default: MAC-IP address pool is empty.

Command Mode: Port Mode.

Usage Guide: None.

Example: Configure that the interface 1/0/3 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-Ethernet1/0/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1

5.5.5 no am all

Command: no am all [ip-pool | mac-ip-pool]

Function: Delete MAC-IP address pool or IP address pool or both pools configured by all users.

Parameters: ip-pool is the IP address pool; **mac-ip-pool** is the MAC-IP address pool; no parameter means both address pools.

Default: Both address pools are empty at the beginning.

Command Mode: Global Mode

Usage Guide: None.

Example: Delete all configured IP address pools.

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

5.5.6 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 Ethernet1/0/3
am interface
am ip-pool 30.10.10.1 20
Interface Ethernet1/0/5
am port
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 Ethernet1/0/6
am port
Interface Ethernet1/0/1
am interface
am ip-pool 10.10.10.1 20
am ip-pool 10.20.10.1 20

Display the AM configuration entries of ehternet1/0/5 of the switch.

Switch#show am interface ethernet 1/0/5
AM is enabled

Interface Etherne1/0/5
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

5.6 Security Feature

5.6.1 dosattack-check srcip-equal-dstip enable

Command: [no] dosattack-check srcip-equal-dstip enable

Function: Enable the function by which the switch checks if the source IP address is equal to the destination IP address; the “no” form of this command disables this function.

Parameter: None

Default: Disable the function by which the switch checks if the source IP address is equal to the destination IP address.

Command Mode: Global Mode

Usage Guide: By enabling this function, data packet whose source IP address is equal to its destination address will be dropped.

Example: Drop the data packet whose source IP address is equal to its destination address.l

Switch(config)# dosattack-check srcip-equal-dstip enable

5.6.2 dosattack-check ipv4-first-fragment enable

This command is not supported by the switch.

5.6.3 dosattack-check tcp-flags enable

Command: [no] dosattack-check tcp-flags enable

Function: Enable the function by which the switch will check the unauthorized TCP label function; the “no” form of this command will disable this function.

Parameter: None

Default: This function disable on the switch by default

Command Mode: Global Mode

Usage Guide: With this function enabled, the switch will be able to drop follow four data packets containing unauthorized TCP label: SYN=1 while source port is smaller than 1024;TCP label positions are all 0 while its serial No. =0;FIN=1,URG=1,PSH=1 and the TCP serial No.=0;SYN=1 and FIN=1. This function can be used associating the “dosattack-check ipv4-first-fragment enable” command.

Example: Drop one or more types of above four packet types.

Switch(config)#dosattack-check tcp-flags enable

5.6.4 dosattack-check srcport-equal-dstport enable

Command: dosattack-check srcport-equal-dstport enable

no 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 command disables this function.

Parameter: None
Default: Disable the function by which the switch will check if the source port is equal to the destination port.
Command Mode: Global Mode
Usage Guide: With this function enabled, the switch will be able to drop TCP and UDP data packet whose destination port is equal to the source port. This function can be used associating the "dosattack-check ipv4-first-fragment enable" function so to block the IPv4 fragment TCP and UDP data packet whose destination port is equal to the source port.
Example: Drop the non-fragment TCP and UDP data packet whose destination port is equal to the source port.
Switch(config)#dosattack-check srcport-equal-dstport enable

5.6.5 dosattack-check tcp-fragment enable

This command is not supported by the switch.

5.6.6 dosattack-check tcp-segment

This command is not supported by the switch.

5.6.7 dosattack-check icmp-attacking enable

Command: [no] dosattack-check icmp-attacking enable
Function: Enable the ICMP fragment attack checking function on the switch; the "no" form of this command disables this function.
Parameter: None
Default: Disable the ICMP fragment attack checking function on the switch
Command Mode: Global Mode
Usage Guide: With this function enabled the switch will be protected from the ICMP fragment attacks, dropping the fragment ICMPv4/v6 data packets whose net length is smaller than the specified value.
Example: Enable the ICMP fragment attack checking function.
Switch(config)#dosattack-check icmp-attacking enable

5.6.8 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

5.6.9 dosattack-check icmpv6-size

This command is not supported by the switch.

5.7 TACACS+

5.7.1 tacacs-server authentication host

Command: tacacs-server authentication host <*ip-address*> [port <*port-number*>] [timeout <*seconds*>] [key {0 | 7} <*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; ***<string>*** is the key string, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 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

5.7.2 tacacs-server key

Command: tacacs-server key {0 | 7} *<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 key string of the TACACS+ server. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 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 0 test

5.7.3 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

5.7.4 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

5.7.5 debug tacacs-server

Command: debug tacacs-server

no debug tacacs-server

Function: Open the debug message of the TACACS+; the "**no debug tacacs-server**" command closes the TACACS+ debugging messages.

Command Mode: Admin Mode

Parameter: None.

Usage Guide: Enable the TACACS+ debugging messages to check the negotiation process of the TACACS+ protocol which can help detecting the failure.

Example: Enable the debugging messages of the TACACS+ protocol.

Switch#debug tacacs-server

5.8 RADIUS

5.8.1 aaa enable

Command: aaa enable

no aaa enable

Function: Enables the AAA authentication function in the switch; the "no AAA enable" command disables the AAA authentication function.

Command mode: Global Mode.

Parameters: No.

Default: AAA authentication is not enabled by default.

Usage Guide: The AAA authentication for the switch must be enabled first to enable IEEE 802.1x authentication for the switch.

Example: Enabling AAA function for the switch.

Switch(config)#aaa enable

5.8.2 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

5.8.3 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

5.8.4 aaa group server radius

This command is not supported by the switch.

5.8.5 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 interface1/0/1.

Switch#debug aaa packet all interface Ethernet 1/0/1

5.8.6 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 1/0/1.

Switch#debug aaa detail attribute interface Ethernet 1/0/1

5.8.7 debug aaa detail connection

Command: debug aaa detail connection

no debug aaa detail connection

Function: Enable the debug information of aaa about connection details; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of aaa about connection details, users can check connection details of aaa, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of aaa about connection details.

Switch#debug aaa detail connection

5.8.8 debug aaa detail escape

This command is not supported by the switch.

5.8.9 debug aaa detail event

Command: debug aaa detail event

no debug detail event

Function: Enable the debug information of aaa about events; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of aaa about events, users can check the information of all kinds of event generated in the operation process of Radius protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of aaa about events.

Switch#debug aaa detail event

5.8.10 debug aaa error

Command: debug aaa error

no debug error

Function: Enable the debug information of aaa about errors; the no operation of this command will disable that debug information.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: By enabling the debug information of aaa about errors, users can check the information of all kinds of errors that occurs in the operation process of Radius protocol, which might help diagnose the cause of faults if there is any.

Example: Enable the debug information of aaa about errors.

Switch#debug aaa error

5.8.11 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

5.8.12 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 command deletes the configuration.

Parameter: ***<ipv6-address>*** is the source IPv6 address of the RADIUS packet, it must 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

5.8.13 radius-server accounting host

Command: radius-server accounting host {<*ipv4-address*> | <*ipv6-address*>} [port <*port-number*>] [key {0 | 7} <*string*>] [primary]

no radius-server accounting host {<*ipv4-address*> | <*ipv6-address*>}

Function: Specifies the IPv4/IPv6 address and the port number, whether be primary server 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;

<string> is the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters;

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. It only configures a RADIUS primary server whether the server use IPv4 address or IPv6 address.

Example: Sets the RADIUS accounting server of IPv6 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

5.8.14 radius-server authentication host

Command: radius-server authentication host {*<ipv4-address>* | *<ipv6-address>*} [port <port-number>] [key *{0* | 7} <string>] [primary] [access-mode {dot1x | telnet}]

no radius-server authentication host {*<ipv4-address>* | *<ipv6-address>*}

Function: Specifies the IPv4 address or IPv6 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 the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters;

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 address or 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

5.8.15 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

5.8.16 radius-server key

Command: radius-server key {0 | 7} <*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, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters.

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 0 test

5.8.17 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

5.8.18 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

5.8.19 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 8-1 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

5.8.20 server

This command is not supported by the switch.

5.8.21 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 ----------

5.8.22 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 ----------

5.8.23 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

5.8.24 show radius authenticated-user count

Command: show radius authenticated-user count

Function: Show the number of on-line users who have already passed the authentication.

Parameter: None.

Command mode: Admin and configuration mode

Default: None.

Usage guide: None.

Example:

Switch#show radius authenticated-user count

The authenticated online user num is: 105

5.8.25 show radius authenticating-user count

Command: show radius authenticating-user count

Function: Show the number of the authenticating-user.

Parameter: None.

Command mode: Admin and configuration mode.

Default: None.

Usage Guide: None.

Example:

Switch#show radius authenticating-user count

The authenticating user num is: 10

5.8.26 show radius count

This command is not supported by the switch.

5.8.27 Radius Escaping

5.8.27.1 radius-server escape { enable | disable}

Command: radius-server escape enable
radius-server escape disable
Function: Enable the AAA radius server escaping function.
Parameters: None.
Default: Disable.
Command Mode: Global Mode.
Usage Guide: After enabled the radius server escaping function, the flow of dot1x or portal authentication client can be allowed when the configured radius server on them is inaccessible. When the configured authentication server is accessible again, the flow allowing rule will be deleted.
Example: Enable the global authentication function.
Switch (Config)# radius-server escape enable

5.8.27.2 radius-server escape detection-interval

Command: radius-server escape detection-interval {default| < second >)}
Function: Configure the detection interval of radius server escaping.
Parameters: default: the default interval is 3 minutes.
second: the interval whose range is 1-1800 seconds.
Default: 180s.
Command Mode: Global Mode.
Usage Guide: The shorter the configured interval is, the radius server escaping function is more flexible. The configured interval should be longer than (Retransmit+1)* Time Out.
Example: Configure the detection interval of radius server escaping as 120s.
Switch(config)#radius-server escape detection-interval 120

5.9 SSL

5.9.1 ip http secure-server

Command: ip http secure-server
no ip http secure-server
Function: Enable/disable SSL function.
Parameter: None.
Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used for enable and disable SSL function. After enable SSL function, the users visit the switch through https client, switch and client use SSL connect, can form safety SSL connect channel. After that, all the data which transmit of the application layer will be encrypted, then ensure the privacy of the communication.

Example: Enable SSL function.

Switch(config)#ip http secure-server

5.9.2 ip http secure-port

Command: ip http secure-port *<port-number>*

no ip http secure-port

Function: Configure/delete port number by SSL used.

Parameter: *<port-number>* means configured port number, range between 1025 and 65535. 443 is for default.

Command Mode: Global Mode.

Default: Not configure.

Usage Guide: If this command is used to configure the port number, then the configured port number is used to monitor. If the port number for https is changed, when users try to use https to connect, must use the changed one. For example: https://device:port_number. SSL function must reboot after every change.

Example: Configure the port number is 1028.

Switch(config)#ip http secure-port 1028

5.9.3 ip http secure- ciphersuite

Command: ip http secure-ciphersuite {des-cbc3-sha|rc4-128-sha| des-cbc-sha}

no ip http secure-ciphersuite

Function: Configure/delete secure cipher suite by SSL used.

Parameter: des-cbc3-sha encrypted algorithm DES_CBC3, summary algorithm SHA.

rc4-128-sha encrypted algorithm RC4_128, summary algorithm SHA.

des-cbc-sha encrypted algorithm DES_CBC, summary algorithm SHA.

default use is **rc4-md5**.

Command Mode: Global Mode.

Default: Not configure.

Usage Guide: If this command is used to configure the secure cipher suite, specified encryption method will be used. The SSL should be restarted to take effect after changes on configuration. When des-cbc-sha is configured, IE 7.0 or above is required.

Example: Configure the secure cipher suite is rc4-128-sha.

Switch(config)# ip http secure- ciphersuite rc4-128-sha

5.9.4 show ip http secure-server status

Command: show ip http secure-server status

Function: Show the status for the configured SSL.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

Switch# show ip http secure-server status

HTTP secure server status: Enabled

HTTP secure server port: 1028

HTTP secure server ciphersuite: rc4-128-sha

5.9.5 debug ssl

Command: debug ssl

no debug ssl

Function: Show the configured SSL information, the no command closes the DEBUG.

Parameter: None.

Command Mode: Admin Mode.

Example:

Switch# debug ssl

%Jan 01 01:02:05 2006 ssl will to connect to web server 127.0.0.1:9998

%Jan 01 01:02:05 2006 connect to http security server success!

5.10 VLAN-ACL

5.10.1 clear vacl statistic vlan

Command: clear vacl [in | out] statistic vlan [<*1-4094*>]

Function: This command can clear the statistic information of VACL.

Parameter: in | out: Clear the traffic statistic of the ingress/egress.

vlan <*1-4094*>: The VLAN which needs to clear the VACL statistic information. If do not input VLAN ID, then clear all VLAN statistic information.

Command mode: Admin Mode.

Default: None.

Usage Guide: Egress direction filtering is not supported by switch.

Example:

Clear VACL statistic information of Vlan1.

Switch#clear vacl statistic vlan 1

5.10.2 show vacl vlan

Command: show vacl [in | out] vlan [<*1-4094*>] | [begin | include | exclude <*regular-expression*>]

Function: This command shows the configuration and the statistic information of VACL.

Parameter: in | out: Show ingress/egress configuration and statistic

vlan <*1-4094*>: The VLAN which needs to show the configuration and the statistic information of VACL. If do not input VLAN ID, then show VACL configuration and statistic information of all VLANs.

begin | include | exclude <*regular-expression*>: the regular expression

. match any characters except the line feed character

^ match the beginning of the row

$ match the end of the row

| match the character string at the left or right of upright line

[0-9] match the number 0 to the number 9

[a-z] match the lowercase a to z

[aeiou] match any letter in “aeiou”

\ Escape Character is used to match the intervocalic character, for example, \$ will match the $ character, but it is not match the end of the character string

\w match the letter, the number or the underline

\b match the beginning or the end of the words

\W match any characters which are not alphabet letter, number and underline

\B match the locations which are not the begin or end of the word

[^x] match any characters except x

[^aeiou] match any characters except including aeiou letters

* repeat zero time or many times

+ repeat one time or many times

(n) repeat n times

(n,) repeat n or more times

(n, m) repeat n to m times

At present, the regular expression used does not support the following syntaxes:

\s match the blank character

\d match the number

\S match any characters except blank character

\D match non-number character

? repeat zero time or one time

Command mode: Admin Mode.

Default: None.

Usage Guide: Egress direction filtering is not supported by switch..

Example:

Switch (config)#show vacl vlan 2

Vlan 2:

IP Ingress access-list used is 100, traffic-statistics Disable.
Switch (config)# show vacl vlan 3
Vlan 3:
IP Ingress access-list used is myacl, packet(s) number is 5.

Displayed Information	Explanation
Vlan 2	The name of VLAN
100, myacl	The name of VACL
traffic-statistics Disable	Disable VACL statistic function
packet(s) number is 5	The sum of out-profile data packets matching this VACL

5.10.3 vacl ip access-group

Command: vacl ip access-group {<1-299> | WORD} {in | out} [traffic-statistic] vlan WORD
no vacl ip access-group {<1-299> | WORD} {in | out} vlan WORD
Function: This command configure VACL of IP type on the specific VLAN.
Parameter: <1-299> | WORD: Configure the numeric IP ACL (include: standard ACL rule <1-99>, extended ACL rule <100-299>) or the named ACL.
in | out: Filter the ingress/egress traffic.
traffic-statistic: Enable the statistic of matched packets number.
vlan WORD: The VLAN will be bound to VACL.
Command mode: Global Mode.
Default: None.
Usage **Guide:** Use ';' or '-' to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch.
Example: Configure the numeric IP ACL and enable the statistic function for Vlan 1-5, 6, 7-9.
Switch(config)#vacl ip access-group 1 in traffic-statistic vlan 1-5; 6; 7-9

5.10.4 vacl ipv6 access-group

Command**: vacl ipv6 access-group (<500-699> | WORD) {in } (traffic-statistic|) vlan WORD**
no ipv6 access-group {<500-699> | WORD} {in } vlan WORD
Function: This command configure VACL of IPv6 on the specific VLAN.
Parameter: <500-699> | WORD: Configure the IPv6 numeric standard ACL or IPV6 standard ACL rule.
inFilter the ingress traffic.
traffic-statistic: Enable the statistic of matched packets number.
vlan WORD: The VLAN will be bound to VACL.
Command mode: Global Mode.
Default: None.
Usage Guide: Use ';' or '-' to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering and extended IPv6 is not supported by switch.
Example: Configure the numeric IPv6 ACL for Vlan 5.

Function Switch(config)#vacl ipv6 access-group 600 in traffic-statistic vlan 5

5.10.5 vacl mac access-group

Command: vacl mac access-group {<700-1199> | WORD} {in } [traffic-statistic] vlan WORD
no vacl mac access-group {<700-1199> | WORD} {in } vlan WORD
Function: This command configure VACL of MAC type on the specific VLAN.
Parameter: <700-1199> | WORD: Configure the numeric IP ACL (include: <700-799> MAC standard access list, <1100-1199> MAC extended access list) or the named ACL.
in: Filter the ingress traffic.
traffic-statistic: Enable the statistic of matched packets number.
vlan WORD: The VLAN will be bound to VACL.
Command mode: Global Mode.
Default: None.
Usage Guide: Use ';' or '-' to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch.
Example: Configure the numeric MAC ACL for Vlan 1-5.
Switch(config)#vacl mac access-group 700 in traffic-statistic vlan 1-5

5.10.6 vacl mac-ip access-group

Command: vacl mac-ip access-group {<3100-3299> | WORD} {in } [traffic-statistic] vlan WORD
no vacl mac-ip access-group {<3100-3299> | WORD} {in } vlan WORD
Function: This command configure VACL of MAC-IP type on the specific VLAN.
Parameter: <3100-3299> | WORD: Configure the numeric MAC-IP ACL or the named ACL.
in: Filter the ingress traffic.
traffic-statistic: Enable the statistic of matched packets number.
vlan WORD: The VLAN will be bound to VACL.
Command mode: Global Mode.
Default: None.
Usage Guide: Use ';' or '-' to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch.
Example: Configure the numeric MAC-IP ACL for Vlan 1, 2, 5.
Switch(config)#vacl mac-ip access-group 3100 in traffic-statistic vlan 1;2;5

5.11 Captive Portal Authentication

5.11.1 Authentication

5.11.1.1 ac-name

Command: ac-name <word>

no ac-name

Function: Configure the parameter of acname in the redirect url. The no command deletes it.

Parameters: <word>, it is the value of acname including 32 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guide: This command is used to configure the parameter of acname in the redirect url. Some portal servers can pass the authentication only with the specific ac-name. So this command should be configured according to the requirement of the portal server.

Example: Configure the ac-name in the redirect url as 0100.0010.010.00 according to the standard of the mobile portal server, and the format is ACN.CTY.PRO.OPE.

Switch(config-cp-instance)#ac-name 0100.0010.010.00

5.11.1.2 authentication roam enable

Command: authentication roam enable <vlan WORD>

no authentication roam enable <vlan WORD>

Function: Enable the user roaming function. The no command disables this function.

Parameters: vlan WORD: the specific vlan is allowed roaming.

Command Mode: captive portal configuration mode.

Default: Disable.

Usage Guide: After enabled this function, the user is allowed roaming. When a user roams from one port to another (the same VLAN), the roaming will be triggered. User can visit the network resources without reauthentication. After disabled this function, the user is not allowed roaming. When a user roams from one port to another, the reauthentication is needed for visiting the network resources.

Example: Enable the roaming function of vlan10.

Switch (config-cp)#authentication roam enable vlan 10

5.11.1.3 captive-portal

Command: captive-portal

Function: Use this command to enter Captive Portal configuration mode.

Parameter: None.

Default: None.

Command Mode: Global configuration mode.

Usage Guide: Use this command to enter Captive Portal configuration mode.

Example: Enter into the global configuration mode for configuring.

Switch(config)#captive-portal

5.11.1.4 captive-portal binding arp (it is not supported currently)

Command: captive-portal binding arp

no captive-portal binding arp

Function: After enabled static arp binding function, a static arp will be bound for the user after the successful authentication. After user is down line, delete the bound static arp. The no command deletes the bound static arp and it will not be bound after the user is on line.

Parameters: None.

Default: None.

Command Mode: captive portal mode.

Usage Guide: Enter into the captive portal mode by using this command.

Example: Enter into the captive portal mode and configure it.

Switch (config)# captive-portal binding arp

5.11.1.5 captive-portal client deauthenticate

Command: captive-portal client deauthenticate {*<1-10>* / *<FF-FF-FF-FF-FF-FF>* { ipv4 | ipv6} *<ip-addr>*}

Function: Deauthenticate the specific Captive Portal client.

Parameters: *<1-10>* is the ID of Captive Portal;

<FF-FF-FF-FF-FF-FF> is the MAC address of client;

ipv4 is the ipv4 address of user;

ipv6 is the ipv6 address of user;

<ip-addr> is the user address, ipv4 address is dotted decimal format, ipv6 address is the format of X:X::X:X.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Deauthenticate the specific Captive Portal client with the specific MAC address, it can also deauthenticate all the users or a single user under the specific captive portal configuration. When there is no parameters, deauthenticate all users.

Example: Deauthenticate the specific Captive Portal client

Switch #captive-portal client deauthenticate (force all the portal users on this controller get down the line)

The specified clients will be deauthenticated. Are you sure you want to deauthenticated clients? [Y/N]

Switch #captive-portal client deauthenticate 1 (force all the users of instance 1 get down the line)

Switch #captive-portal client deauthenticate 34-08-04-30-07-ca ipv4 100.1.1.1 (force one user get down the line)

5.11.1.6 captive-portal client re-auth log { enable | disable }

Command: captive-portal client re-auth log enable
captive-portal client re-auth log disable
Function: When the port, vlan or mac of the user is changed and it needs the reauthentication, the command of show logging buffer can record the log. The no command means not to record the log when reauthenticating.
Parameters: None.
Default: Disable.
Command Mode: captive portal mode.
Usage Guide: When the port, vlan or mac of the user is changed and it needs the reauthentication, the command of show logging buffer can record the log.
Example: Switch (config-cp)# captive-portal client re-auth log enable

5.11.1.7 captive-portal client keep-alive flow-detection enable

Command: captive-portal client keep-alive flow-detection enable
no captive-portal client keep-alive flow-detection enable
Function: Enable the keep-alive function of user. The no command disables this function.
Parameters: None.
Default: Disable.
Command Mode: captive portal mode.
Usage Guide: After enabled this function, it can keep alive for the user when the user is on line.
Example: Enter into the captive portal mode and configure it.
Switch (config-cp)#captive-portal client keep-alive flow-detection enable

5.11.1.8 captive-portal client keep-alive flow-detection interval

Command: captive-portal client keep-alive flow-detection interval <3-120>
no captive-portal client keep-alive flow-detection interval
Function: Configure the inquiring interval of user keep-alive. The no command configures the interval to be the default value.
Parameters: <3-120>: the range is 3-120 minutes.
Default: 5 minutes.
Command Mode: captive portal mode.
Usage Guide: After configured this command, the keep-alive timer inquires the user online status every once in a interval.
Example: Enter into the captive portal mode and configure it.
Switch (config-cp)# captive-portal client keep-alive flow-detection interval 3

5.11.1.9 captive-portal client keep-alive flow-detection number

Command: captive-portal client keep-alive flow-detection number <1-10>
no captive-portal client keep-alive flow-detection number
Function: Configure the times of continuous failed query that the keep-alive timer is allowed. The

no command configures it to be the default value.
Parameters: <1-10>: the range is from 1 to 10.
Default: 3 times.
Command Mode: captive portal mode.
Usage Guide: After configured this command, the keep-alive timer can inquire the user online status for configured times, if the user is no online always, it judges the user is down the line. Otherwise, the user is online once in the times of query, it judges the user is online. The times will be configured again.
Example: Enter into the captive portal mode and configure it.
Switch (config-cp)# captive-portal client keep-alive flow-detection interval 3

5.11.1.10 clear

Command: clear
Function: This command sets the configuration of the instance to be the default value.
Parameter: None.
Default: None.
Command Mode: Captive Portal Instance configuration mode.
Usage Guide: Set the configuration of the portal instance to be the default value.
Example: Set the configuration of the instance to be the default value.
Switch(config-cp-instance)# clear

5.11.1.11 configuration

Command: configuration *<cp-id>*
no configuration *<cp-id>*
Function: Use this command to enter Captive Portal instances Mode. The no command will delete the Portal Captive instance configuration..
Parameter: *<cp-id>* is the number of Captive Portal instances, range is 1 to 10.
Default: None.
Command Mode: Captive Portal global configuration mode.
Usage Guide: This configuration is used to configure Captive Portal instances. Each instance represents a class of users, users under the same instance have the same flow and rate configuration, etc., and vice versa. No command will delete a captive portal configuration. If there is an interface associated with a instance, then the no command will be invalid.
Example: Set the ID parameter as 4.
Switch(config-cp)#configuration 4

5.11.1.12 debug captive-portal packet

Command: debug captive-portal packet {send|receive|all}
no debug captive-portal packet {send|receive|all}
Function: Enable the packet debugging on-off of the captive portal authentication. The no

command disables it.

Parameters: send: enables the debugging information of sending packet of captive portal;

receive: enables the debugging information of receiving packet of captive portal;

all: enables the debugging information of sending, receiving and dumping packet of captive portal.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the packet debugging on-off of the captive portal authentication.

Example: Enable all the packets debugging information of the captive portal authentication.

Switch#debug captive-portal packet all

5.11.1.13 debug captive-portal trace

Command: debug captive-portal trace

no debug captive-portal trace

Function: Enable the tracing debugging of the captive portal authentication. The no command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the tracing debugging of the captive portal authentication.

Example: Enable the tracing debugging of the captive portal authentication.

Switch#debug captive-portal trace

5.11.1.14 debug captive-portal alive-detail

Command: debug captive-portal alive-detail

no debug captive-portal alive-detail

Function: It is the detailed debug information of portal authentication keep-alive.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Example: Switch#debug captive-portal alive-detail

5.11.1.15 debug captive-portal alive-status

Command: debug captive-portal alive-status

no debug captive-portal alive-status

Function: It is the debug information of portal authentication keep-alive status.

Parameters: None.

Default: None.

Function

Command Mode: Admin Mode.

Example: Switch#debug captive-portal alive-status

5.11.1.16 debug captive-portal alive-time

Command: debug captive-portal alive-time

no debug captive-portal alive-time

Function: It is the debug information of portal authentication keep-alive time.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Example: Switch#debug captive-portal alive-time

5.11.1.17 debug captive-portal error

Command: debug captive-portal error

no debug captive-portal error

Function: Enable the error debugging of the captive portal authentication. The no command disables it.

Parameters: None.

Command Mode: Admin Mode.

Default: Disable.

Usage Guide: This command is used to enable the error debugging of the captive portal authentication.

Example: Enable the error debugging of the captive portal authentication.

Switch#debug captive-portal error

5.11.1.18 enable (global)

Command: enable

disable

Function: Use this command to enable the Captive Portal function of the controller globally, use disable function to disable the Captive Portal function of the controller globally.

Parameter: None.

Default: Disable.

Command Mode: Captive Portal global configuration mode.

Usage Guide: Use this command to enable global Captive Portal characteristics on the controller.

Example: Enable the global Captive Portal function on the controller.

Switch(config-cp)#enable

5.11.1.19 enable (instance)

Command: enable

disable

Function: Enable Captive Portal configuration.

Parameter: None.

Default: Enable Captive Portal configuration.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: disable command will disable the captive-portal function, after disabling this command, the portal users will be forced offline.

Example: Enable captive-portal function.

Switch(config-cp-instance)#enable

5.11.1.20 external portal-server server-name

Command: external portal-server server-name <*name*> {ipv4 | ipv6} <*ipaddr*> [port <*1-65535*>]

no external portal-server {ipv4 | ipv6}server-name <*name*>

Function: Configure the external portal server. Launch the redirect page through this server, after inputting the correct user name and password, the authentication is successful and the client can access the outside network.

Parameter: <*name*> is name of external portal server.

<*ipaddr*> is ip address of external portal server.

ipv4 the configured portal server address is ipv4 address.

ipv6 the configured portal server address is ipv6 address.

<1-65535> is number of portal server.

Default: None.

Command Mode: Captive Portal global configuration mode.

Usage Guide: Configure external portal servers, 10 can be configured at most. Each cp configuration can be bound to one portal server.

Example: Configure a external portal server.

Switch(config-cp)# external portal-server server-name x1 ipv4 1.0.0.1 port 11111

5.11.1.21 http-redirect-filter <1-32> {ip A.B.C.D| domain WORD}

Command: http-redirect-filter <1-32> {ip A.B.C.D| domain WORD}

no http-redirect-filter (<1-32>|all)

Function: Appoint the IP or domain name for the HTTP redirection of portal authentication. Only the HTTP packet with this IP or domain name can be redirected. The no command deletes the domain name or ip address. The http packet with the mac which is not authenticated will be redirected to the portal server.

Parameters: <1-32>: the ID number of the rule (index);

ip A.B.C.D: the appointed IP address of HTTP redirection;

domain WORD: the appointed domain name of HTTP redirection, the maximum range is 256.

Default: This command is not configured as default.

Command Mode: Captive Portal configuration mode.

Usage Guide: Configure the authentication domain name or ip address.
Example: Appoint the ip address as 1.1.1.1.
Switch (config-cp)# http-redirect-filter 1 ip 1.1.1.1
Appoint the domain name as www.example.com.
Switch (config-cp)# http-redirect-filter 1 domain www.example.com

5.11.1.22 http-redirect-filter <1-32>

Command: http-redirect-filter <1-32>
no http-redirect-filter <1-32>
Function: Bind a rule to a instance of the captive portal. The no command deletes the redirect binding.
Parameters: <1-32>: the ID number of the rule (index).
Default: This command is not configured as default.
Command Mode: Captive Portal instance mode.
Usage Guide: Bind a rule to a instance of the captive portal.
Example: Bind the rule to the instance.
Switch (config-cp-instance)# http-redirect-filter 1

5.11.1.23 name

Command: name *<cp-name>*
no name
Function: Define the name of Captive Portal configuration.
Parameter: *<cp-name>*, the name of Captive Portal configuration, 32 characters can be included at most and they can be numbers and letters.
Default: None.
Command Mode: Captive Portal Instance configuration mode.
Usage Guide: Define the name of Captive Portal configuration.
Example: Define the name of Captive Portal configuration as abc123.
Switch(config-cp-instance)#name abc123

5.11.1.24 nas-ipv4

Command: nas-ipv4 < *A.B.C.D*>
no nas-ipv4 < *A.B.C.D*>
Function: Define the Captive Portal nas-ip address.
Parameters: < *A.B.C.D* >: IPv4 address of NAS.
Default: None.
Command Mode: Captive Portal mode.
Usage Guide: Define the Captive Portal nas-ip address.
Example: Configure the Captive Portal nas-ip address as 10.1.1.1.
Switch (config-cp)#nas-ip 10.1.1.1

5.11.1.25 interface [ethernet |] *IFNAME* vlan

Command: interface [ethernet |] IFNAME vlan [add | remove |] WORD

no interface [ethernet |] IFNAME

Function: Enable the port and vlan under the instance. One instance can be only bind to one port, but multiple vlan pools can be bound.

Parameters: [ethernet |] IFNAME :interface name.

[add | remove |] WORD:vlan list.

Default: None.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Enable the portal function under the port and bind the port to one instance. After binding, the rule under the instance can be applied to this port. If the parameter of vlan is not appointed, the flow of all vlan under the port must be authenticated. Only the flow of the appointed vlan should be authenticated if the vlan is appointed. The flow of other vlan will be allowed.

If the parameter of vlan is not appointed, the portal authentication of all vlan will be disabled and the flow will be recovered normally. If the vlan is appointed, the portal authentication of the appointed vlan will be disabled and the flow of this vlan will be recovered normally. The flow of this vlan will be allowed.

Example: Configure the port of 1/0/1 and vlan3 under the instance configuration 1

Switch (config-cp-instance) #interface ethernet 1/0/1 vlan add 3

5.11.1.26 portal-server

Command: portal-server {ipv4 | ipv6} <*name*>

no portal-server {ipv4 | ipv6}

Function: This command can bind specific external portal server for the CP configuration. Networks under this CP configuration all redirect authentication through this portal server.

Parameter: <name> binding Portal server name.

ipv4 the bond portal server address is ipv4 address.

ipv6 the bond portal server address is ipv6 address.

Default: None.

Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Use this command to bind specific external portal server for the CP configuration; it can also unbind the specific external portal server.

Example: Bind specific external portal server for the CP configuration.

Switch(config-cp -instance)#portal-server ipv4 x1

5.11.1.27 radius accounting

Command: radius accounting

no radius accounting

Function: Enable the accounting function of Captive Portal instance. The no command disables it.

Parameters: None.
Default: Disable.
Command Mode: Captive Portal Instance Mode.
Usage Guide: Enable the accounting function of Captive Portal instance.
Example: Enable the accounting function of Captive Portal instance.
Switch (config-cp-instance)#radius accounting

5.11.1.28 radius-accounting update interval

Command: radius-accounting update interval <*60-3600*>
no radius-accounting update interval
Function: Configure the accounting updating interval of the portal user that the switch sends to radius. The no command recovers it to be the default value.
Parameters: <*60-3600*> is the interval, the unit is second.
Default: 300 seconds.
Command Mode: Captive Portal Instance Mode.
Usage Guide: Configure the accounting updating interval of the portal user
Example: Configure the accounting updating interval of the portal user that the switch sends to radius as 60s.
Switch (config-cp-instance)# radius-accounting update interval 60

5.11.1.29 radius-acct-server

Command: radius-acct-server *<server-name>*
no radius-acct-server
Function: Define the radius accounting server name of the captive portal. The no command deletes it.
Parameters: <*server-name*>: name of radius accounting server.
Default: None.
Command Mode: Captive Portal Instance Mode.
Usage Guide: Define the radius accounting server name of the captive portal.
Example: Define the radius accounting server name of the captive portal as radius_aaa_1.
Switch (config-cp-instance)#radius-acct-server radius_aaa_1

5.11.1.30 radius-auth-server

Command: radius-auth-server *<server-name>*
no radius-auth-server
Function: Use this command to define the RADIUS authentication server of the Captive Portal configuration. The no command deletes the configuration.
Parameter: *<server-name>*, RADIUS authentication server name of Captive Portal configured.
Default: None.
Command Mode: Captive Portal Instance configuration mode.

Usage Guide: Define the RADIUS authentication server of the Captive Portal configuration.

Example: Define the RADIUS authentication server of the Captive Portal configuration as radius_aaa_1.

Switch(config-cp-instance)#radius-auth-server radius_aaa_1

5.11.1.31 redirect url-head <word>

Command: redirect url-head <word>

no redirect url-head

Function: Configure the redirect url-head including transmission protocol, host name, port and path. The no command deletes it.

Parameters: <word>, It is the redirect url-head such as https://200.101.13.4:8080/index.jsp or http:// www.portal.com/index.jsp. 128 characters can be input at most.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guide: This command is used to configure the redirect url-head including transmission protocol, host name, port and path. Configures according to the redirect url of the portal server. The transmission protocol, host name, port and path should be same for redirecting.

Example: Configure the redirect url-head as http://17.16.1.26/control.

Switch(config-cp-instance)#redirect url-head http://17.16.1.26/control

5.11.1.32 redirect attribute ssid enable

Command: redirect attribute ssid enable

no redirect attribute ssid enable

Function: Configure the redirect url to carry the parameter of ssid. The no command disables this function.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Default: Disable.

Usage Guide: This command is used to configure the redirect url to carry the parameter of ssid. After enabled this command, the redirect url will carry the ssid associated with client when the client conducts the redirection.

Example: Configure the redirect url to carry the parameter of ssid.

Switch(config-cp-instance)#redirect attribute ssid enable

5.11.1.33 redirect attribute ssid name

Command: redirect attribute ssid name <word>

no redirect attribute ssid name

Function: Configure the name of the parameter of ssid carried in the redirect url. The no command recovers it to be the default value.

Parameters: <word>, it is the ssid name including 32 characters at most.

Command Mode: Captive Portal Instance Mode.
Default: ssid.
Usage Guide: This command is used to configure the name of the parameter of ssid carried in the redirect url.
Example: Configure the name of the parameter of ssid carried in the redirect url as ssid.
Switch(config-cp-instance)#redirect attribute ssid name ssid

5.11.1.34 redirect attribute nas-ip enable

Command: redirect attribute nas-ip enable
no redirect attribute nas-ip enable
Function: Configure the redirect url to carry the parameter of nas-ip. The no command disables this function.
Parameters: None.
Command Mode: Captive Portal Instance Mode.
Default: Disable.
Usage Guide: This command is used to configure the redirect url to carry the parameter of nas-ip. After enabled this command, the redirect url will carry the IP address of switch associated with client when the client conducts the redirection.
Example: Configure the redirect url to carry the parameter of nas-ip.
Switch(config-cp-instance)#redirect attribute nas-ip enable

5.11.1.35 redirect attribute nas-ip name

Command: redirect attribute nas-ip name <word>
no redirect attribute nas-ip name
Function: Configure the name of the parameter of nas-ip carried in the redirect url. The no command recovers it to be the default value.
Parameters: <word>, it is the nas-ip name including 32 characters at most.
Command Mode: Captive Portal Instance Mode.
Default: acname.
Usage Guide: This command is used to configure the name of the parameter of nas-ip carried in the redirect url.
Example: Configure the name of the parameter of nas-ip carried in the redirect url as nasip.
Switch(config-cp-instance)#redirect attribute nas-ip name nasip

5.11.1.36 vlan-pool <1-255> <WORD>

Command: vlan-pool <1-255> <WORD>
no vlan-pool <1-255>
Function: Before enable the authentication for the specific VLAN, configure the VLAN pool first. Appoint the range of the vlan or some vlan ID in the vlan pool and bind this vlan to the port. It can appoint one vlan to enable the authentication. The no command deletes the vlan pool.

Parameters: <1-255>: vlan-pool ID number (index);
WORD: vlan id list.
Default: None.
Command Mode: Global Mode.
Usage Guide: It can appoint one vlan to enable the authentication. Configure the vlan pool and check if the element in the vlan pool is same with the one in other vlan pool. The element in the vlan which is already bound to the port cannot be modified.
Example: Enable the portal authentication function of vlan 1-100 and configure the vlan pool.
Switch (config)#vlan-pool 1 1-100

5.11.1.37 session-timeout

Command: session-timeout *<0-86400>*
no session-timeout
Function: Define the session timeout of the Captive Portal. The no command disables this function.
Parameters: <*0-86400*>: the session timeout, unit is second. 0 means the timeout function is not effective.
Default: 86400.
Command Mode: Captive Portal Instance Mode.
Usage Guide: Define the session timeout of the Captive Portal.
Example: Define the session timeout of the Captive Portal as 100s.
Switch (config-cp-instance)# session-timeout 100

5.11.1.38 show captive-portal

Command: show captive-portal
Function: Shows the characteristics status of the Captive Portal.
Parameter: None.
Default: None.
Command Mode: Admin mode
Usage Guide: Show the relevant state parameters of the captive portal function on this switch.
Example: Show Captive Portal status of enable and disable.
captive portal enable:
Switch#show captive-portal
Administrative Mode..... Enable
Operational Status..... Enabled
CP IP Address..... 101.1.1.3
captive portal disable:
Switch#show captive-portal
Administrative Mode..... Disable
Operational Status..... Disabled
Disable Reason..... Administrator Disabled

CP IP Address..... 0.0.0.0

5.11.1.39 show captive-portal status

Command: show captive-portal status
Function: Shows the status of all the Captive Portal instance in the system.
Parameter: None.
Default: None.
Command Mode: Admin mode
Usage Guide: This command shows the captive portal configuration and the supported property parameters on this switch.
Example: Show the Captive Portal status of the controller.
Switch#show captive-portal status
Peer Switch Statistics Reporting Interval..... 120
Authentication Timeout..... 300
Authentication Type..... External
Supported Captive Portals..... 10
Configured Captive Portals..... 9
Active Captive Portals..... 0
Local Supported Users..... 128
Configured Local Users..... 0
System Supported Users..... 1024
Authenticated Users..... 0

5.11.1.40 show captive-portal configuration

Command: show captive-portal configuration *<cp-id>*
Function: Show the status of Captive Portal configuration.
Parameter: ***<cp-id>*** is the ID number of captive portal, range is 1 to 10.
Default: None.
Command Mode: Admin mode
Usage Guide: Show the configured parameters of portal instance.
Example: Show the configured situation of captive portal1.
Switch#show captive-portal configuration 1
CP ID..... 1
CP Name..... default
Operational Status..... Enabled
Block Status..... Not Blocked
Configured Locales..... 1
Authenticated Users..... 0
Permit-all Status..... Disabled

5.11.1.41 show captive-portal configuration interface

Command: show captive-portal configuration <*cp-id*> interface <IFNAME or ethernet>

Function: Shows all the interface information assigned to the captive portal configuration.

Parameter: ***<cp-id>,*** ID number of cp;

IFNAME ,Interface Name or number

Ethernet, Ethernet port

Default: None.

Command Mode: Admin mode

Usage Guide: Shows the interface state of the a portal instance.

Example: Shows all the interface information of Captive Portal configuration.

Switch # show captive-portal configuration 1 interface e1/0/1

CP ID..... 1

CP Name..... Default

Interface..... 1

Interface Description..... Ethernet1/0/1

Operational Status..... Enabled

Block Status..... Not Blocked

Authenticated Users..... 0

5.11.1.42 show captive-portal configuration status

Command: show captive-portal configuration [<*cp-id*>] status

Function: Shows the configuration information of all or specific Captive Portal.

Parameter: ***<cp-id>,*** ID number of cp, the parameter **<cp-id>** means the content of a instance, without the parameter to show all the current configured instance parameters.

Default: None.

Command Mode: Admin mode

Usage Guide: Show detailed configuration parameters of portal instance.

Example: Show all Captive Portal configuration information.

Show the status of all the instances:

Switch # show captive-portal configuration status

CP ID	CP Name	Mode	Protocol	Verification
1	Default	Enable	HTTP	RADIUS
2	Default	Enable	HTTP	RADIUS

5.11.1.43 show captive-portal client status

Command: show captive-portal client [<*FF-FF-FF-FF-FF-FF*> { ipv4 | ipv6} <*ip-addr*>] status

Function: This command shows detailed connection information or an overview of users connected to the captive portal.

Parameter: <*FF-FF-FF-FF-FF-FF*> is the MAC address of the user.

ipv4: user address is ipv4 address.

ipv6: user address is ipv6 address.

<*ip-addr*> is user address. Ipv4 address is decimal format with point and ipv6 address is the format of X:X::X:X.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the status of all or a portal user.

Example: Show detailed information of user1 connected to the captive portal.

```
Switch # show captive-portal client status
MAC Address       IP Address          User Name   Protocol   Mode     Session Time
20-6a-8a-65-0d-17 66.1.1.2            user1       HTTP       RADIUS   0d:00:00:47
```

5.11.1.44 show captive-portal configuration client

Command: show captive-portal configuration [<*cp-id*>] client status

Function: This command shows the client information through the portal authentication in an interface.

Parameter: <*cp-id*>, ID number of Captive Portal.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the user parameters of a portal instance.

Example: Show all the portal configuration information of the client passed authentication.

```
Switch #show captive-portal configuration 1 client status
CP ID..................................... 1
CP Name................................... Default
  Client MAC Address    Client IP Address   Interface     Interface Description

   00-24-8c-00-99-27     10.1.1.51            1922          Port-Channel2
```

5.11.1.45 show captive-portal ext-portal-server status

Command: show captive-portal ext-portal-server status

Function: Use this command to check the status of the external portal server.

Parameter: None.

Default: None.

Command Mode: Admin mode.

Usage Guide: Check the status of the external portal server.

Example: Check the status of the external portal server.

```
Switch #show captive-portal ext-portal-server status
Server Name              Server IP Address              port       SocketNo
-------------------- ---------------------------------------- -------- --------
x1                       100.1.1.2                          7749              0
x2                       100.1.1.1                          7749              0
```

5.11.1.46 show captive-portal interface configuration status

Command: show captive-portal interface configuration [<*cp-id*>] status

Function: This command shows the interface information of all captive portal configuration or a specific configuration.

Parameter: <*cp-id*>, captive portal ID.

Default: None.

Command Mode: Admin mode

Usage Guide: This command shows the binding relationship of all or a portal instances with interface.

Example: Show the interface information of all captive portal configuration.

Switch #show captive-portal interface configuration status

CP ID	CP Name	Interface	Interface Description	Type
1	Default	1	Ethernet1/0/1	Physical

5.11.2 Free-resource

5.11.2.1 free-resource(global)

Command: free-resource destination { ipv4 | ipv6} <*ip-addr*><*netmask*> }

no free-resource destination { ipv4 | ipv6} <*ip-addr*><*netmask*> }

Function: Configure the free-resource rules, the client who conforms the source IP address in rules can access the resources of the destination IP address in rules, the switch does not redirect, the client can access directly without Portal authentication.

Parameter: ipv4 the configured free resource address is ipv4 address

ipv6 the configured free resource address is ipv6 address

<*ip-addr*> free-resource rules interviewees'/visitors' IP addresses.

<*netmask*> free-resource rules interviewees'/visitors' IP addresses.

Default: None.

Command Mode: Global configuration mode.

Usage Guide: Configure the client address segment (visitor) which can be free to access the resources and the address segment which is free to provide the resource (interviewee).

Example: Set free-resource rules.

Switch (config)# free-resource destination ipv4 1.1.1.1/24

5.11.3 Authentication White-list

5.11.3.1 free-mac

Command: free-mac < MACADD>< MACMASK>

no free-mac < MACADD>< MACMASK>

Function: Add the MAC without needing to authenticate. The no command deletes it.

Parameters: < MACADD>: mac address;

< MACMASK>: mac mask.

Default: None.

Command Mode: Global Mode.

Usage Guide: For the user with the specific MAC without needing to authenticate, it means to allow the user without any authentication.

Example: Configure the MAC without needing to authenticate as 00-01-11-11-11-11.

Switch(Config)#free-mac 00-01-11-11-11-11

5.11.4 Automatic Page Pushing after Successful Authentication (it is not supported currently)

5.11.4.1 redirect attribute url-after-login enable

Command: redirect attribute url-after-login enable

no redirect attribute url-after-login enable

Function: Enable the function that the redirect url carrys the pushed url after the successful authentication. The no command disables this function.

Parameters: None.

Command Mode: Captive Portal Instance Mode.

Default: Disable.

Usage Guide: This command is used to enable the function that the redirect url carrys the pushed url after the successful authentication. After enabled this command, the redirect url pushed by switch will carry the url which needs to be pushed after the successful authentication. At the same time, when the <url-value> of redirect attribute url-after-login value is configured as empty, the carried url is the page url that the user access before the authentication. If it is not empty, the carried url is the page url configured by <url-value>.

Example: Enable the function that the redirect url carrys the pushed url after the successful authentication.

Switch(config-cp-instance)#redirect attribute url-after-login enable

5.11.4.2 redirect attribute url-after-login name

Command: redirect attribute url-after-login name <name>

no redirect attribute url-after-login name

Function: Configure the attribute name of the pushed url after the successful authentication which is carried in the redirect url. The no command recovers it to be the default value.

Parameters: <name>, it is the attribute name including 32 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: The default name is srcurl.

Usage Guide: This command is used to configure the attribute name of the pushed url after the successful authentication which is carried in the redirect url.

Example: Configure the attribute name of the pushed url after the successful authentication which is carried in the redirect url as redirect.

Switch(config-cp-instance)#redirect attribute url-after-login name redirect

5.11.4.3 redirect attribute url-after-login encode

Command: redirect attribute url-after-login encode {plain-text|base64}

Function: Configure the encode of the pushed url after the successful authentication which is carried in the redirect url.

Parameters: plain-text, it is the plain-text;

base64, It is the base64 encode.

Command Mode: Captive Portal Instance Mode.

Default: The default encode is plain-text.

Usage Guide: This command is used to configure the encode of the pushed url after the successful authentication which is carried in the redirect url. It can be configured according to the encode supported by the portal server.

Example: Configure the encode of the pushed url after the successful authentication which is carried in the redirect url as base64.

Switch(config-cp-instance)#redirect attribute url-after-login encode base64

5.11.4.4 redirect attribute url-after-login value

Command: redirect attribute url-after-login value <url-value>

no redirect attribute url-after-login value

Function: Configure the appointed url which is popped up after the success authentication. The no command deletes it.

Parameters: <url-value>, it is the configured appointed url including 512 characters at most.

Command Mode: Captive Portal Instance Mode.

Default: None.

Usage Guide: This command is used to configure the appointed url which is popped up after the success authentication. If enable the function that the redirect url carries the pushed url after the successful authentication, the redirect url will carry the url with the <url-value>.

Example: Configure the appointed url which is popped up after the success authentication as http://www.test.com.

Switch(config-cp-instance)#redirect attribute url-after-login value http://www.test.com

5.11.5 No Perception of Portal

5.11.5.1 fast-mac-auth

Command: fast-mac-auth

no fast-mac-auth

Function: This command configures to enable the quick mac authentication function. The no command disables it.

Parameters: None.

Command Mode: captive portal config mode.

Default: Disable.

Usage Guide: After enabled this command, there is no need to carry on the portal authentication if the mac authentication is successful.

Example: Enable the quick mac authentication function.

Switch(config-cp-instance)#fast-mac-auth

5.11.6 Portal Escaping

5.11.6.1 portal-server-detect server-name <name>

Command: portal-server-detect server-name <name> [interval <interval>] [retry <retries>][action {log | permit-all | trap }]

no portal-server-detect server-name <name>

Function: Enable the Portal server escaping function and configure the related parameters and the server configuration of status changing.

Parameters: <name> is the Portal server name, it is the string including 1 to 32 characters and the upper and lower case letters should be distinguished. This portal server must exist. <interval>: it is the interval of probing attempt, the range is from 20 to 600 and the unit is second. The default value is 20. <retries>: it is the maximum number of the probing failures, the range is from 1 to 5 and the default value is 3. If the probing failures achieve this value, the server is considered unreachable. { log | permit-all | trap }: when the unreachable status of the Portal server changed, it can trigger the configuration including the following situations and multiple configurations can be selected at the same times.

- log: when the unreachable status of the Portal server changed, the log information can be sent. In the log, it records the portal server name and the status information before and after the change of the server status.
- trap: when the unreachable status of the Portal server changed, the trap information can be sent to the network management server. In the trap, it records the portal server name and the status information before and after the change of the server status.
- permit-all: it is also named as portal escaping. It means to cancel the portal authentication temporarily and allow all the portal users accessing the network when the portal server is in the unreachable status (down). If the server status changes to the reachable status (up), the portal authentication function will be recovered.

Default: Disable. The default values of interval, retries and action are 20, 3 and permit-all respectively.

Command Mode: Captive Portal Global Configuration Mode.

Usage Guide: This command can be used to enable the portal escaping function when the portal server has fault. After enabled this function, there is no effect for the user authentication if the connection between switch and Portal server is normal; only when the connection between the switch and Portal server is broken, the user can be allowed accessing the network without the authentication. The operations can enable this function too, but the triggered configuration must be selected as log or trap.

Example: Enable the escaping function of the portal server whose name is test. Configure the interval as 30s, configure the retries as 2 and configure the configuration of the server status change as log and permit-all.

Switch (config-cp)# portal-server-detect server-name test interval 600 retry 2 action log permit-all trap

5.11.6.2 portal-server-detect client-deauth

Command: portal-server-detect client-deauth

no portal-server-detect client-deauth

Function: Enable this command, the server status will change from down to up, all the users are forced down line. The no command disables this function, which means not to force the online user to get down the line after configured the detection status of portal server to change from down to up.

Parameters: None.

Default: Enable.

Command Mode: captive portal mode.

Usage Guide: All the users are forced down line when the server status is changed after enabled this command. It is the hidden command, the command of show run cannot view it.

Switch (config-cp)# portal-server-detect client-deauth

5.11.6.3 show captive-portal ext-portal-server server-name <name> status

Command: show captive-portal ext-portal-server server-name <name> status

Function: Show the portal server status including the server address and if the portal escaping function is enabled.

Parameters: <name> is the Portal server name, it is the string including 1 to 32 characters and the upper and lower case letters should be distinguished.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Checking the server status is the important method to check the fault. When the portal escaping function is not effective, the configuration may be wrong; the command can be

modified to help the administrator to remove the fault. If there is not the parameter of <name>, the status of all the servers will be shown. If there is the parameter of <name>, the detailed status information of the server will be shown.

Example: Show the status of all the ext-portal-server.

Show the detailed status of the server named as Portaltest.

Switch (config-cp)#show captive-portal ext-portal-server server-name Portaltest status

Server Name..... portaltest

Server IP..... 101.1.1.6

Server Port..... 7749

Server Key.....

Detect Mode..... Enable

Detect Interval..... 20

Detect Retries..... 3

Detect Trap Mode..... Disable

Detect Log Mode..... Disable

Detect Permit-all Mode..... Enable

Detect Operational Mode..... Enable

Detect Operational Status..... Down

Detect Operational Fails..... 1

Detect Operational Time..... 0d:00:00:11

5.12 MAB

5.12.1 authentication mab

Command: authentication mab {radius|local} (none|)

no authentication mab

Function: Configure the authentication mode and priority of MAC address authentication, the no command restores the default authentication mode.

Parameters: radius means RADIUS authentication mode; local means the local authentication; none means the authentication is needless.

Default: Using RADIUS authentication mode.

Command Mode: Global mode

Usage Guide: none option is used to the fleeing function of MAC address authentication. If all configured RADIUS servers don't respond, switch will adopt none authentication mode to allow that MAC address authentication users access the network directly. The option of local is used for the local authentication of MAC address, it authenticates through the local user name and password. If configured as the method of **authentication mab radius local none**, judge if configured the user name and password used in mab authentication in local when the radius server has no response. If it has been configured, use the local authentication, if not, use the

Function

backup none authentication.

Example: Configure the local authentication and the fleeing function of MAC address authentication.

Switch(config)#authentication mab radius local none

5.12.2 clear mac-authentication-bypass binding

Command: clear mac-authentication-bypass binding {mac WORD | interface (ethernet IFNAME | IFNAME) | all}

Function: Clear MAB binding information.

Parameters: MAC: Delete MAB binding of the specified MAC address

IFNAME: Delete MAB binding of the specified port

all: Delete all MAB binding

Command Mode: Admin Mode

Default: None.

Usage Guide: None.

Example: Delete all MAB binding.

Switch#clear mac-authentication-bypass binding all

5.12.3 debug mac-authentication-bypass

Command: debug mac-authentication-bypass {packet | event | binding}

Function: Enable the debugging of the packet information, event information or binding information for MAB authentication.

Parameters: packet: Enable the debugging of the packet information for MAB authentication.

event: Enable the debugging of the event information for MAB authentication.

binding: Enable the debugging of the binding information for MAB authentication.

Command Mode: Admin Mode

Default: None.

Usage Guide: None.

Example: Enable the debugging of the packet information for MAB authentication.

Switch#debug mac-authentication-bypass packet

5.12.4 mac-authentication-bypass binding-limit

Command: mac-authentication-bypass binding-limit <*1-100*>

no mac-authentication-bypass binding-limit

Function: Set the max binding number of MAB. The no command will restore the default binding number as 3.

Parameters: <*1-100*> the max binding number of MAB, ranging from 1 to 100.

Command Mode: Port Mode

Default: The max binding number of MAB is 3.

Usage Guide: Set the max binding number of MAB. When the binding number reaches to the max value, the port will stop binding, if the max binding number is less than the current binding number of the port, the setting will be unsuccessful.
Example: Configure the max binding number as 10.
Switch(Config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mac-authentication-bypass binding-limit 10

5.12.5 mac-authentication-bypass enable

Command: mac-authentication-bypass enable
no mac-authentication-bypass enable
Function: Enable the global and port MAB function. The no command disables MAB function.
Parameters: None.
Command Mode: Global Mode and Port Mode
Default: Disable the global and port MAB function.
Usage Guide: To process MAB authentication of a port, enable the global MAB function first, and then, enable the MAB function of the corresponding port.
Example: Enable the global and port Eth1/0/1 MAB function.
Switch(Config)#mac-authentication-bypass enable
Switch(Config)#interface ethernet 1/0/1
Switch(Config-If-Ethernet1/0/1)#mac-authentication-bypass enable

5.12.6 mac-authentication-bypass guest-vlan

Command: mac-authentication-bypass guest-vlan <1-4094>
no mac-authentication-bypass guest-vlan
Function: Set guest vlan of MAB authentication. The no command deletes guest vlan.
Parameters: <*1-4094*>: guest vlan ID, ranging from 1 to 4094.
Command Mode: Port Mode
Default: None.
Usage Guide: Set guest vlan of MAB authentication, only Hybrid port use this command, it is not take effect on access port. After MAB authentication is failing, if the existent guest vlan is configured by the port connecting to the MAB user, the MAB user can join and access guest vlan.
Example: Configure guest vlan of MAB authentication for port 1/0/1
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mac-authentication-bypass guest-vlan 10

5.12.7 mac-authentication-bypass spoofing-garp-check

Command: mac-authentication-bypass spoofing-garp-check enable
no mac-authentication-bypass spoofing-garp-check enable

Function: Enable the spoofing-garp-check function, MAB function will not deal with spoofing-garp any more; the no command disables the function.
Parameters: None.
Command Mode: Global Mode
Default: Disable spoofing-garp-check function.
Usage Guide: When the terminal of Windows operating system detects the address conflict, it will sends a gratuitous ARP to correct the error ARP entries generated by gratuitous ARP of the conflict detection. This command is used to detect the spoofing-garp when occuring the address conflict, MAB function is not deal with the packet any more. Notice: when enabling the check function, all ARP will be processed the software check, it will add switch's load.
Example: Enable spoofing-garp-check function.
Switch(Config)#mac-authentication-bypass spoofing-garp-check enable

5.12.8 mac-authentication-bypass timeout linkup-period

Command: mac-authentication-bypass timeout linkup-period <0-30>
no mac-authentication-bypass timeout linkup-period
Function: Set the interval between down and up when VLAN binding in a port is changing to assure the user can obtain IP again.
Parameters: <*0-30*>: After the port is shutdown automatically, the interval before it up again, the unit is second, 0 means there is no down/up operation.
Command Mode: Global Mode
Default: The interval is 0.
Usage Guide: When MAB authentication is successful, belong to vlan according to auto-vlan setting, when MAB authentication is failing, belong to vlan according to guest-vlan setting. After linkup-period is set, when VLAN binding of a port is changing, the port will be shutdown automatically, and will be up again after linkup-period to assure the client obtain IP.
Example: Configure down/up time as 12s.
Switch(Config)#mac-authentication-bypass timeout linkup-period 12

5.12.9 mac-authentication-bypass timeout offline-detect

Command: mac-authentication-bypass timeout offline-detect (0 | <60-7200>)
no mac-authentication-bypass timeout offline-detect
Function: Configure offline-detect time. The no command restores the default value.
Parameters: (0 | <60-7200>): offline-detect time, the range is 0 or 60 to 7200s.
Command Mode: Global Mode
Default: offline-detect time is 180s.

Usage Guide: When offline-detect time is 0, the switch does not detect MAB binding, when offline-detect time is 60s to 7200s, the switch timely detects the flow corresponding to the MAB binding. If there is no flow in the period of offline-detect time, it will delete this binding and forbid the flow to pass.

Example: Configure offline-detect time as 200s.

Switch(Config)#mac-authentication-bypass timeout offline-detect 200

5.12.10 mac-authentication-bypass timeout quiet-period

Command: mac-authentication-bypass timeout quiet-period <1-60>

no mac-authentication-bypass timeout quiet-period

Function: Set quiet-period of MAB authentication. The no command restores quiet-period as the default value.

Parameters: <*1-60*>: quiet-period, ranging from 1 to 60s.

Command Mode: Global Mode

Default: quiet-period is 30s.

Usage Guide: If MAB authentication is failing, within the quiet-period the switch will not respond the authentication request of this MAC, after quiet-period, it will respond the request again.

Example: Configure quiet-period of MAB authentication as 60s.

Switch(Config)#mac-authentication-bypass timeout quiet-period 60

5.12.11 mac-authentication-bypass timeout reauth-period

Command: mac-authentication-bypass timeout reauth-period <1-3600>

no mac-authentication-bypass timeout reauth-period

Function: Set the reauthentication interval at failing authentication state. The no command restores the default value.

Parameters: <*1-3600*>: reauthentication interval, ranging from 1 to 3600s.

Command Mode: Global Mode

Default: reauthentication interval is 30s.

Usage Guide: At failing authentication state, the user processes the reauthentication timely until the authentication is successful; at the successful state, the user can access the network resources.

Example: Configure reauthentication time as 20s.

Switch(Config)#mac-authentication-bypass timeout reauth-period 20

5.12.12 mac-authentication-bypass timeout stale-period

Command: mac-authentication-bypass timeout stale-period <0-60>

no mac-authentication-bypass timeout stale-period

Function: Set the time that delete the binding user after MAB port is down. The no command restores the default value.

Parameters: <*1-60*>: The time that delete the binding, ranging from 0 to 60s.

Command Mode: Global Mode

Default: 30s.

Usage Guide: If the time that delete the binding as 0, delete all user binding of this port as soon as the MAB port is down, if the time is bigger than 0, delete the user binding with a delay after the MAB port is down.

Example: Configure the deletion time as 40s.

Switch(Config)#mac-authentication-bypass timeout stale-period 40

5.12.13 mac-authentication-bypass username-format

Command: mac-authentication-bypass username-format {

mac-address (groupsize (1|2|4|12) |) (separator WORD |) (lowercase | uppercase |) | {fixed username WORD password WORD}}

Function: Set the authenticate method of MAB authentication.

Parameters: mac-address: Use MAC address of MAB user as username and password to authenticate.

groupsize (1|2|4|12): The size of an interval using the MAC address of the MAB user, which is 2 by default.

separator WORD: Use the separator of MAB user's MAC address. The separator supports' - '': ''. ', The default interval is' - '.

lowercase | uppercase |: Use the case of the MAC address of the MAB user, which defaults to lowercase.

fixed username WORD password WORD: Use the specified username and password to authenticate, the length of username and password ranges between 1 and 32 characters.

Command Mode: Global Mode

Default: Use MAC address of MAB user as username and password to authenticate.

Usage Guide: There are two methods for MAB authentication: use MAC address of MAB user as username and password to authenticate or use the specified username and password to authenticate. If there is no specified username and password, the device uses the first method to authenticate by default.

Example: All MAB users use the same username and password to authenticate, the username is mab-user, the password is mab-pwd.

Switch(Config)#mac-authentication-bypass username-format fixed username mab-user password mab-pwd

5.12.14 show mac-authentication-bypass

Command: show mac-authentication-bypass {interface {ethernet IFNAME | IFNAME) |}
Function: Show the binding information of MAB authentication.
Parameters: interface {ethernet IFNAME|IFNAME}: The port name.
Command Mode: Admin Mode
Default: None.
Usage Guide: None.
Example: Show the binding information of all MAB users.
Switch#show mac-authentication-bypass

The Number of all binding is 5

MAC Interface Vlan ID State

05-0a-eb-6a-7f-88 Ethernet1/0/1 1 MAB_QUIET

04-0a-eb-6a-7f-88 Ethernet1/0/1 1 MAB_QUIET

03-0a-eb-6a-7f-88 Ethernet1/0/1 1 MAB_QUIET

02-0a-eb-6a-7f-88 Ethernet1/0/1 1 MAB_AUTHENTICATED

00-0a-eb-6a-7f-8e Ethernet1/0/1 1 MAB_AUTHENTICATED

Displayed information	Explanation
The Number of all binding	The binding number of all MAB users, include the successful authentication user and the failing authentication user at quiet-period state
MAC	MAC address
Interface	The binding port
Vlan	The VLAN that MAB user belongs
State	Authentication state

Switch(config)#show mac-authentication-bypass int e1/0/1

Interface Ethernet1/0/1 user config:

MAB enable: Enable

Binding info: 1

MAB Binding built at SUN JAN 01 01:14:48 2006

VID 1, Port: Ethernet1/0/1

Client MAC: 00-0a-eb-6a-7f-8e

Binding State: MAB_AUTHENTICATED

Binding State Lease: 164 seconds left

Displayed information	Explanation
MAB enable	MAB function enabled or not
Binding info	The MAB binding number of the specified port
MAB Binding built at	The time when the user binding was created
VID	The VLAN that MAB user belongs
Port	The binding port
Client MAC	MAC address
Binding State	Authentication state
Binding State Lease	Remain time before the binding release

5.13 PPPoE Intermediate Agent

5.13.1 debug pppoe intermediate agent packet {receive | send} interface ethernet <interface-name>

Command: debug pppoe intermediate agent packet (receive | send|) interface ethernet <interface-name>

no debug pppoe intermediate agent packet (receive | send|) interface ethernet <interface-name>

Function: Enable PPPoE packet debug for the specified port, the no command disables it.

Parameter: receive: Enable the debug that receive PPPoE packet.

send: Enable the debug that send PPPoE packet.

ehernet: Physical port

interface-name: Port name

Command Mode: Admin mode

Default: Disable PPPoE packet debug for the specified port.

Usage Guide: Enable PPPoE packet debug for the specified port to show PPPoE packet received and sent by this port.

Example: Enable PPPoE intermediate debug for port ethernet1/0/2.

Switch#debug pppoe intermediate agent packet send interface ethernet 1/0/2

5.13.2 pppoe intermediate-agent

Command: pppoe intermediate-agent

no pppoe intermediate-agent

Function: Enable global PPPoE intermediate agent function. The no command disables global PPPoE intermediate agent function.

Parameter: None.

Command Mode: Global mode.

Default: Disable global PPPoE intermediate agent function.

Usage Guide: After enable global PPPoE IA function, process the packet of PPPoE discovery stage according to the related configuration.

Example: Enable global PPPoE intermediate agent function.

Switch(config)#pppoe intermediate agent

5.13.3 pppoe intermediate-agent (Port)

Command: pppoe intermediate-agent

no pppoe intermediate-agent

Function: Enable PPPoE intermediate agent function of the port. The no command disables PPPoE intermediate agent function of the port.

Parameter: None.

Command Mode: Port mode

Default: Disable PPPoE intermediate agent function of the port.

Usage Guide: After enable PPPoE IA function of the port, add vendor tag for PPPoE packet of the port.

Note: 1. It must enable global pppoe intermediate-agent function.

2. At least one port is connected to PPPoE server, and the port mode is trust.

Example: Enable PPPoE intermediate agent function of the port ethernet 1/0/2.

Switch(config-if-ethernet1/0/2)#pppoe intermediate agent

5.13.4 pppoe intermediate-agent circuit-id

Command: pppoe intermediate-agent circuit-id <string>

no pppoe intermediate-agent circuit-id <string>

Function: Configure circuit ID of the port, the no command cancels this configuration.

Parameter: <string>: circuit-id, the max character number is 63 bytes.

Command Mode: Port mode

Default: This configuration is null.

Usage Guide: This command configures circuit-id alone for each port, the priority is higher than pppoe intermediate-agent identifier-string command.

Example: Configure circuit-id as abcd/efgh on port ethernet1/0/3 of vlan3.

Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id abcd/efgh
After port ethernet1/0/3 of vlan3 receives PPPoE packet, circuit-id value of the added vendor tag as ”abcd/efgh”.

5.13.5 pppoe intermediate-agent delimiter

Command: pppoe intermediate-agent delimiter <WORD>
no pppoe intermediate-agent delimiter
Function: Configure the delimiter among the fields in circuit-id and remote-id, the no command cancels the configuration.
Parameter: <WORD>: the delimiter, its range is (#|.|,|;|:|/|space).
Command Mode: Global mode
Default: The fields is comparted with ’\0’.
Usage Guide: After configuring the delimiter, the added fields of circuit-id and remote-id use the configured delimiter to compart. Notice: The global **pppoe intermediate-agent** function must be enabled.
Example: Configure the delimiter.
Switch(config)#pppoe intermediate-agent delimiter space

5.13.6 pppoe intermediate-agent format

Command: pppoe intermediate-agent format (circuit-id | remote-id) (hex | ascii)
no pppoe intermediate-agent format (circuit-id | remote-id)
Function: Configure the format with hex or ASCII for circuit-id and remote-id, the no command cancels the configuration.
Parameter: hex: hexadecimal
ascii: ASCII code
Command Mode: Global mode
Default: This configuration is null.
Usage Guide: Encapsulation circuit-id and remote-id with hex ASCII format to vendor tag. Notice: The global **pppoe intermediate-agent** function must be enabled.
Example: Configure the trust port 1/0/1 to enable vendor-tag strip function.
Switch(config)#pppoe intermediate-agent format remote-id ascii

5.13.7 pppoe intermediate-agent remote-id

Command: pppoe intermediate-agent remote-id <string>
no pppoe intermediate-agent remote-id <string>

Function: Configure remote-id of the port, the no command cancels this configuration.
Parameter: <string>: remote-id, the max character number is 63 bytes.
Command Mode: Port mode
Default: This configuration is null.

Usage Guide: Configure remote-id for each port, if there is no configuration, use switch's MAC as remote-id value.

Example: Configure remote-id as abcd on port ethernet1/0/2.

Switch(config-if-ethernet1/0/2)# pppoe intermediate-agent remote-id abcd

5.13.8 pppoe intermediate-agent trust

Command: pppoe intermediate-agent trust

no pppoe intermediate-agent trust

Function: Configure the port as trust port, the no command configures the port as untrust port.

Parameter: None.

Command Mode: Port mode

Default: Untrust port.

Usage Guide: The port which connect to server must be configured as trust port. Note: At least one trust port is connected to PPPoE server.

Example: Configure port ethernet1/0/1 as trust port.

Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust

5.13.9 pppoe intermediate-agent type self-defined circuit-id

Command: pppoe intermediate-agent type self-defined circuit-id {vlan | port | id (switch-id (mac | hostname) | remote-mac) | string WORD}

no pppoe intermediate-agent type self-defined circuit-id

Function: Configure the self-defined circuit-id, the no command cancels the configuration.

Parameter: vlan: VLAN ID

port: Port ID

id switch-id mac: the local MAC address

id switch-id hostname: the local host name

id remote-mac: the remote MAC address

string WORD: the specified keyword

Command Mode: Global mode

Default: This configuration is null.

Usage Guide: This configuration and type tr-101 circuit-id are mutually exclusive, it will clear the corresponding configuration of type tr-101 circuit-id.

Example: Configure the self-defined circuit-id as vlan port id switch-id hostname.

Switch(config)#pppoe intermediate-agent type self-defined circuit-id vlan port id switch-id hostname

5.13.10 pppoe intermediate-agent type self-defined remoteid

Command: pppoe intermediate-agent type self-defined remoteid {mac | vlan-mac | hostname | string WORD}

no pppoe intermediate-agent type self-defined remote-id

Function: Configure the self-defined remote-id, the no command cancels the configuration.

Parameter: mac: Ethernet port MAC address

vlan-mac: IP interface MAC address

hostname: the local host name

string WORD: the specified keyword

Command Mode: Global mode

Default: This configuration is null.

Usage Guide: Configuration order of this command according to the fields order in remote-id.

Example: Configure the self-defined remote-id as string abcd mac hostname.

Switch(config)#pppoe intermediate-agent type self-defined remoteid string abcd mac hostname

5.13.11 pppoe intermediate-agent type tr-101 circuit-id access-node-id

Command: pppoe intermediate-agent type tr-101 circuit-id access-node-id <string>

no pppoe intermediate-agent type tr-101 circuit-id access-node-id

Function: Configure access-node-id field value of circuit ID in the added vendor tag with tr-101 standard.

Parameter: <string>: access-node-id, the max character number is 47 bytes.

Command Mode: Global mode

Default: MAC address of the switch

Usage Guide: Use this configuration to create access-node-id of circuit ID in vendor tag. circuit-id value is access-node-id +" eth "+ Slot ID + delimiter + Port Index + delimiter + Vlan ID, access-node-id occupies n bytes (n<48), " eth " is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte. In default state, access-node-id value of circuit-id is switch's MAC, it occupies 6 bytes. For example: MAC address is "0a0b0c0d0e0f", Slot ID is 12, Port Index is 34, Vlan ID is 567, the default circuit-id value is "0a0b0c0d0e0f eth 12/034:0567".

Example: Configure access-node-id value of circuit ID as abcd in vendor tag.

Switch(config)#pppoe intermediate-agent access-node-id abcd

After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is "abcd eth 01/003:0003".

5.13.12 pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

Command: pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option {sp | sv | pv | spv} delimiter <WORD> [delimiter <WORD>]

no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

Function: Configure circuit-id of the added vendor tag with tr-101 standard, the no command deletes this configuration.

Parameter: <string>: identifier-string, the max character number is 47 bytes.

{sp | sv | pv | spv}: This option can select the combination format for slot, port, vlan, sp means slot and port, sv means slot and vlan, pv means port and vlan, spv means slot, port and vlan.

<WORD>: The delimiter between slot, port and vlan, the range is (# | . | , | ; | : | / | space). Note: There are two delimiter WORDs in spv combo mode, the first between slot and port, the second between port and vlan.

Command Mode: Global mode

Default: This configuration is null.

Usage Guide: This command is used to configure global circuit id, the priority is higher than pppoe intermediate-agent access-node-id command. circuit-id value is access-node-id +" eth "+ Slot ID + delimiter + Port Index + delimiter + Vlan ID, access-node-id occupies n bytes (n<48), " eth " is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte.

Example: Configure access-node-id as xyz, use spv combination mode, delimiter with "#"between Slot ID and Port ID, delimiter with "/"between Port ID and Vlan ID.

Switch(config)#pppoe intermediate-agent identifier-string xyz option spv delimiter # delimiter /

Switch# show pppoe intermediate-agent identifier-string option delimiter

config identifier string is : xyz

config option is : slot , port and vlan

the first delimiter is : "# "

the second delimiter is : "/ "

After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is "xyz eth 01#003/0003".

5.13.13 pppoe intermediate-agent vendor-tag strip

Command: pppoe intermediate-agent vendor-tag strip

no pppoe intermediate-agent vendor-tag strip

Function: Enable vendor-tag strip function of the port, the no command cancels this function.

Parameter: None.

Command Mode: Port mode

Default: Disable vendor-tag strip function of the port.

Usage Guide: If the received packet includes vendor tag from server to client, strip this vendor tag.

Note: 1. Must enable global pppoe intermediate-agent function.

2. It must be configured on trust port.

Example: Trust port ethernet1/0/1 enables vendor tag strip function.

Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust

Function Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip

5.13.14 show pppoe intermediate-agent access-node-id

Command: show pppoe intermediate-agent access-node-id
Function: Show the configured access node ID.
Parameter: None.
Command Mode: Admin mode
Default: The configuration information is null.
Usage Guide: This command is used to show access-node-id configured by user.
Example: Show access-node-id configuration information.
Switch#pppoe intermediate-agent access-node-id abcd
Switch#show pppoe intermediate-agent access-node-id
pppoe intermediate-agent access-node-id is : abcd

5.13.15 show pppoe intermediate-agent identifier-string option delimiter

Command: show pppoe intermediate-agent identifier-string option delimiter
Function: Show the configured identifier-string, the combination format and delimiter of slot, port and vlan.
Parameter: None.
Command Mode: Admin mode
Default: The configuration information is null.
Usage Guide: Show the configured identifier-string, the combo format and delimiter of slot, port and vlan.
Example: Show the configuration information for pppoe intermediate-agent identifier-string.
Switch#pppoe intermediate-agent identifier-string abcd option spv delimiter # delimiter /
Switch# show pppoe intermediate-agent identifier-string option delimiter
config identifier string is : abcd
config option is : slot , port and vlan
the first delimiter is : "# "
the second delimiter is : "/ "

5.13.16 show pppoe intermediate-agent info

Command: show pppoe intermediate-agent info [interface ethernet <interface-name>]
Function: Show the related PPPoE IA configuration information of all ports or the specified port.
Parameter: ehernet: physical port
interface-name: port name

Command Mode: Admin mode
Default: The configuration information is null.
Usage Guide: Check the configuration information of the corresponding port, show whether the port is trust port, strip function is enabled, rate limit is enabled, show the configured circuit ID and remote ID.
Example: Show pppoe intermediate-agent configuration information of port ethernet1/0/2.

```
Switch# show pppoe intermediate-agent info interface ethernet 1/0/2
Interface       IA      Trusted   vendor Strip   Rate limit   circuit id remote id
----------  ------  ------  -----------  -------  ---------  ----------
Ethernet1/0/2  yes        no          no              no          test1/port1     host1
```

5.14 QoS

5.14.1 accounting

Command: accounting
no accounting
Function: Set statistic function for the classified traffic.
Parameter: None.
Command mode: Policy map configuration mode
Default: Do not set statistic function.
Usage Guide: After enable this function, add statistic function to the traffic of the policy class map, the messages can only red or green when passing policy. When print statistic information, in packets means classify packets numbers and not support the classify of color.
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
```

5.14.2 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 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 nexthop 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

5.14.3 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 command deletes the specified class map.
Parameters: <*class-map-name*> is the class map name.
Default: No class map is configured by default.
Command mode: Global Mode
Usage Guide:
Example: Creating and then deleting a class map named "c1".
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#exit
Switch(config)#no class-map c1

5.14.4 clear 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

5.14.5 drop

Command: drop

no drop

Function: Drop data package that match the class, the no command cancels the assigned action.

Parameters: None.

Default: Do not set the action.

Command mode: Policy class map configuration mode

Usage Guide: Drop the specified packet after configure this command.

Example: Drop the packet which satisfy c1.

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1

Switch(Config-PolicyMap-p1-Class-c1)#drop

Switch(Config-PolicyMap-p1-Class-c1)#exit

Switch(Config-PolicyMap-p1)#exit

5.14.6 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, MAC ACL or IPv6 standard ACL or MAC-IP 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 range 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 range is 0~1048575;

vlan <vlan-list> match specified VLAN ID, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the range is 1~4094;

cos <cos-list> match specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS, the range 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. (The deny rule is not supported issuing in PBR, please pay attention to avoid it.) 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

5.14.7 mls qos aggregate-policy

Command: mls qos aggregate-policy <policer_name> <bits_per_second> burst-group <normal_burst_bytes>

[no] mls qos aggregate-policy <policer_name>

Function: Define a aggregate policy command. The no command delete mode configuration.

Parameters:

policer_name: it is the aggregate policy name.

bits_per_second: it define the information rate, namely CIR, the unit is kbit per second, and it ranges from 1 to 10000000;

normal_burst_bytes: it define the committed burst size, namely CBS, the unit is kilobyte, and it ranges from 1 to 8192, when the CBS more than the maximum of chips , it uses the biggest value that chip support to set hardware, CLI have not notice information;

Command Mode: Global Mode.

Default: The default is no policy action.

Usage Guide: It only supports single cylinder configuration, when configuring, if configured CBS, not support configure color, green packets only supports transmit, red packets only supports drop.

Example: Set 10000 as CIR, CBS is 512.

Switch (config)#policy burst 1 512

Switch(config)# mls qos aggregate-policy 1 1000 burst-group 1

5.14.8 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: Port Configuration Mode.

Usage Guide: Configure the default CoS value for switch port. In default configuration, the message ingress cos from this port are default value whether the message with tag. If the message without tag, the message cos value for tag is enactmented.

Example: Setting the default CoS value of ethernet port 1/0/1 to **7,** i.e., packets coming in through this port will be assigned a default CoS value of 7 if no CoS value present .

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#mls qos cos 7

5.14.9 mls qos internal-priority

This command is not supported *by* the switch.

5.14.10 mls qos map

Command: mls qos map {cos-intp <intp1…intp8> | cos-dp<dp1…dp8> | dscp-intp <in-dscp list> to <intp> | dscp-dp <in-dscp list> to <dp> | dscp-dscp <in-dscp list> to <out-dscp>}

no mls qos map {cos-intp | cos-dp | dscp-intp | dscp-dp | dscp-dscp}

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

Parameters**: cos-intp <intp1…intp8>** defines the mapping from CoS to intp (queue) value, <intp1..intp8> are 8 intp value corresponding to the 0 to 7 CoS value, each intp value is delimited with space, ranging from 0 to 3;

cos-dp<dp1…dp8> defines the mapping from cos to intp (queue), <dp1…dp8> is 8 drop priority and it corresponding to the Cos value from 0 to 7, every drop priority is separated by space, and it ranges from 0 to 2;

dscp-intp defines the mapping from DSCP to intp (queue).

dscp-dp defines the mapping from dscp to drop priority.

dscp-dscp defines the mapping from entrance dscp to export dscp, <in-dscp list> is the input dscp value, the most is 8 and it separated by space from each other, and it ranges from 0 to 63, <out-dscp> is output dscp value and it ranges from 0 to 63.

Default: Default mapping values are:

Default CoS-TO-INTP Map

CoS Value	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
INTP Value	0	0	1	1	2	2	3	3

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-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				

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

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

Command mode: Global Mode

Usage Guide: INTP means the chip internal priority setting. Because of the internal DSCP value have 64 and the chip internal priority (queue) only 8, the dscp-intp mapping need 8 continuum internal dscp mapping to the same INTP.

Example: 1. Setting the CoS-to-INTP mapping value to the default 0 8 16 24 32 40 48 56 to 0 1 2 3 3 2 1 0.

Switch(config)#mls qos map cos-intp 0 1 2 3 3 2 1 0

5.14.11 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 of the port 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 Configuration Mode.

Usage Guide: After configure this command, the queue management algorithm of the **port** is set.

Example: Setting the queue management algorithm as sp.

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#mls qos queue algorithm sp

5.14.12 mls qos queue drop-algorithm

This command is not supported by the switch.

5.14.13 mls qos queue weight

Command: mls qos queue weight <weight0..weight3>

no **mls qos queue weight**

Function: After configure this command, the queue weight is set.

Parameters: <weight0..weight3> defines the queue weight, for WRR algorithm, this configuration is valid, but SP algorithm 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 4 weight values. The different chips support the different weight range, if the setting exceeds the chip range, it will prompt the right range.

Default: The queue weight is 1 2 3 4.

Command mode: Global Mode.

Usage Guide: The absolute value of WRR is meaningless. WRR allocates bandwidth by using 4 weight values. If it is set as 0, the priority of the queue is highest. If more queues are set as 0, the queue with the higher priority will be higher than before. Note: only one or two queues can be set as 0 and must be set at behind.

Example: Configure the queue weight as 1 2 3 4.

Switch(config)#mls qos queue weight 1 2 3 4

5.14.14 mls qos queue wrr weight

This command is not supported by the switch.

5.14.15 mls qos queue wred

This command is not supported by switch.

5.14.16 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-ethernet1/0/1)#mls qos queue wdrr weight 10 10 20 20 40 40 80 80

5.14.17 mls qos queue bandwidth

Command: mls qos queue <queue-id> 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.

<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 8 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 maximum-bandwidth is 128kbps for ethernet1/0/2 queue1.

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)# mls qos queue 1 bandwidth 128

5.14.18 mls qos trust

Command: mls qos trust {cos | dscp }

no mls qos trust {cos | **dscp }**

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

Parameters: dscp configures the port to trust DSCP status. cos configures the COS port to trust status.

Default: Not trust CoS value, the default is trust COS value.

Command mode**:** Port Configuration Mode.

Usage Guide:

trust **dscp** mode: Set the intp field based dscp-to-intp mapping.

trust cos mode: Set the intp field based cos-to-intp mapping.

Example: Set trust dscp of port 1/0/1, not trust cos.

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ehternet1/1)# mls qos trust dscp

Switch(config-if-ehternet1/1)#no mls qos trust cos

5.14.19 pass-through-cos

This command is not supported by the switch.

5.14.20 pass-through-dscp

This command is not supported by the switch.

5.14.21 policy

Command: policy <bits_per_second> burst-group <burst-group-id>

no policy

Function: Support non-aggregate policy command of double color, the no command delete mode configuration.

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

burst-group-id: It is CBS burst-group id and it ranges from 1 to 2.

Default: No policy action.

Command mode: Policy class map configuration Mode.

Usage Guide: **Configure information rate in policy class map configuration mode. Not support the color configuration** and the default green packets is transmit, red packets drop.

Example: Set information rate 1000 in policy class map configuration mode, the CBS is 512, the more than cir rate will send and do nothing for packets.

Switch (config)#policy burst 1 512

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 burst-group 1

5.14.22 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 command deletes the specified aggregate policy.

Parameters: <*aggregate-policy-name*> is the policy set name.

Default: No policy 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

5.14.23 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: Policy class map opertion can be done in 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

5.14.24 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 or deletes all the policy maps applied on the ingress direction of the port .

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

no command will delete all the policy maps applied on the ingress direction of the port if there is not the specified policy map name.

Default: No policy map is bound to port 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 port1/1.

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

5.14.25 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 or deletes all the policy maps applied in the ingress direction of the vlan interface .

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

vlan <vlan-list> the vlan list of binding policy map.

no command will deletes all the policy maps applied in the ingress direction of the vlan interface if there is not the specified policy map name.

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

5.14.26 set

Function

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, do not distinguish v4 and v6.

ip precedence <new-precedence> new IP Precedence.

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 Precedence of the packets matching 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

5.14.27 show class-map

Command: show class-map [<*class-map-name*>]

Function: Displays class map of QoS.

Parameters: <*class-map-name*> is the class map name.

Default: N/A.

Command mode: Admin Mode.

Usage Guide: Displays all configured class-map or specified class-map information.

Example:

Switch # show class-map

Class map name:c1, used by 1 times

match acl name:1

Displayed information	Explanation
Class map name:c1	Name of the Class map
used by 1 times	Used times
match acl name:1	Classifying rule for the class map.

5.14.28 show policy-map

Command: show policy-map [<*policy-map-name*>]

Function: Displays policy map of QoS.

Parameters: <*policy-map-name*> is the policy map name.
Default: N/A.
Command mode: Admin Mode.
Usage Guide: Displays all configured policy-map or specified policy-map information.
Example:

```
Switch#show policy-map
Policy Map c1, used by 0 time(s)
Policy Map p1, used by 0 time(s)
   Class Map name: c1
            policy CIR: 20000 CBS: 2000
       conform-action:
         transmit
       exceed-action:
         drop
```

Displayed information	Explanation
Policy Map p1	Name of policy map
Class map name:c1	Name of the class map referred to
policy 20000 2000	Policy implemented
used by 0 port	Number of port that use the policy

5.14.29 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.
Default: N/A.
Command mode: Admin Mode.
Usage Guide: There is only red or green when packets passing police. In the print information, in packets means classify packets numbers and not supports the statistic information of color.
Example:

```
Switch#show mls qos interface ethernet 1/0/1
Ethernet1/0/1:
Default COS: 0
Trust: COS
Attached Policy Map for Ingress: p1
Classmap              classified(in packets)
c1                    0
Rule    ID            classified(in packets)
```

Function （If there is no Accounting for Class Map, show NA）

Egress 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          1       2       3       4       5       6       7       8
  ------------------------------------------------------------
WrrWeight   1       2       3       4       5       6       7       8
WdrrWeight 1       2       4       8       16      32      64      64

Bandwidth Guarantee Configuration:
Queue       1          2          3          4          5          6          7          8
  ------------------------------------------------------------------
MinBW(K) 0          0          0          0          0          0          0          0
MaxBW(K) 0          0          0          0          0          0          0          0
```

Display Information	Explanation
Ethernet1/0/2	Port name
default cos:0	Default CoS value of the port
Trust: COS	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 , WDDR or PQ queue out method
Queue weights	Queue weights configuration
Bandwidth Guarantee Configuration	Bandwidth guarantee configuration

Switch(config)#show mls qos interface ethernet1/0/2 queuing
Ethernet1/0/2:

Egress 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

WrrWeight 1 2 3 4 5 6 7 8

WdrrWeight 10 20 40 80 160 320 640 1280

Bandwidth Guarantee Configuration:

Queue 1 2 3 4 5 6 7 8

MinBW(K) 0 0 0 0 0 0 0 0

MaxBW(K) 0 0 0 0 0 0 0 0

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

Switch # show mls qos interface ethernet 1/0/2 policy

Ethernet1/0/2:

Attached Policy Map for Ingress: p1

Accounting: ON

Classmap classified in-profile out-profile (in packets)

c1 0 0 0

Display Information	Explanation
Ethernet1/0/2	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 packets)
   c1                      0
   Rule    ID              classified(in packets)
```

5.14.30 show mls qos in {interface <interface-name> policy | vlan <vlan-id>

Command: show mls qos in {interface <interface-name> policy | vlan <vlan-id>
Function: Show the policy configuration information of the in direction of port or vlan.
Parameters: <interface-name>: port name.
Command Mode: Admin and configuration mode
Default: None.
Usage Guide: Show the policy configuration information of the in direction.
Example: Show the policy configuration information of the in direction.

```
Switch#show mls qos in interface ethernet1/0/1 policy
Ethernet1/0/1:
Attached Policy Map for Ingress: p
```

5.14.31 show mls qos interface wred

This command is not supported by the switch.

5.14.32 show mls qos maps

Command: show mls qos maps [cos-intp | cos-dp | dscp-intp | dscp-dp | dscp-dscp] | [begin | include | exclude <regular-expression>]
Function: Display the configuration of QoS mapping.
Parameters: cos-intp: The mapping from ingress L2 **CoS** to internal priority
cos-intp: The mapping from ingress L2 CoS to drop priority
dscp-intp: **The** mapping from ingress DSCP to internal priority
dscp-intp: The mapping from ingress DSCP to drop priority
intp-dscp: The mapping from outgress internal to DSCP priority

Default: None.

Command mode: Admin and Configuration **Mode**.

Usage Guide: Display the map configuration information of QoS**.**

Example: Display configuration information of the mapping table.

Ingress COS-TO-Internal-Priority map:

COS: 0 1 2 3 4 5 6 7

INTP: 0 1 2 3 4 5 6 7

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 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-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

5.14.33 show mls qos vlan

Command: show mls qos vlan <v-id>
Parameters: v-id: the ranging from 1 to 4094.
Command Mode: Admin mode.
Default: None.
Example:
Switch# show mls qos vlan 1
Vlan 1:
Attached Policy Map for Ingress: 1
Classmap classified(in packets)
c1 0
Rule ID classified(in packets)

Switch# show mls qos vlan 7
Vlan 7:
Attached Policy Map for Ingress: 7
Classmap classified(in packets)
C7 0
Rule ID classified(in packets)

5.14.34 show mls qos aggregate-policy

Command: show mls qos aggregate-policy [<aggregate-policy-name>]

Function: Display the aggregate-policy configuration information of QoS.
Parameters: <aggregate-policy-name> is the aggregate policy name.
Default: None.
Command Mode: Admin mode and configuration mode.
Usage Guide: Display all configured **aggregate-policy** or appointed **aggregate-policy** information.
Example:
Switch(config)#show mls qos aggregate-policy a2
aggregate policy a2
CIR: 1000 CBS: 1024
conform-action:

transmit
exceed-action:
drop
Not used by any policy map

Display Information	Explanation
aggregate policy a2 CIR: 1000 CBS: 1024 conform-action: transmit exceed-action: drop	The configuration of aggregate policy.
Not used by any Policy Map	The referenced times of aggregate policy.

5.14.35 transmit

Command: transmit
no transmit
Function: Transmit data package that match the class, the no command cancels the assigned action.
Parameters: None.
Default: Do not set the action.
Command mode: Policy class map configuration mode
Usage Guide: Send the packet directly after configure this command.
Example: Send the packet which satisfy c1.
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#transmit
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit

5.15 Flow-based Redirection

5.15.1 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 MAC ACL, digital extensive MAC ACL, nomenclatural standard MAC **ACL**, nomenclatual extensive MAC, digital standard IPv6 ACL, and nomenclatural standard IPv6 ACL. Parameters of ***Timerange*** **and** Portrange cannot 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.

Notice: Redirect does not support redirect flow to the 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 1/0/1

Switch(Config-If-Ethernet1/0/1)# access-group 1 redirect to interface ethernet 1/0/6

5.15.2 match vlan <1-4096> redirect interface (ethernet|) IFNAME

This command is not supported by the switch.

5.15.3 port-redirect match vlan <1-4094> source-port interface (ethernet|) IFNAME destination-port interface (ethernet|) IFNAME

This command is not supported by the switch.

5.15.4 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 1/0/1:

RX flow (access-list 1) is redirected to interface Ethernet1/0/6

5.15.5 vlan-port-redirect vlan maximum <1-1000>

This command is not supported by the switch.

5.16 Flexible QinQ

5.16.1 Add

Command: add s-vid <new-vid>

no add s-vid

Function: Add specified tunnel tag for data packets of mapped classify table, the no command cancel configuration.

Parameters: s-vid <new-vid> appointed VID of tunnel VLAN Tag.

Default: The default is not add tag.

Command Mode: Policy classify table configuration mode.

Usage Guide: After configured the command, add appointed tunnel tag or inner tag for packets of mapping classify table. When use QinQ function, the data packets that sent only have inner VLAN Tag or no Tag, it needs add s-vid commands to add appointed tunnel VLAN Tag, otherwise data have not tunnel VLAN in switch.

Example: Add a VLAN Tag that VID is 2 to satisfied c1 classify rule packets.

Switch(config)#policy-map p1

Switch(Config-PolicyMap-p1)#class c1

Switch(Config-PolicyMap-p1-Class-c1)#add s-vid2

5.16.2 delete

This command is not supported by the switch.

5.16.3 Match

Command: match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| ipv6 access-group <*acl-index-or-name*> | ipv6 dscp <dscp-list> | ipv6 *flowlabel* <flowlabel-list> | *vlan* <vlan-list> | *cos* <cos-list> }

no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp
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 command deletes the specified match standard.

Parameter: access-group <*acl-index-or-name*> match the specified IP ACL or MAC –IP ACL or standard IPV6 ACL, the parameters are the number or name of ACL

ip dscp <*dscp-list*> and **ipv6 dscp <*dscp-list*>** match the specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values, the ranging is 0 to 63

ip precedence <*ip-precedence-list*> match the specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0 to 7

ipv6 access-group <*acl-index-or-name*> match the specified IPv6 ACL, the parameter is the number or name of IPv6 ACL

ipv6 flowlabel <flowlabel-list> match the specified IPv6 flow label, the parameter is IPv6 flow label value, the ranging is 0 to 1048575

vlan <*vlan-list*> match the specified VLAN ID of the external VLAN Tag, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the ranging is 1 to 4094

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

c-vlan <vlan-list> match the specified customer VLAN ID, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the ranging is 1 to 4094

Default: There is no match standard.

Command Mode: Class-map Mode

Usage Guide: Only one match standard can be configured in a class map. When configuring the ACL match, permit rule is the match option, it will apply Policy Map action. Deny rule is the excluding option, it does not apply Policy Map action. If it has been configured other match rule, the operation is failure, but configuring the same match rule will cover the previous.

Example: Create a class-map named c1, and configure the class rule of the 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

5.16.4 service-policy

Command: service-policy <*policy-map-name*> in

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

Function: Bind the specified policy of flexible QinQ to the ingress of the port, the no command cancels the binding.

Parameters: service-policy <*policy-map-name*>: The specified policy-map name of flexible QinQ.

Default: No policy map is bound to port.
Command mode: Port Mode.
Usage Guide: Only one policy map can be bound to each port, the function takes effect after the policy map is bound to a port. At present, do not support the configuration with add commend and delete command in policy.
Example: Apply policy-map p1 (p1 corresponds with the action that modify s-vid) to Ethernet port 1/0/1 for flexible QinQ.
Switch(Config-If-Ethernet1/0/1)#dot1q-tunnel enable
Switch(Config-If-Ethernet1/0/1)#service-policy p1 in

5.16.5 set

Command: set {s-vid <new-vid> | cos <*cos-list*>|drop-precedence<dp-list>|internal-priority<inp-list>|ip{dscp<dscp-list>|precedence <pri-list>}|s-tpid<tpid-list> }
no set{s-vid| cos |drop-precedence|internal-priority|ip{dscp|precedence}|s-tpid }
Function: Assign the new cos and vid value to the packets which match the class map, no command cancels the operation.
Parameters: s-vid: modify tunnel VID of VLAN Tag; cos: modify cos value of packets; **drop-precedence:** modify drop priority; **internal-priority:** modify inner priority; **ip:** modify ip dscp value or precedence value; **s-tpid:** modify tunnel tpid value of packets.
Default: Do not modify the value.
Command Mode: Policy class-map configuration mode
Usage Guide: Only modify the new value again for the classified flow that correspond the match standard.
Example: Set an external VLAN Tag' VID as 3 for the packet which satisfy c2 class rule.
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c2
Switch(Config-PolicyMap-p1-Class-c2)#set s-vid 3
Switch(Config-PolicyMap-p1-Class-c2)#exit

Chapter 6 Commands for Reliability

6.1 MSTP

6.1.1 MSTP

6.1.1.1 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)#

6.1.1.2 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)#

6.1.1.3 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 64; in the command "**no instance *<instance-id>* [vlan *<vlan-list>*]**", ***<instance-id>*** sets the instance number. The valid number is from 0 to 64. ***<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 64 MSTIs (except for CISTs). CIST can be treated as MSTI 0. All the other instances are considered as instance 1 to 64.

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

6.1.1.4 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)#name mstp-test

6.1.1.5 no

Command: no <*instance-id*> | <*name*> | <*revision-level*>

Function: Cancel one command or set it as initial value.

Parameter: ***<instance-id>*** instance number, ***<name>*** MSTP region name, ***<revision-level>*** is account the modify value of MST configuration caption.

Command mode: MSTP Region Mode

Default: The default revision level is 0.

Usage Guide: This command deletes the specified instance and MSTP region name, restore the default of modify value is 0.

Example: Delete instance 1.

Switch(Config-Mstp-Region)#no instance 1

6.1.1.6 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

6.1.1.7 show

Command: show

Function: Display the information of current running system.

Command mode: MSTP Region Mode.

Usage Guide: This command can check the detail information of system.

Example: Display the information of current running system.

Switch(Config-Mstp-Region)#show

6.1.1.8 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 interface1/0/2.

Switch(config)#spanning-tree

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#no spanning-tree

6.1.1.9 spanning-tree cost

Command: spanning-tree cost *<cost>*

no spanning-tree cost

Function: Sets path cost of the current port; the command "**no spanning-tree cost**" restores the default setting.

Parameter: ***<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

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

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 port and the designated port of the instance.

Example: On the port1/0/2, set the port cost is 3000000.

Switch(Config-If-Ethernet1/0/2)#spanning-tree cost 3000000

6.1.1.10 spanning-tree cost-format

This command is not supported by the switch.

6.1.1.11 spanning-tree digest-snooping

Command: spanning-tree digest-snooping

no spanning-tree digest-snooping

Function: Configure the port to use the authentication string of partner port; the command "**no spanning-tree digest-snooping**" restores to use the port generated authentication string.

Parameter: None

Command mode: Port Mode

Default: Don't use the authentication string of partner port.

Usage Guide: According to MSTP protocol, the region authentication string is generated by MD5 algorithm with public authentication key, intstance ID, VLAN ID. Some manufactory don't use the public authentication key, this causes the incompatibility. After the command is executed the port can use the authentication string of partner port, realize compatibility with these manufactories equipment.

Note: Because the authentication string is related to instance ID and VLAN ID, the command may cause recognizing the equipment that with different instance and VLAN relation as in the same region. Before the command is executed, make sure that instance and VLAN relation is accord for

all the equipment. If there are more than one equipment connected, all the connected ports should execute this command.

Example: Configure the authentication string of partner port.

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#spanning-tree digest-snooping

Switch(Config-If-Ethernet1/0/2)#

6.1.1.12 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.

Command Mode: Port Mode

Default: Auto Packet Format.

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 1/0/2

Switch(Config-If-Ethernet1/0/2)#spanning-tree format standard

Switch(Config-If-Ethernet1/0/2)#

6.1.1.13 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

6.1.1.14 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

6.1.1.15 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 1/0/7-8 as point-to-point type.

Switch(config)#interface ethernet 1/0/7-8

Switch(Config-Port-Range)#spanning-tree link-type p2p force-true

6.1.1.16 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

6.1.1.17 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

6.1.1.18 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 1/0/2 to run in the MSTP mode.

Switch(Config-If-Ethernet1/0/2)#spanning-tree mcheck

6.1.1.19 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

6.1.1.20 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)#

6.1.1.21 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 0-64. <cost> sets ***path cost***, different cost formats have different ranges. For the default dot1t **mode** the valid range is 1-200,000,000, and for dot1d is 1-65535.

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

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

Port Speed	Port Type	Port Cost	
		802.1D-2008	802.1T
0		65535	200,000,000
10Mbps	Half- duplex Full- duplex aggregation link with 2 ports aggregation link with 3 ports aggregation link with 4 ports	100 99 95 95 95	2,000,000 1,999,999 1,000,000 666,666 500,000
100Mbps	Half- duplex Full- duplex	19 18	200,000 199,999

	aggregation link with 2 ports aggregation link with 3 ports aggregation link with 4 ports	15 15 15	100,000 66,666 50,000
1000Mbps	Full- duplex aggregation link with 2 ports aggregation link with 3 ports aggregation link with 4 ports	4 3 3 3	20,000 10,000 6,666 5,000

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 port1/0/2, set the MSTP port cost in the instance 2 to 3000000.

Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 2 cost 3000000

6.1.1.22 spanning-tree cost-format

Command: spanning-tree cost-format {dot1d | dot1t}

Function: In global mode, users can select path-cost format with dot1d or dot1t, the default format is dot1t.

Command Mode: Global mode.

Default: count path-cost with dot1t format.

Usage Guide: There are two formats about cost value: they are dot1d marked on IEEE802.1d-2008 and dot1t marked on IEEE802.1t, but path-cost ranges of them are different, dot1d range from 1 to 65535, and dot1t range from 1 to 200,000,000.

If users already configured the cost value of link with **spanning-tree cost** command manually, changing path-cost format with **cost-format** command is successful after the previous configuration is cleared only.

Example: Set the cost format in global mode

Switch(config)#spanning-tree cost-format dot1d

6.1.1.23 spanning-tree mst loopguard

Command: spanning-tree [mst <instance-id>] loopguard

no spanning-tree [mst <instance-id>] loopguard

Function: Enable the loopguard function for specified instance, the no command disables this function.

Parameter: ***<instance-id>***: MSTP instance ID.

Command mode: Port Mode.

Default: Disable loopguard function.

Usage Guide: The command can avoid root port or alternate port to be changed as designated port due to invalid unilateralism link. When the receiving timer is time, the configured port with loopguard is set as block state.

Example: Configure port 1/0/2 as loopguard mode for instance 0.

Switch(Config)#interface ethernet 1/0/2

Switch(Config-Ethernet-1/0/2)#spanning-tree mst 0 loopguard

Switch(Config-Ethernet-1/0/2)#

6.1.1.24 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 1/0/2 for the instance 1.

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 1 port-priority 32

6.1.1.25 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

6.1.1.26 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 1/0/2 in instance 0.

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 0 rootguard

Switch(Config-If-Ethernet1/0/2)#

6.1.1.27 spanning-tree portfast

Command: spanning-tree portfast [bpdufilter | bpduguard] [recovery <30-3600>]

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

recovery: configure the border port can be recovered automatically after implement bpduguard violation operation

<30-3600>: the recovery time, do not recover it by default

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 guard, the recovery time as 60s.

Switch(config)#interface ethernet 1/0/2

Switch(Config-If-Ethernet1/0/2)#spanning-tree portfast bpduguard recovery 60
Switch(Config-If-Ethernet1/0/2)#

6.1.1.28 spanning-tree port-priority

Command: spanning-tree port-priority *<port-priority>*

no spanning-tree port-priority

Function: Set the port priority; the command "**no spanning-tree port-priority**" restores the default setting.

Parameter: ***<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, 48…240.

Command mode: Port Mode

Default: The default port priority is 32768.

Usage Guide: By setting the port priority to designated port. The lower the value of the port priority is, the higher the priority is.

Example: Set the port priority as 4096 on the port 1.

Switch(Config-If-Ethernet1/0/1)#spanning-tree port-priority 4096

6.1.1.29 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

6.1.1.30 spanning-tree rootguard

Command: spanning-tree rootguard

no spanning-tree rootguard

Function: Set the port is root port, "**no spanning-tree rootguard**" command sets the port is non-root port.

Parameter: None.

Command mode: Port Mode.

Default: Port is non-root port.

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: Set the port 1 is root port.

Switch(Config-If-Ethernet1/0/1)#spanning-tree rootguard

6.1.1.31 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)#

6.1.1.32 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 1/0/2

Switch(Config-If-Ethernet1/0/2)#spanning-tree tcflush disable

Switch(Config-If-Ethernet1/0/2)#

6.1.1.33 spanning-tree transmit-hold-count

Command: spanning-tree transmit-hold-count <*tx-hold-count-value*>

no spanning-tree transmit-hold-count

Function: Set the max transmit-hold-count of port.

Parameter: tx-hold-count-value: ranging from 1 to 20, the default value is 10.

Command mode: Global Mode

Default: 10.

Usage Guide: Set the max number for sending BPDU within the Hello Time interval to control BPDU flow. The variable is used to whole MST bridge.

Example: Set the max transmit-hold-count as 20.

Switch(config)#spanning-tree transmit-hold-count 20

6.1.2 Monitor and Debug

6.1.2.1 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, and 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 port1/0/1.

Switch#debug spanning-tree

Switch#debug spanning-tree bpdu rx interface e1/0/1

6.1.2.2 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)#
```

6.1.2.3 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: 03: 0f: 01: 0e: 30
Bridge Times :   Max Age 20, Hello Time 2, Forward Delay 15
Force Version:   3

############################## Instance 0 ##############################
Self Bridge Id     : 32768 -    00: 03: 0f: 01: 0e: 30
```

```
Root Id              : 16384.00: 03: 0f: 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:
Ethernet1/0/1 Ethernet1/0/2 (Total 2)

 PortName         ID         ExtRPC    IntRPC   State Role       DsgBridge        DsgPort
-------------- ------- --------- --------- --- ---- ------------------ -------
 Ethernet1/0/1   128.001             0           0 FWD ROOT 16384.00030f010f52 128.007
 Ethernet1/0/2   128.002             0           0 BLK ALTR 16384.00030f010f52 128.011

############################## Instance 3 ##############################
Self Bridge Id     : 0.00: 03: 0f: 01: 0e: 30
Region Root Id     : this switch
Int.RootPathCost : 0
Root Port ID       : 0
Current port list in Instance 3:
Ethernet1/0/1 Ethernet1/0/2 (Total 2)

   PortName         ID       IntRPC     State Role       DsgBridge        DsgPort
-------------- ------- --------- --- ---- ------------------ -------
 Ethernet1/0/1   128.001             0 FWD MSTR       0.00030f010e30 128.001
 Ethernet1/0/2   128.002             0 BLK ALTR       0.00030f010e30 128.002

############################## Instance 4 ##############################
Self Bridge Id     : 32768.00: 03: 0f: 01: 0e: 30
Region Root Id     : this switch
Int.RootPathCost : 0
Root Port ID       : 0
Current port list in Instance 4:
Ethernet1/0/1 Ethernet1/0/2 (Total 2)

   PortName         ID       IntRPC     State Role       DsgBridge        DsgPort
-------------- ------- --------- --- ---- ------------------ -------
 Ethernet1/0/1 128.001             0 FWD MSTR 32768.00030f010e30 128.001
 Ethernet1/0/2 128.002             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

6.1.2.4 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

6.1.3 MSTP Spanning-tree Process

6.1.3.1 spanning-tree process

Command: spanning-tree process <process-id>
no spanning-tree **process <process-id>**
Function: Create the new mstp process.
Parameters: process-id: the range is 1-31.
Command Mode: Global Mode.
Default: None.
Usage Guide: Create the new mstp process. Multiple mstp processes can be configured on one device and each process is standalone. The process 0 exists only as default.
Example: Create the new mstp process 1.
Switch(config)#spanning-tree process 1

6.1.3.2 spanning-tree tc-notify process0

Command: spanning-tree tc-notify process0
no spanning-tree tc-notify **process0**
Function: The process N notifies tc to the instance in mstp process 0.
Parameters: None.
Command Mode: mstp process mode.
Default: None.
Usage Guide: When there is a change in mstp process N, the device will receive the tc packet, at the same time, the process N will notify tc to the instance in mstp process 0 on the shared link. It makes the process 0 refresh the table entry for ensuring the traffic not to break off.
Example: Configure to notify TC of process 1 to process 0.
Switch(Config-Mstp-Process-1)#spanning-tree tc-notify process0

6.1.3.3 spanning-tree binding-process

Command: spanning-tree binding-process <process-id>
no spanning-tree **binding-process <process-id>**
Function: Add the port into the process N.
Parameters: process-id: the range is 1-31.
Command Mode: Port Mode.
Default: All the ports belong to process 0.

Usage Guide: Configure the port to join the appointed mstp process N. The port will enter into process N from the process 0. This command is mutually exclusive to the shared port configuration command (link-share).

Example: Add the Ethernet1/0/2 into process 1.

Switch(Config-If-Ethernet1/0/2)#spanning-tree binding-process 1

6.1.3.4 spanning-tree binding-process link-share

Command: spanning-tree binding-process < process-id > link-share

no **spanning-tree binding-process < process-id > link-share**

Function: Configure the port belong to the shared port of process N.

Parameters: process-id: the range is 1-31.

Command Mode: Port Mode.

Default: The port is only in the mstp calculating of process 0.

Usage Guide: Configure the port belong to the shared port of process N. Except for process 0, the configured port can be in the mstp calculating of multiple processes, but the port status can be only configured by process 0. This command can be configured for more than once.

Example: Configure the Ethernet1/0/2 as the shared port of process 1 and 0.

Switch(Config-If-Ethernet1/0/2)#spanning-tree binding-process 1 link-share

6.2 ERPS

6.2.1 ethernet tcn-propagation erps to {erps | stp}

Command: ethernet tcn-propagation erps to {erps | stp}

no ethernet tcn-propagation erps to

Function: Configure the topology changing transmission notification method. Currently, the R-APS event notification among the ERPS rings is supported and it is used for the sub ring topology to send R-APS event packets to the interconnection ring after changing to notify the neighbor ring. The topology changing only takes effect in this ring as default but not be transmitted out of the ring. It does not affect the neighbor topology connected to it. The no command deletes this notification method.

Parameters: erps: topology changing sends the R-APS event packets to notify the connection ring of this device; stp: topology changing sends the stp packets to notify the stp topology connected to this device.

Default: ERPS ring topology changing only takes effect in this ring but does not send the notification packets.

Command Mode: Global Mode.

Usage Guide: Configure the topology changing transmission notification method supported by this device as the appointed method. The ERPS ring instance detects the changing, it will send the notification packets. If configured erps method, it will send the R-APS event packets to other

ERPS rings; if configured stp method, it will send the stp packets outward.

Example:

Configure to send R-APS event notification to the interconnection ring after the topology changing.

Switch(config)#ethernet tcn-propagation erps to erps

Configure to send STP notification to the interconnection ring after the topology changing.

Switch(config)#ethernet tcn-propagation erps to stp

Delete the topology changing transmission notification method.

Switch(config)#no ethernet tcn-propagation erps to

6.2.2 erps-ring <ring-name>

Command: erps-ring < *ring-name* >

no erps-ring < *ring-name* >

Function: Create ERPS ring and enter into the ERPS ring configuration mode. If the ERPS ring has existed, enter into the ERPS ring configuration mode. The no command deletes the ERPS ring.

Parameters: <*ring-name*>: the ERPS ring name created. The maximum character number is 64 and it is made up with letters, numbers and the underlines. The first and last character cannot be the underline.

Command Mode: Global Mode.

Default: Do not configure any ERPS ring.

Usage Guide: If the inputted string of ring name exceeds 64 bytes, there will be the message of "Valid ERPS ring name should be no more than 64 bytes!" If the inputted string format of ring name is not lawful, there will be the message of "Invalid ERPS ring name!" If the total number of ERPS rings configured has reached the maximum value, there will be the message of "Support ERPS ring max number: 32!" If the ERPS ring existed, enter into the ERPS ring configuration mode, otherwise, create it and enter into the ERPS ring configuration mode.

Example:

Create the ERPS ring of ring1

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#

Delete the EPRS ring of ring1

Switch(config)#no erps-ring ring1

6.2.3 version {v1 | v2}

Command: version {v1 | v2}

no version

Function: Configure the supported version of the ERPS ring. Currently it achieves the newest version of v2 and it can be compatible with v1. V1 does not support the management commands of MS, FS, etc. It does not support the multi-instance either. But it supports the Revertive switch only. If the instance is not configured on ERPS ring, the version can be configured multiple times and subject to the last time. If the ERPS ring instance has configured on the ring, the version

cannot be modified. The no command recovers to be the default status of v2.

Parameters: {v1 | v2}: parameters selection. V1 means to support v1 which is released in 2008-06 and the amendment (2009-04). v2 means to support v2 which is released in 2010-03 and the amendment (2010-06).

Command Mode: ERPS Ring Configuration Mode.

Default: V2.

Usage Guide:

1. If configured ERPS ring instance on this ERPS ring, there will be the message of “Cann't config version on ERPS ring whitch has ERPS instance, please delete ERPS instance firstly!” Otherwise, enter into the next step;

2. Configure the ERPS ring to support the appointed protocol version;

3. If configured ERPS ring to support v1, this ring will not support multi-instance. ERPS ring instance does not support the management commands of MS, FS, etc. and the non-revertive switch is not effective. It only support revertive switch.

4. If configured ERPS ring to support v1, the instance of this ring will deal with the ERPS packets according to the v1 format. Package the R-APS packets and resolve the fields according to v1 format. The fields defined by v2 will not be dealt.

Example:

Configure the ERPS ring of ring1 to support v1

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#version v1

Configure the ERPS ring of ring1 to support v2

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#version v2

Delete v1 supported by the ERPS ring of ring1

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#no version

6.2.4 open-ring

Command: open-ring

no open-ring

Function: Configure the ERPS ring as the sub ring of open type. If configured ERPS ring instance on the ring, the ERPS ring type cannot be modified, the instance must be deleted first. The configuration of all the nodes in the ring must be the same; this type of ERPS can connect to other ERPS rings to be used in the interconnection topology. The no command deletes this configuration and recovers to be the default major ring of close type.

Parameters: None.

Command Mode: ERPS Ring Configuration Mode.

Default: The ERPS ring is major ring of close type as default.

Usage Guide: If the ERPS ring instance has been configured on the ring, there will be the message of “Cann't config open-ring on ERPS ring whitch has ERPS instance, please delete ERPS instance firstly!” Otherwise, enter into the next step. Configure this ERPS ring type as sub ring.

Example:

Configure the ERPS ring of ring1 as sub ring of open type.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#open-ring

Delete the configuration of the sub ring of open type.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#no open-ring

6.2.5 raps-virtual-channel {with | without}

Command: raps-virtual-channel {with | without}

Function: Configure if there is the R-APS virtual channel in ERPS ring. Configure it only on all the nodes of the sub ring and the configuration must be the same.

Parameters: {with | without}: parameter selection. If select with, the R-APS virtual channel is existed in this ERPS ring; if select without, the R-APS virtual channel is not existed in this ERPS ring.

Command Mode: ERPS Ring Configuration Mode.

Default: The R-APS virtual channel is not existed in ERPS ring.

Usage Guide:

a) If it is major ring, there will be the message of “Cann't config R-APS virtual channel on ERPS major ring!”

b) Configure if there is the R-APS virtual channel in ERPS ring according to the configuration.

Inputting: Success or error. If there is not R-APS virtual channel on the ERPS ring, the R-APS channel of all the instances of ERPS ring will be unblocked forever and it only blocks the data channel; otherwise, the R-APS channel and the data channel will be blocked at the same time.

Example:

Configure that there is R-APS virtual channel in the ERPS sub ring of ring1.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#raps-virtual-channel with

6.2.6 erps-ring <ring-name> port0 [port1-none]

Command: erps-ring <ring-name> port0 [port1-none]

no erps-ring <ring-name> port0

Function: Configure the port0 of the ERPS ring node. There is only one port0 on each node. If the port0 has existed, the current configuration will not be covered and there will be only the error notice. If configured port1-none, it means there is no port0 on this ring, and it is the interconnection node. The no command deletes the port0.

Parameters: <ring-name>: ERPS ring name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines.

[port1-none]: there is only the port0 on this ERPS ring node, no port1 and it is the interconnection node.

Command Mode: Port Mode.。

Default: Do not configure port0 on ERPS ring.

Usage Guide:

If the inputted string of ring name exceeds 64 bytes, there will be the message of "Valid ERPS ring name should be no more than 64 bytes!"

If the inputted string format of ring name is not lawful, there will be the message of "Invalid ERPS ring name!"

If enabled stp mutual exclusion, there will be the message of "Port %s has enable stp or other mutex module!" %s is the port name;

If this port is the member port of aggregation port, there will be the message of "Port %s is LAG member port!" %s is the port name;

If the ERPS ring did not exist, there will be the message of "The ERPS ring doesn't exist!"

If the port0 has existed in ERPS ring, there will be the message of "Port0 exists on the ERPS ring already!"

If this port is configured as port1 of ERPS ring, there will be the message of "Port %s is already configed as port1 on the ERPS ring!" %s is the port name;

If this ERPS ring is not open-ring type, the port1-none cannot be configured, there will be the message of "Can not config port1-none on ERPS major ring!"

Configure this port as the port0 of the appointed ERPS ring;

Check if the ERPS ring configuration is integral; if it is integral, check if the ERPS instance configuration is integral; if it is integral, activate the instance as active and run the protocol.

Example:

Configure e 1/0/1 as the port0 of ERPS ring1

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#erps-ring ring1 port0

Delete the e 1/0/1 as port0 of ERPS ring1

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#no erps-ring ring1 port0

6.2.7 erps-ring <ring-name> port1

Command: erps-ring <ring-name> port1

no erps-ring <ring-name> port1

Function: Configure the port1 of the ERPS ring node. There is only one port1 on each node. If the port1 has existed, the current configuration will not be covered and there will be only the error notice. If configured port1-none, it means the configuration of port1 is not successful. The no command deletes the port1.

Parameters: <ring-name>: ERPS ring name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines.

Command Mode: Port Mode.。

Default: Do not configure port1 on ERPS ring.

Usage Guide:

If the inputted string of ring name exceeds 64 bytes, there will be the message of "Valid ERPS ring name should be no more than 64 bytes!"

If the inputted string format of ring name is not lawful, there will be the message of “Invalid ERPS ring name!”

If enabled stp mutual exclusion, there will be the message of “Port %s has enable stp or other mutex module!” %s is the port name;

If this port is the member port of aggregation port, there will be the message of “Port %s is LAG member port!” %s is the port name;

If the ERPS ring did not exist, there will be the message of “The ERPS ring doesn't exist!”

If the port1 has existed in ERPS ring, there will be the message of “Port1 exists on the ERPS ring already!”

If this port is configured as port0 of ERPS ring, there will be the message of “Port %s is already configed as port0 on the ERPS ring!” %s is the port name;

If configured port1-none on this ERPS ring, there will be the message of “Has configed port1-none on the ERPS open ring!”

Configure this port as the port1 of the appointed ERPS ring;

Check if the ERPS ring configuration is integral; if it is integral, check if the ERPS instances configuration is integral; if it is integral, activate the instance as active and run the protocol.

Example:

Configure e 1/0/1 as the port1 of ERPS ring1

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#erps-ring ring1 port1

Delete the e 1/0/1 as the port1 of ERPS ring1

Switch(config)#interface ethernet 1/0/1

Switch(config-if-ethernet1/0/1)#no erps-ring ring1 port1

6.2.8 failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep <mep-id> rmep<rmep-id>

Command: {port0 | port1} failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep <mep-id> rmep<rmep-id>

no {port0 | port1} failure-detect

Function: Configure the fault detection type of ERPS ring ports. If it is detected as cc type, the maintenance domain, maintenance set that cc belongs to and the monitoring link (it is conditioned with (mep-id, rmep-id)) should be appointed. The premise of this configuration is that the corresponding ring port has been joined into ERPS ring. The no command deletes the fault detection type of ERPS ring ports.

Parameters: {port0 | port1}: parameter selection. Port0 means the fault detection type of port0. Port1 means the fault detection type ofport1.

{cc | physical-link-or-cc}: parameter selection. cc means that the ERPS ring port detection is cc

report fault. physical-link-or-cc means that the ERPS ring port detection is cc report fault and physical link fault.

<domain-name>: the cfm domain name of ERPS ring port detection.

<ma-name>: the service name that cfm belongs to of ERPS ring port detection.

<mep-id>: the local mep id that cfm monitored of ERPS ring port detection.

<rmep-id>: the remote mep id that cfm monitored of ERPS ring port detection.

Command Mode: ERPS Ring Configuration Mode.

Default: ERPS ring port only detects the physical link fault as default.

Usage Guide:

If the inputted string of domain name exceeds 43 bytes, there will be the message of "Valid domain name should be no more than 43 bytes!"

If the inputted string format of domain name is not lawful, there will be the message of "Invalid domain name!"

If the inputted string of service name exceeds 45 bytes, there will be the message of "Valid service name should be no more than 45 bytes!"

If the inputted string format of service name is not lawful, there will be the message of "Invalid service name!"

If local mep and remote mep are the same, there will be the message of "The local mep can not be the same as the remote mep!" otherwise, enter into the next step;

Configure the fault detection type of ERPS ring ports as the appointed type. If the type is cc, save the configured md, ma, mep and rmep information to use for matching after receiving the cfm fault notification.

Example:

Configure the detection type of ERPS ring1 port0as cc.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#port0 failure-defect cc domain domain1 service serivice1 mep 1 rmep 2

Delete this configuration.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#no port0 failure-defect

6.2.9 erps-instance <instance-id>

Command: erps-instance <instance-id>

no erps-instance <instance-id>

Function: Create the ERPS ring instance and enter into the ERPS ring instance configuration mode. If this ERPS ring instance has existed, enter into the ERPS instance configuration mode. If ERPS ring supports v2, multiple ERPS ring instances can be configured. The no command deletes the ERPS ring instance.

Parameters: <instance-id>: id of ERPS ring, the range is 1 to 48.

Command Mode: ERPS Ring Configuration Mode.

Default: Do not configure any ERPS ring instance.

Usage Guide: If the ERPS ring supports v1, there will be the message of "Doesn't support multiple ERPS instance capability on the ring running version 1!" when configured more than one ERPS

instance.

If the configured instance exceeds the maximum ERPS instance number supported, there will be the message of “Support ERPS instance max number: 32 per ERPS ring!”

If the ERPS ring instance has existed on the ERPS ring, enter into the ERPS ring instance configuration mode;

Otherwise, create the corresponding ERPS ring instance and enter into the ERPS ring instance configuration mode.

Example:

Configure the ERPS ring instance 1 on ERPS ring1.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#

Delete the ERPS ring instance 1 on ERPS ring1.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#no erps-instance 1

Switch(config-erps-ring-inst-1)#

6.2.10 description

Command: description <instance-name>

no description <instance-name>

Function: Configure the description string of ERPS instance.

Parameters: <instance-name>: ERPS instance name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines. The no command deletes the ERPS instance name.

Command Mode: ERPS Instance Configuration Mode.

Default: Do not configure the ERPS instance name as default.

Usage Guide: Judge the length of the string, if exceed 64, there will be the message of “Valid ERPS instance name should be no more than 64 bytes!” if the string format is not lawful, there will be the message of “Invalid ERPS instance name!” otherwise, configure the ERPS instance name as the appointed string.

Example:

Configure the ERPS instance1 name on ring1 as instance1.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)# description instance1

Delete this name of instance1.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)# no description

6.2.11 ring-id <ring-id>

Command: ring-id <ring-id>

no ring-id <ring-id>

Function: Configure the last byte of R-APS packets destination MAC address sent by ERPS ring node to carry ring-id. If ERPS ring supports v1, ring-id only can be configured as 1. The no command configures it not to carry the ring-id, it means that the MAC is 01-19-A7-00-00-01.

Parameters: <ring-id>: ERPS ring id and the range is 1 to 64.

Command Mode: ERPS Instance Configuration Mode.

Default: The MAC address is 01-19-A7-00-00-01 as default.

Usage Guide: If ERPS ring supports v1, ring-id only can be configured as 1. Because v1 only supports the destination MAC address of 01-19-A7-00-00-01, otherwise, there will be the message of "Cann't config ringid other than 1 on the ERPS ring running version 1!"

If ERPS ring supports v2, configure the last byte of R-APS packets destination MAC address sent by ERPS ring node to carry the appointed ring-id.

Example:

Configure the last byte of R-APS packets destination MAC address sent by ERPS ring1 instance2 to carry the ring-id 2.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 2

Switch(config-erps-ring-inst-2)#ring-id 2

Configure the last byte of R-APS packets destination MAC address sent by ERPS ring1 instance2 not to carry the ring-id, it means the destination MAC is 01-19-A7-00-00-01.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 2

Switch(config-erps-ring-inst-2)#no ring-id

6.2.12 rpl {port0 | port1} {owner | neighbour}

Command: rpl {port0 | port1} {owner | neighbour}

no rpl {port0 | port1}

Function: Configure the member port of ERPS ring instance as RPL owner or RPL neighbour, the RPL node roles of different instances on the same ERPS ring cannot be configured on the same member port. The no command configures the member port of ERPS ring instance as the ordinary transmission port member.

Parameters: {port0 | port1}: parameter selection. Port0 means the RPL role of port0 in ERPS ring instance; port1 means the RPL role of port1 in ERPS ring instance.

{owner | neighbour }: parameter selection. Owner means to configure the appointed member port as rpl owner; neighbour means to configure the appointed member port as rpl neighbour.

Command Mode: ERPS Instance Configuration Mode.

Default: None, it is the ordinary transmission node type.

Usage Guide: If configured port1-none, the node role of port1 cannot be configured, there will be the message of "Has configed port1-none on the ERPS open ring!"

If this instance node is already rpl owner or rpl neighbour, cannot run this command to any member port, there will be the message of "Has configed port rpl role: %s on the ERPS

instance!" %s is the configured rpl role;

If other instance has configured the appointed rpl role on the ERPS ring, there will be the message of "Has configed port rpl role: %s in this or other ERPS instance on the ERPS ring!" configure the appointed member port on the ERPS ring of that instance as the appointed node role.

Example:

Configure the port0 of ERPS ring1 instance1 as RPL owner node.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)# rpl port0 owner

Configure the port0 of ERPS ring1 instance1 as the ordinary transmission port role.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)# no rpl port0

6.2.13 non-revertive

Command: non-revertive

no non-revertive

Function: Configure the ERPS ring instance as non-revertive. If this ERPS ring supports v1, this command is null and cannot be configured. The no command configures the ERPS ring instance as revertive. If this ERPS ring supports v1, this command is null. This command can be configured only on the RPL owner node of the sub ring.

Parameters: None.

Command Mode: ERPS Instance Configuration Mode.

Default: ERPS ring instance supports the revertive as default.

Usage Guide: If ERPS ring supports v1, there will be the message of "Cann't config non-revertive on the ERPS ring running version 1!"

If the ERPS ring supports v2, configure this ERPS ring instance to support the non-revertive.

Example:

Configure the ERPS ring1 instance1 to support the non-revertive.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#non-revertive

Delete this configuration.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no non-revertive

6.2.14 guard-timer <guard-times>

Command: guard-timer <guard-times>

no guard-timer

Function: Configure the Guard timer. The guard timer is used for the Ethernet node to avoid the error handling and the close loop according to the outdated R-APS packets. In the starting time of the timer, any R-APS packets received (the R-APS packets that the Request/State="1110" are except) will be dropped. The no command configures the guard timer as the default value.

Parameters: <guard-times>: the interval is 10ms and the range is 10ms to 2s.

Command Mode: ERPS Instance Configuration Mode.

Default: 500ms.

Usage Guide: If the timer is not enabled, configure the guard timer of ERPS ring instance as the appointed time; if it is enabled, configure the guard timer as the configuration value immediately. The timer will not be cleared, it will run still according to the last configuration time and this configuration will be effective next time.

Example:

Configure the guard timer of ERPS ring1 instance1 as 1s.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)guard-timer 100

Configure the guard timer of ERPS ring1 instance1 as the default value.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1) no guard-timer

6.2.15 holdoff-timer < holdoff-times>

Command: holdoff –timer <holdoff-times>

no holdoff -timer

Function: Configure the Holdoff timer. The Holdoff timer is used for the Ethernet node to block the default report time. When the new default happened or the default was more serious, this default will not be reported to the protection switching for handling immediately if the useful Holdoff timer is not 0, but enable the Holdoff timer. When the timer is time out, check if the link default in the timer starting still existed. If there is still the default, report it to handle it with protection switching, this default is not necessarily the one in the timer starting. The no command configures the Holdoff timer as the default value.

Parameters: <holdoff-times>: the interval is 1s and the range is 0 to 10s.

Command Mode: ERPS Instance Configuration Mode.

Default: 0s.

Usage Guide: If the timer is not enabled, configure the holdoff timer of ERPS ring instance as the appointed time; if it is enabled, configure the holdoff timer as the configuration value immediately. The timer will not be cleared, it will run still according to the last configuration time and this configuration will be effective next time.

Example:

Configure the Holdoff timer of ERPS ring1 instance1 as 5s.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#holdoff –timer 5

Configure the Holdoff timer of ERPS ring1 instance1 as the default value.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no holdoff –timer

6.2.16 wtr-timer <wtr-times>

Command: wtr-timer <wtr-times>

no wtr-timer

Function: Configure the WTR timer. WTR timer is used to avoid the frequent protection switching of RPL owner node because of the periodic (intermittent) default. When RPL owner port received the default recovery packets, after some time, and then check if the default still existed on the other nodes and prevent blocking RPL owner port immediately to cause the chokepoint shocking. The no command configures the WTR timer as the default.

Parameters: <wtr-times>: the interval is 1min and the range is from 1 to 12min.

Command Mode: ERPS Instance Configuration Mode.

Default: 5min.

Usage Guide: If the timer is not enabled, configure the WTR timer of ERPS ring instance as the appointed time; if it is enabled, configure the WTR timer as the configuration value immediately. The timer will not be cleared, it will run still according to the last configuration time and this configuration will be effective next time.

Example:

Configure the WTR timer of ERPS ring1 instance1 as 10min.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#wtr-timer 10

Configure the WTR timer of ERPS ring1 instance1 as the default value.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no wtr-timer

6.2.17 protected-instance

Command: protected-instance <instance-list>

no protected-instance <instance-list>

Function: Configure the protection instance of ERPS ring instance. ERPS ring instance can protect all the MSTP instances. The same instance cannot be quoted by multiple ERPS ring instances under the same topology. Under the same ERPS ring instance, run this command more than once to protect instance, the result will be accumulated. The no command deletes the protection instance of ERPS ring instance.

Parameters: <instance-list>: the MSTP instance list protected by ERPS ring instance, such as i, j-k. The number of the instances in the list is not limited.

Command Mode: ERPS Instance Configuration Mode.

Default: ERPS ring instance does not protect any MSTP instance.

Usage Guide: If the inputting instance has been protected by other ERPS instance, there will be the message of "Instance: %d is protected by erps instance: %d on ring: %s!" the first %d is mstp instance id and the second is erps instance id; %s is ERPS ring name;

Configure the protection instance of ERPS ring instance as the appointed MSTP instance;

Check if the ERPS instance configuration is complete, if it is complete, activate the instance as active, and run the protocol.

Example:

Configure the protection instance of ERPS ring1 instance1 as instance 2.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#protected-instance 2

Delete this configuration.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)#no protected-instance 2

6.2.18 raps-mel <level-value>

Command: raps-mel <level-value>

no raps-mel

Function: Configure the level of R-APS channel.

Parameters: <level-value>: the level value of APS packets, range is from 0 to 7.

Command Mode: ERPS Instance Configuration Mode.

Default: Level is 7.

Usage Guide: Configure the level of R-APS channel of ERPS ring instance as the appointed level. If configured successfully, the mel field of the R-APS packet sent by this ERPS ring instance will be added as the appointed level and only the R-APS packets with the level that is larger than or same as the appointed level can be allowed passing by, or notify the error. The no command configures the level as the default of 7. The MEL field in the protocol packets is used to detect if the current packet can pass by. If the MEL value configured in ERPS ring is letter than the value in the fault detection protocol, it means that the packet level is low and cannot pass by. The level configuration of all the nodes in the instance must be identical.

Example:

Configure the level of R-APS channel of ERPS ring1 instance1 as 5.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)raps-mel 5

Configure the level of R-APS channel of ERPS ring1 instance1 as 7.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)no raps-mel

6.2.19 control-vlan <vlan-id>

Command: control-vlan <vlan-id>

no control-vlan

Function: Configure the control vlan of R-APS packets of R-APS channel. In the ERPS ring instance, this vlan is only used to transmit ERPS protocol packets but not to forward the user business packets. It improves the ERPS protocol security. User makes sure the configuration uniqueness. This vlan is as the vlan tag when sending R-APS packets. The protection VLAN configuration of all the nodes in the instance must be identical. The no command deletes the control vlan.

Parameters: <vlan-id>: vlan id of R-APS packets, range is from 2 to 4094.

Command Mode: ERPS Instance Configuration Mode.

Default: Do not configure any control vlan.

Usage Guide: User configuration should meet the following situations:

The protection VLAN configuration of all the nodes in the instance must be identical;

The control vlan has uniqueness;

If the ring type with the instance is major ring, the control vlan and the protection vlan are in the same instance;

If the ring type with the instance is sub open-ring and it is the virtual channel method without R-APS, the control vlan belongs to one instance all alone;

The member port belongs to the control vlan and protection vlan.

The control vlan handling is as below:

a) If the inputting VLAN does not existed, there will be the message of “Error, VLAN %d does not exist!” %d is the inputting value;
b) If this ERPS ring instance has configured the control VLAN, there will be the message of “Control vlan has existed already!”
c) Configure the control VLAN of the ERPS ring instance as the appointed VLAN;
d) Check if the ERPS instance is integral, if it is integral, activate the instance as active and run the protocol.

Notice: The ordinary data vlan and the control vlan of the different erps instances cannot associated with the same MSTI.

Example:

Configure the control vlan of ERPS ring1 instance1 as vlan10.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)control-vlan 10

Delete this configuration.

Switch(config)#erps-ring ring1

Switch(config-erps-ring)#erps-instance 1

Switch(config-erps-ring-inst-1)no control-vlan

6.2.20 forced-switch {port0 | port1}

Command: forced-switch {port0 | port1}

Function: Run the forced switch on the port of ERPS ring node. Two or more forced switch are allowed existing at the same time in one ERPS ring instance. But only one forced switch command can be existed on one ring node. User should avoid using multiple forced switch in ERPS ring instance to cause the ERPS ring instance splitting.

Parameters: {port0 | port1}: parameter selection, port0 means to run the forced switch configuration on port0 of the ring node; port1 means to run the forced switch configuration on port1 of the ring node.

Command Mode: ERPS Instance Configuration Mode.

Default: No forced switch in ERPS ring instance.

Usage Guide: If this ring supports version1, there will be the message of "Doesn't support the command on the ring running version 1!" otherwise, enter into the next step;

If this instance configuration is not integral, it is on the status of unactive, there will be the message of "The request is rejected because the ERP instance in unactive state!" otherwise, enter into the next step;

If the local forced switch has existed on the node of this ring instance (on same time, only one of port0 and port1 can be in the status of local FS), there will be the message of "The FS request is rejected because an local FS request is present!" otherwise, enter into the next step;

If the forced switch is on the current highest priority, block the data channel and R-APS channel of this ERPS ring instance on the appointed member port (port0 or port1), and unblock the other member port of this ring node;

When the forced switch command is the highest priority command, send the P-APS (FS) packets with FS message on the two ring ports (port0 and port1) stably and steadily;

For the node which received the R-APS (FS) packets, if there is no higher priority request in local, unblock all the blocked ring ports;

The node which received the R-APS (FS) packets should run the flush FDB configuration according the corresponding demand.

Example:

Run the forced switch configuration on the port0 of ERPS ring1 instance1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#force-switch port0
```

6.2.21 manual-switch {port0 | port1}

Command: manual-switch {port0 | port1}

Function: Run the manual switch on the port of ERPS ring node. Only one manual switch is allowed existing in one ERPS ring instance, and the premise is that there is no SF fault or FS command in ERPS ring instance.

Parameters: {port0 | port1}: parameter selection, port0 means to run the manual switch configuration on port0 of the ring node; port1 means to run the manual switch configuration on port1 of the ring node.

Command Mode: ERPS Instance Configuration Mode.

Default: No manual switch in ERPS ring instance.

Usage Guide: If this ring supports version1, there will be the message of “Doesn't support the command on the ring running version 1!” otherwise, enter into the next step;

If this instance configuration is not integral, it is on the status of unactive, there will be the message of “The request is rejected because the ERP instance in unactive state!” otherwise, enter into the next step;

If the MS status has existed in ERPS ring node, there will be the message of “The MS request is rejected because an existing MS request is present!”

If the manual switch has existed on the node of this ring instance, there will be the message of “The MS request is rejected because an existing FS request is present!” otherwise, enter into the next step;

If there has been the fault in ERPS ring instance, there will be the message of “The MS request is rejected because an existing SF is present!” otherwise, enter into the next step;

If the manual switch is on the current highest priority, block the data channel and R-APS channel of this ERPS ring instance on the appointed member port (port0 or port1), and unblock the other member port of this ring node;

When the manual switch command is the highest priority command, send the P-APS (MS) packets with MS message on the two ring ports (port0 and port1) stably and steadily;

For the node which received the R-APS (MS) packets, if there is no higher priority request in local, unblock all the blocked ring ports;

The node which received the R-APS (MS) packets should run the flush FDB configuration according the corresponding demand.

Example:

Run the manual switch configuration on the port0 of ERPS ring1 instance1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#manual-switch port0
```

6.2.22 clear command

Command: clear command

Function: Run the clear command to the member port of ERPS ring node, it can clear the management command of the local activity: forced switch command and manual switch command; it can be also used to trigger the link switch under the revertive mode before WTR or WTB is time out; and trigger the link to switch from the standby link RPL back to the intrinsic link under the non-revertive mode after the fault recovery. For the last two situations, run this command on the rpl owner node universally.

Parameters: None.

Command Mode: ERPS Instance Configuration Mode.

Default: No clear command in ERPS ring instance.

Usage Guide: If this ring supports version1, there will be the message of “Doesn't support the command on the ring running version 1!” otherwise, enter into the next step;

If this instance configuration is not integral, it is on the status of unactive, there will be the message of “The request is rejected because the ERP instance in unactive state!” otherwise,

enter into the next step;

If the forced or manual switch command has existed on the node of this ring instance, clear the switch command and keep the block status of the data channel and R-APS channel of the blocked member ports. And send the P-APS (NR) packets on the two member ports stably and steadily until received R-APS (NR, RB) packets and known the RPL is blocked. Or the higher level request happens on the ring (such as SF);

If the local forced or manual switch has existed on the node of this ring instance, clear the command and then receive the R-APS (NR) packets whose node ID is larger than the local node ID. Unblock all the ring ports without SF fault and stop sending the R-APS (NR) packets on the two member ports.

If the ERPS ring instance that RPL owner node is in is the revertive mode and the WTR or WTB timer is enabled, delete the timer, block the RPL port and send the R-APS (NR, RB) packets on the two ring ports; and run flush FDB configuration, trigger the link switch in advance. Otherwise, enter into the next step;

If the ERPS ring instance that RPL owner node is in is the non-revertive mode, block the RPL port and send the R-APS (NR, RB) packets on the two ring ports; and run flush FDB configuration, trigger the link to switch from the standby link RPL back to the intrinsic link.

Example:

Run clear configuration on ERPS ring1 instance1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#clear command
```

6.2.23 show erps ring {<ring-name> | brief}

Command: show erps ring {<ring-name> | brief}

Function: Read the ERPS ring information.

Parameters: <*ring-name*>: ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines. The first and last characters cannot be underlines. If it is not appointed, show all the ERPS rings of this device.

brief: Show the ERPS ring main information.

Command Mode: Admin Mode.

Default: None.

Example: show all the ERPS rings information.

```
Switch#show erps ring brief
  Ring-Name          Ring-topo      Port0    Port1    Version  Inst-Count
  ----------------------------------------------------------------------------------------------------
  ring1              maijor-ring    1/0/1    1/0/2    V2       1
  ring2              open-ring      1/0/5    1/0/6     V2       1
```

Fields	Explanation
Ring-Name	ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines.

	The first and last characters cannot be underlines.
Ring-topo	ERPS ring topology mode: major-ring, open-bring
Port0	Port0 information of ERPS ring
Port1	Port1 information of ERPS ring
Version	Version that ERPS ring supports: V1, V2
Inst-Count	Instances number range of ERPS ring: 1 to 64

Show the ERPS ring1 information:

```
Switch#show erps ring ring1
R: RPL Owner
N: RPL Neighbour
C: Common Node
-------------------------------------------------------------------------------------------------
R-APS ring topology: open-ring
R-APS Virtual-Channel: with
Port0: Ethernet1/0/1                    Failure-detect type: physical-link-or-cc
Port1: Ethernet1/0/2                    Failure-detect type: physical-link
Instance  Contral  Protected  WTR_Timer  Guard_Timer  Holdoff_Timer  Port0 Port1
ID        Vlan     Instance   (min)      (csec)       (second)
-------------------------------------------------------------------------------------------------
1         10       3          6          100          0              R     C
2         20       4          5          500          0              C     C
```

Fields	Explanation
Instance ID	Id number of ERPS ring instance, range is from 1 to 64.
Contral Vlan	R-APS channel vlan, package R-APS packet of tag
Protected Instance	MSTP instance protected by ERPS ring instance
WTR_Timer	Wait to Restore timer, range is from 1 to 12min.
Guard_Timer	Guard timer, range is from 10ms to 2s
Holdoff_Timer	Holdoff timer, range is from 0 to 10s
Port0	Port0 information of ERPS ring
Port1	Port1 information of ERPS ring
R-APS ring topology	ERPS ring topology mode: major-ring, open-bring
R-APS Virtual-Channel	If it is ERPS sub ring, whether there is the R-APS virtual channel: with, without

6.2.24 show erps instance [ring <ring-name> [instance <instance-id>]]

Command: show erps instance [ring <ring-name> [instance <instance-id>]]

Function: Show the ERPS ring instance information.

Parameters: <*ring-name*>: ERPS ring name, the maximum characters number is 64 and it is made

up with letters, numbers and underlines. The first and last characters cannot be underlines. If it is not appointed, show all the ERPS ring instances of this device.

<instance-id>: ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show all the ERPS ring instances information.

Command Mode: Admin Mode.

Default: None.

Example:

Show all the ERPS ring instances information.

```
Switch#show erps instance
ERPS Ring ring1
  Instance 1
  Description: instance1
  Protected Instance: 1
  Revertive mode: non-revertive
  R-APS MEL: 7
  R-APS Virtual-Channel: with
  Control Vlan: 10
  Ring ID:
  Guard Timer (csec): 100
  Holdoff Timer (seconds): 0
  WTR Timer (min): 6
  ----------------------------------------------------------------
  Port          Role          Port-Status
  ----------------------------------------------------------------
  port0         RPL Owner     Blocked
  port1         Common        Forwarding
```

Fields	Explanation
Description	ERPS ring instance name
Protected Instance	MSTP instance protected by ERPS ring instance
Revertive mode	ERPS ring link mode: revertive, non-revertive
R-APS MEL	Level of R-APS channel, package R-APS packets
R-APS Virtual-Channel	If the ERPS ring is the sub ring, the R-APS virtual channel of the inherited ring: with, without
Ring ID	The ring-id number carried by the packets sent by ERPS ring instance, range is from 1 to 64.
Contral Vlan	R-APS channel vlan, package R-APS packet of tag
WTR_Timer	Wait to Restore timer, range is from 1 to 12min
Guard_Timer	Guard timer, range is from 10ms to 2s
Holdoff_Timer	Holdoff timer, range is from 0 to 10s
Port	ERPS ring port information: port0, port1
Role	ERPS ring node roles: RPL Owner, RPL neighbor, Common

Port Status	Blocked: port is in block status forwarding: port is in forwarding status

6.2.25 show erps status [ring <ring-name> [instance <instance-id>]]

Command: show erps status [ring <ring-name> [instance <instance-id>]]

Function: Show the status information of ERPS ring instance.

Parameters: <*ring-name*>: ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines. The first and last characters cannot be underlines. If it is not appointed, show all the ERPS rings of this device.

<instance-id>: ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show all the ERPS ring instances status information.

Command Mode: Admin Mode.

Default: None.

Example:

Show all the ERPS ring instances status information.

```
Switch#show erps status
ERPS ring ring1 instance 1 status：
Active：1
Node State：Idle
Time last topology change : Jan 01 00:17:25 2012
-------------------------------------------------------------------------------------------------
Port      Interface     Port-Status       Signal-Status     R-RAPS-NodeId       BPR
-------------------------------------------------------------------------------------------------
Port0     1/0/1           blocked           Non-failed      00-00-00-00-00-00     0
Port1     1/0/2           forwarding        Non-failed        00-00-00-00-00-00     0
```

Active	Current active status of ERPS ring instance: 1, 0
Node State	Current status of ERPS ring instance: Idle, Protection, Forced-switch, Manual-switch, Pending
Port Status	Blocked: the port is in block status Forwarding: the port is in forwarding status
Signal Status	ERPS ring port fault status: Non-failed: no fault Failed: fault happened
Remote R-APS NodeId	NodeId information carried by the receiving last R-APS saved by ERPS ring port, it is mac information.
BPR	The block link information carried by the receiving last R-APS saved by ERPS ring port, it is port0 or port1 which was blocked.
Time last topology change	Topology switching last time

6.2.26 show erps statistics [ring <ring-name> [instance <instance-id>]]

Command: show erps statistics [ring <ring-name> [instance <instance-id>]]

Function: Show the statistic information of ERPS ring instance.

Parameters: <ring-name>: ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines. The first and last characters cannot be underlines. If it is not appointed, show the statistic information of all the ERPS rings of this device.

<instance-id>: ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show the statistic information of all the ERPS ring instances of this device.

Command Mode: Admin Mode.

Default: None.

Example:

Show the statistic information of ERPS ring instance.

```
Switch#show erps statistics ring 1 instance 1
Statistics for ERPS ring ring1 instance 1：
R-APS          Port0(Tx/Rx)          Port1(Tx/Rx)
--------------------------------------------------------------------------
NR                  3/0                  3/0
NR,RB               0/0                  0/0
SF              19129/0              19129/0
MS                  0/0                  0/0
FS                  0/0                  0/0
EVENT               0/0                  0/0
--------------------------------------------------------------------------
TOTOL          19132/0              19132/0
```

6.2.27 clear erps statistics [ring <ring-name> [instance <instance-id>]]

Command: clear erps statistics [ring <ring-name> [instance <instance-id>]]

Function: Clear the statistic information of ERPS.

Parameters: <ring-name>: ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines. The first and last characters cannot be underlines. If it is not appointed, clear the statistic information of all the ERPS rings of this device.

<instance-id>: ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, clear the statistic information of all the ERPS ring instances of this device.

Command Mode: Admin Mode.

Default: None.

Example: Clear the statistic information of ERPS ring1 instance1.

```
Switch#clear erps statistics ring 1 instance 1
```

6.2.28 debug erps

Command: debug erps packet [detail] {send | receive] {[ring <ring-name> [instance <instance-id>]] | [port]}

debug erps fsm [ring <ring-name> [instance <instance-id>]]

debug erps timer [ring <ring-name> [instance <instance-id>]]

no debug eprs

Function: Enable the debug information of ERPS. The no command disables this information.

Parameters: packet: Enable the packets debug information.

detail: Enable the detail debug information of packets.

send: Enable the sending packets debug information.

received: Enable the receiving packets debug information.

fsm: Enable the status device debug information.

timer: Enable the timer debug information.

<ring-name>: ERPS ring name, the maximum characters number is 64 and it is made up with letters, numbers and underlines. The first and last characters cannot be underlines.

<instance-id>: ID of ERPS ring instance, range is from 1 to 48.

Command Mode: Admin Mode.

Default: Do not show.

6.2.29 debug erps error

Command: debug erps error

no debug erps error

Function: Show the default information of ERPS. The no command disables this information.

Parameters: None.

Command Mode: Admin Mode.

Default: Do not show.

6.2.30 debug erps event

Command: debug erps event

no debug erps event

Function: Show the event information of ERPS. The no command disables this information.

Parameters: None.

Command Mode: Admin Mode.

Default: Do not show.

6.2.31 no debug all

Command: no debug all

Function: Disable all the debug information of this device.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: When using no debug all command to disable all the debug information of the switch, this command is effective to the debug information of ERPS, the debug information of ERPS will be disabled too.

6.2.32 show debugging

Command: show debugging

Function: Enable all the debug information of this module.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: When using **show debugging erps** command to show the debug information, this module supports this command.

6.3 MRPP

6.3.1 control-vlan

Command: control-vlan <*vid*>

no control-vlan

Function: Configure control VLAN ID of MRPP ring; the "**no control-vlan**" command deletes control VLAN ID.

Parameter: ***<vid>*** expresses control VLAN ID, the valid range is from 1 to 4094.

Command Mode: MRPP ring mode

Default: None

Usage Guide: The command specifies Virtual VLAN ID of MRPP ring, currently it can be any value in 1-4094. To avoid confusion, it is recommended that the ID is non-configured VLAN ID, and the same to MRPP ring ID. In configuration of MRPP ring of the same MRPP loop switches, the control VLAN ID must be the same, otherwise the whole MRPP loop may not be able to 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

6.3.2 clear mrpp statistics

Command: clear mrpp statistics [<*ring-id*>]

Function: Clear statistic information of MRPP data packet of MRPP ring receiving and transferring.

Parameter: ***<ring-id>*** is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it clears all of MRPP ring statistic information.

Command Mode: Admin Mode.

Default: None.

Usage Guide: None.

Example: Clear statistic information of MRPP ring 4000 of switch.

Switch#clear mrpp statistics 4000

6.3.3 debug mrpp

Command: debug mrpp

no debug mrpp

Function: Open MRPP debug information; "**no description**" command disables MRPP debug information.

Command Mode: Admin Mode

Parameter: None.

Usage Guide: Enable MRPP debug information, and check message process of MRPP protocol and receive data packet process, it is helpful to monitor debug.

Example: Enable debug information of MRPP protocol.

Switch#debug mrpp

6.3.4 enable

Command: enable

no enable

Function: Enable configured MRPP ring, the "**no enable**" command disables this enabled MRPP ring.

Parameter:

Command Mode: MRPP ring mode

Default: Default disable MRPP ring.

Usage Guide: Executing this command, it must enable MRPP protocol, and if other commands have configured, the MRPP ring is enabled.

Example: Configure MRPP ring 4000 of switch to primary node, and enable the MRPP ring.

Switch(config)#mrpp enable

Switch(config)#mrpp ring 4000

Switch(mrpp-ring-4000)#control-vlan 4000

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

Switch(mrpp-ring-4000)#fail-timer 18

Switch(mrpp-ring-4000)#hello-timer 6

Switch(mrpp-ring-4000)#enable

Switch(mrpp-ring-4000)#exit
Switch(config)#in ethernet1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config)#in ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port

6.3.5 errp domain

Command: errp domain <*domain-id*>
no errp domain <*domain-id*>
Function: Create ERRP domain, the no command deletes the configured ERRP domain.
Parameter: <*domain-id*> domain ID of ERRP, the range between 1 and 15.
Command Mode: Global mode
Usage Guide: If domain ID of ERRP needs to be configured, the compatible mode of ERRP should be enabled firstly. When executing this command, it should create a new ERRP domain if there is no ERRP domain. However, the no command is used to delete the corresponding domain ID of ERRP.
Example: Configure domain ID for ERRP globally.
Switch(Config)#errp domain 1

6.3.6 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

6.3.7 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

6.3.8 mrpp eaps compatible

Command: mrpp eaps compatible

no mrpp eaps compatible

Function: Enable the compatible mode for EAPS, the no command disables the compatible mode.

Parameter: None.

Command Mode: Global mode

Default: Disable the compatible function of EAPS.

Usage Guide: If the compatible function of EAPS needs to be configured, MRPP protocol should be enabled firstly. When executing **no mrpp eaps compatible** command, it should ensure that the switch has enabled MRPP protocol.

Example: Enable the compatible function of EAPS globally.

Switch(Config)#mrpp enable

Switch(Config)#mrpp eaps compatible

6.3.9 mrpp enable

Command: mrpp enable

no mrpp enable

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

Parameter: None.

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

6.3.10 mrpp errp compatible

Command: mrpp errp compatible

no mrpp errp compatible

Function: Enable the compatible mode for ERRP, the no command disables the compatible mode.

Parameter: None.

Command Mode: Global mode

Default: Disable the compatible function of ERRP.

Usage Guide: If the compatible function of ERRP needs to be configured, MRPP protocol should be enabled firstly. Furthermore, the port with ERRP compatible mode should be configured as hybrid or trunk mode and allow the packets with Control Vlan information.

Example: Enable the compatible function of ERRP globally.

Switch(Config)#mrpp enable

Switch(Config)#mrpp errp compatible

Switch(Config)#mrpp ring 2

Switch(mrpp-ring-2)#control-vlan 4000

Switch(config-if-ethernet1/51)#switchport mode hybrid

Switch(config-if-ethernet1/51)#switchport hybrid allowed vlan 4000 tag

Switch(config-if-ethernet1/52)#switchport mode hybrid

Switch(config-if-ethernet1/52)#switchport hybrid allowed vlan 4000 tag

6.3.11 mrpp poll-time

Command: mrpp poll-time <20-2000>

Function: Configure the query interval of MRPP.

Command mode: Global mode.

Usage Guide: Configure the query time to adjust the query interval of MRPP, the default interval is 100ms.

Example: Set the query time as 200ms.

Switch(Config)# mrpp poll-time 200

6.3.12 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

6.3.13 mrpp ring primary-port

Command: mrpp ring <*ring-id*> primary-port {cos <cos>|}

no mrpp ring <*ring-id*> primary-port

Function: Specify MRPP ring primary-port and the cos which is brought in the packet head tag of port sending packet.

Parameter: <*ring-id*> is the ID of MRPP ring; range is <1-4096>.

<cos> is the cos value in the packet head; range is <0-7>.

Command Mode: Port mode

Default: There is no configuration and the cos value is 0 as default.

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 1/0/1.

Switch(Config)#interface ethernet 1/0/1

Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port

6.3.14 mrpp ring secondary-port

Command: mrpp ring < *ring-id* > secondary-port {cos <cos>|}

no mrpp ring < *ring-id* > secondary-port

Function: Specify secondary of MRPP ring and the cos which is brought in the packet head tag of port sending packet.

Parameter: <*ring-id*> is the ID of MRPP ring; range is <1-4096>.

<cos> is the cos value in the packet head; range is <0-7>.

Command Mode: Port mode

Default: There is no configuration and the cos value is 0 as default.

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 1/0/3.

Switch(config)#interface ethernet1/0/3
Switch(Config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port

6.3.15 node-mode

Command: node-mode {maser | transit}
Function: Configure the type of the node to primary node or secondary node.
Parameter: None.
Command Mode: MRPP ring mode.
Default: Default the node mode is secondary node.
Usage Guide: None.
Example: Configure the switch to primary node. MRPP ring 4000.
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#node-mode master

6.3.16 show mrpp

Command: show mrpp [<*ring-id*>]
Function: Display MRPP ring configuration.
Parameter: ***<ring-id>*** is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it display all of MRPP ring configuration.
Command Mode: Admin and Configuration Mode.
Default: None
Usage Guide: None
Example: Display configuration of MRPP ring 4000 of switch
Switch# show mrpp 4000

6.3.17 show mrpp statistics

Command: show mrpp statistics [<*ring-id*>]
Function: Display statistic information of data packet of MRPP ring receiving and transferring.
Parameter: ***<ring-id>*** is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it displays all of MRPP ring statistic information.
Command Mode: Admin and Configuration Mode.
Default: None
Usage Guide: None
Example: Display statistic information of MRPP ring 4000 of switch.
Switch# show mrpp statistic 4000

6.4 ULPP

6.4.1 clear ulpp flush counter interface

Command: clear ulpp flush counter interface *<name>*

Function: Clear the statistic information of the flush packets.

Parameter: *<name>* is the name of the port.

Default: None.

Command mode: Admin mode.

Usage Guide: None.

Example: Clear the statistic information of the flush packets for the port1/0/1.

Switch#clear ulpp flush counter interface e1/0/1

ULPP flush counter has been reset.

6.4.2 control vlan

Command: control vlan *<integer>*

no control vlan

Function: Configure the control VLAN of ULPP group; the no command restores the default value.

Parameter: *<integer>* is the control VLAN ID that sends the flush packets, range from 1 to 4094.

Default: The default is VLAN 1.

Command mode: ULPP group configuration mode.

Usage Guide: Configure the control VLAN of ULPP group. This VLAN must correspond the existent VLAN, after it is configured, this VLAN can't be deleted. It must belong to the VLAN protected by ULPP group to avoid flush packets loopback.

Example: Configure the sending control VLAN of ULPP group as 10.

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# control vlan 10

6.4.3 debug ulpp error

Command: debug ulpp error

no debug ulpp error

Function: Show the error information of ULPP. The no operation disables showing the error information of ULPP.

Parameter: None.

Default: Do not display.

Command mode: Admin mode.

Usage Guide: None.

Example: Show the error information of ULPP.

Switch# debug ulpp error

Unrecognized Flush packet received.

6.4.4 debug ulpp event

Command: debug ulpp event

no debug ulpp event

Function: Show the event information of ULPP. The no operation disables showing the event information of ULPP.

Parameter: None.

Default: Do not display.

Command mode: Admin mode.

Usage Guide: None.

Example: Show the event information of ULPP.

Switch# debug ulpp event

ULPP group 1 state changes:

Master port ethernet 1/0/1 in ULPP group 1 changed state to Forwading.

Slave port ethernet 1/0/2 in ULPP group 1 changed state to Standby.

6.4.5 debug ulpp flush content interface

Command: debug ulpp flush content interface *<name>*

no debug ulpp flush content interface *<name>*

Function: Show the contents of the receiving flush packets. The no operation disables the shown contents.

Parameter: *<name>* is the name of the port.

Default: Do not display.

Command mode: Admin mode.

Usage Guide: None.

Example: Show the contents of the receiving flush packets for the port1/0/1.

Switch# debug ulpp flush content interface e1/0/1

Flush packet content:

Destination MAC: 01-03-0f-cc-cc-cc

Source MAC: 00-a0-cc-d7-5c-ea

Type: 8100

Vlan ID: 1

Length: 518

Control Type: 2

Control Vlan: 10

MAC number:0

Vlan Bitmap:

6.4.6 debug ulpp flush {send | receive} interface

Command: debug ulpp flush {send | receive} interface *<name>*

no debug ulpp flush {send | receive} interface *<name>*

Function: Show the information of the receiving/sending flush packets, it only shows the receiving packets, but do not show the detailed contents of the packets. The no operation disables the shown information.

Parameter: <*name*> is the name of the port.

Default: Do not display.

Command mode: Admin mode.

Usage Guide: None.

Example: Show the information that send the flush packets for the port1/0/1.

Switch# debug ulpp flush send interface e1/0/1

Flush packet send on port Ethernet 1/0/1.

6.4.7 description

Command: description *<string>*

no description

Function: Configure the description character string of ULPP group. The no command deletes the description.

Parameter: *<string>* is the name of ULPP group, the max number of the characters is 128.

Default: Do not configure ULPP name by default.

Command mode: ULPP group configuration mode.

Usage Guide: None.

Example: Configure the description of ULPP group as snr.

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# description snr

6.4.8 flush disable arp

Command: flush disable arp

Function: Disable sending the flush packets of deleting ARP.

Parameter: None.

Default: By default, enable the sending function of the flush packets which are deleted by ARP.

Command mode: ULPP group configuration mode.

Usage Guide: If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to delete the entries of ARP.

Example: Disable sending the flush packets of deleting ARP.

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# flush disable arp

6.4.9 flush disable mac

Command: flush disable mac

Function: Disable sending the flush packets of updating MAC address.

Parameter: None.

Default: By default, enable sending the flush packets of updating MAC address.

Command mode: ULPP group configuration mode.

Usage Guide: If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to update the MAC address table.

Example: Disable sending the flush packets of updating MAC address.

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# flush disable mac

6.4.10 flush disable mac-vlan

Command: flush disable mac-vlan

Function: Disable sending the flush packets of deleting the dynamic unicast mac according to vlan.

Parameter: None.

Default: Disable.

Command mode:ULPP group configuration mode.

Usage Guide: If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to delete the dynamic unicast mac according to vlan.

Example: Disable sending the flush packets deleted by mac-vlan.

Switch(config)#ulpp group 1

Switch(ulpp-group-1)#flush disable mac-vlan

6.4.11 flush enable arp

Command: flush enable arp

Function: Enable sending the flush packets of deleting ARP.

Parameter: None.

Default: By default, enable sending the flush packets of deleting ARP.

Command mode: ULPP group configuration mode.

Usage Guide: If enable this function, when the link is switched, it will actively send the flush packets to notify the upstream device, so as to delete the list entries of ARP.

Example: Enable sending the flush packets of deleting ARP.

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# flush enable arp

6.4.12 flush enable mac

Command: flush enable mac

Function: Enable sending the flush packets of updating MAC address.

Parameter: None.

Default: By default, enable sending the flush packets of updating MAC address.

Command mode: ULPP group configuration mode.

Usage Guide: If enable this function, when the link is switched, it will actively send the flush

packets to notify the upstream device, so as to update the MAC address table.

Example: Enable sending the flush packets of updating MAC address.

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# flush enable mac

6.4.13 flush enable mac-vlan

Command: flush enable mac-vlan

Function: Enable sending the flush packets of deleting the dynamic unicast mac according to vlan.

Parameter: None.

Default: Disable.

Command mode:ULPP group configuration mode.

Usage Guide: If configure this command, when the link is switched, it will actively send the flush packets to notify the upstream device to delete the dynamic unicast mac according to vlan.

Example: Enable sending the flush packets deleted by mac-vlan.

Switch(config)#ulpp group 1

Switch(ulpp-group-1)#flush enable mac-vlan

6.4.14 preemption delay

Command: preemption delay *<integer>*

no preemption delay

Function: Configure the preemption delay, the no command configures the preemption delay as the default value.

Parameter: *<integer>*: the preemption delay, range from 1 to 600, in second.

Default: The default preemption delay is 30.

Command mode: ULPP group configuration mode.

Usage Guide: The preemption delay is the delay time before the master port is preempted as the forwarding state, for avoiding the link oscillation in a short time. After the preemption mode is enabled, the preemption delay takes effect.

Example: Configure the preemption delay as 50s for ULPP group.

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# preemption delay 50

6.4.15 preemption mode

Command: preemption mode

no preemption mode

Function: Enable/disable the preemption mode of ULPP group.

Parameter: None.

Default: Do not preempt.

Command mode: ULPP group configuration mode.

Usage Guide: If the preemption mode configured by ULPP group, and the slave port is in forwarding state, and the master port is in the standby state, the master port will turn into the forwarding state and the slave port turn into the standby state after the preemption delay.

Example: Configure the preemption mode of ULPP group.

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# preemption mode

6.4.16 protect vlan-reference-instance

Command: protect vlan-reference-instance *<instance-list>*

no protect vlan-reference-instance *<instance-list>*

Function: Configure the protective VLANs of ULPP group, the no command cancels the protective VLANs.

Parameter: *<instance-list>* is MSTP instance list, such as: i; j-k. The number of the instances is not limited in the list.

Default: Do not protect any VLANs by default that means any instances are not quoted.

Command mode: ULPP group configuration mode.

Usage Guide: Quote the instances of MSTP to protect the VLANs. The VLAN corresponds to this instance is at the forwarding state on one port of this group, and at the blocked state on another port of this group. Each ULPP group can quotes all instances of MSTP. And it can quotes the inexistent MSTP instances that means any VLANs are not protected, the different ULPP groups can't quote the same instance.

Example: Configure the protective VLAN quoted from instance 1 for ULPP group.

Switch(config)# ulpp group 20

Switch(ulpp-group-20)# protect vlan-reference-instance 1

6.4.17 show ulpp flush counter interface

Command: show ulpp flush counter interface {ethernet <IFNAME> | <IFNAME>}

Function: Show the statistic information of the flush packets.

Parameter: <IFNAME> is the name of the ports.

Default: None.

Command mode: Admin mode.

Usage Guide: Show the statistic information of the flush packets, such as: the information of the flush packets number which has been received, the time information that receive the flush packets finally.

Example: Show the statistic information of the flush packets for ULPP group1.

Switch# show ulpp flush counter interface e1/0/1

Received flush packets: 10

6.4.18 show ulpp flush-receive-port

Command: show ulpp flush-receive-port

Function: Show the port which receive flush packet, flush type and control VLAN.

Parameter: None.

Default: None.

Command mode: Admin mode.

Usage Guide: None.

Example: Show the information that the port receives flush packets.

```
Switch# show ulpp flush-receive-port
ULPP flush-receive portlist:
Portname              Type    Control Vlan
-------------------------------------------------
Ethernet1/0/1         ARP     1
Ethernet1/0/3         MAC     1;3;5-10
```

6.4.19 show ulpp group

Command: show ulpp group [group-id]

Function: Show the configuration information of the ULPP groups which have been configured.

Parameter: [group-id]: Show the information of the specific ULPP group.

Default: By default, show the information of all ULPP groups which have been configured.

Command mode: Admin mode.

Usage Guide: Show the configuration information of ULPP groups which have been configured, such as: the state of the master port and the slave port, the preemption mode, the preemption delay, etc.

Example: Show the configuration information of ULPP group1.

```
Switch# show ulpp group 1
ULPP group 1 information:
Description: abc
Preemption mode: on
Preemption delay: 30s
Control VLAN:1
Protected VLAN: Reference Instance 1
Member                Role            State
--------------------------------------------------------------
Ethernet1/0/1         MASTER          FORWARDING
Ethernet1/0/2         SLAVE           STANDBY
```

6.4.20 ulpp control vlan

Command: ulpp control vlan *<vlan-list>*

no ulpp control vlan *<vlan-list>*

Function: Configure the receiving control VLANs of the port, the no command restores the default value.

Parameter: ***<vlan-list>*** specify the control VLAN list that receives the flush packets, such as: i; j-k. The number of VLANs in Each character string can not exceed 100. The receiving control VLAN of the port can be added.

Default: The default is VLAN 1.

Command mode: Port mode.

Usage Guide: Configure the receiving control VLAN for the port. This VLAN must correspond the existent VLAN, after it is configured, this VLAN can't be deleted.

Example: Configure the receiving control VLAN as 10.

Switch(config)# interface ethernet 1/0/1

Switch(config-If-Ethernet1/0/1)# ulpp control vlan 10

6.4.21 ulpp flush disable arp

Command: ulpp flush disable arp

Function: Disable receiving the flush packets of deleting ARP.

Parameter: None.

Default: By default, disable receiving the flush packets of deleting ARP.

Command mode: Port mode.

Usage Guide: If this command is configured, then it will not receive the flush packets of deleting ARP.

Example: Disable receiving the flush packets of deleting ARP.

Switch(config)# interface ethernet 1/0/1

Switch(config-If-Ethernet1/0/1)# ulpp flush disable arp

6.4.22 ulpp flush disable mac

Command: ulpp flush disable mac

Function: Disable receiving the flush packets of updating MAC address.

Parameter: None.

Default: By default, disable receiving the flush packets of updating MAC address.

Command mode: Port mode.

Usage Guide: If this command is configured, then it will not receive the flush packets of updating MAC address.

Example: Disable receiving the flush packets of updating MAC address.

Switch(config)# interface ethernet 1/0/1

Switch(config-If-Ethernet1/0/1)# ulpp flush disable mac

6.4.23 ulpp flush disable mac-vlan

Command: ulpp flush disable mac-vlan

Function: Disable receiving the flush packets of mac-vlan type.

Parameter: None.

Default: Disable.

Command mode: Port mode.

Usage Guide: If enabling this function, forward the hardware of the flush packets with mac-vlan type received in port. It will not be analyzed.

Example: Disable receiving the flush packets deleted by mac-vlan of port.

Switch(config)#interface e1/0/2

Switch(config-if-ethernet1/0/2)#ulpp flush disable mac-vlan

6.4.24 ulpp flush enable arp

Command: ulpp flush enable arp

Function: Enable receiving the flush packets of deleting ARP.

Parameter: None.

Default: By default, disable receiving the flush packets of deleting ARP.

Command mode: Port mode.

Usage Guide: Enable this function to receive the flush packets which delete ARP.

Example: Enable receiving of the flush packets of deleting ARP.

Switch(config)# interface ethernet 1/0/1

Switch(config-If-Ethernet1/0/1)# ulpp flush enable arp

6.4.25 ulpp flush enable mac

Command: ulpp flush enable mac

Function: Enable receiving the flush packets of updating MAC address.

Parameter: None.

Default: By default, disable receiving the flush packets of updating MAC address.

Command mode: Port mode.

Usage Guide: Enable receiving the flush packets of updating MAC address table.

Example: Enable receiving the flush packets of updating the MAC address.

Switch(config)# interface ethernet 1/0/1

Switch(config-If-Ethernet1/0/1)# ulpp flush enable mac

6.4.26 ulpp flush enable mac-vlan

Command: ulpp flush enable mac-vlan

Function: Enable receiving the flush packets of mac-vlan type.

Parameter: None.

Default: Disable.

Command mode: Port mode.

Usage Guide: If enabling this function, configure the interface to receive the flush packets handled mac-vlan type and delete the dynamic unicast mac according to vlan information in the packets.

Example: Enable receiving the flush packets deleted by mac-vlan of port.

Switch(config)#interface e1/0/2

Switch(config-if-ethernet1/0/2)#ulpp flush enable mac-vlan

6.4.27 ulpp group

Command: ulpp group *<integer>*

no ulpp group *<integer>*

Function: Create a ULPP group. If this group exists, then enter the configuration mode of ULPP group. The no command deletes a ULPP group.

Parameter: *<integer>* is the ID of ULPP group, range from 1 to 48.

Command mode: Global Mode.

Default: Any ULPP groups are not configured.

Usage Guide: None.

Example: Configure ulpp group 20 or enter the mode of ulpp group 20.

Switch(config)# ulpp group 20

Switch(ulpp-group-20)#

6.4.28 ulpp group master

Command: ulpp group *<integer>* master

no ulpp group *<integer>* master

Function: Configure the master port of ULPP group, the no command deletes the master port.

Parameter: *<integer>* is the ID of ULPP group, range from 1 to 48.

Default: There is no master port configured by default.

Command mode: Port mode.

Usage Guide: There is no sequence requirement for the master and slave port configuration in a group, but the protective VLANs must be configured before the member ports. Each group has only one master port, if the master port exists, then the configuration fail.

Example: Configure the master port of ULPP group.

Switch(config)# interface ethernet 1/0/1

Switch(config-If-Ethernet1/0/1)# ulpp group 20 master

6.4.29 ulpp group slave

Command: ulpp group *<integer>* slave

no ulpp group *<integer>* slave

Function: Configure the slave port of ULPP group, the no command deletes the slave port.

Parameter: *<integer>* is the ID of ULPP group, the range from 1 to 48.

Default: There is no slave port configured by default.

Command mode: Port mode.

Usage Guide: There is no sequence requirement for the master and slave port configuration in a group, but the protective VLANs must be configured before the member ports. Each group has only one slave port, if the slave port exists, then the configuration is fail.

Example: Configure the slave port of ULPP group.

Switch(config)# interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp group 20 slave

6.5 ULSM

6.5.1 debug ulsm event

Command: debug ulsm event
no debug ulsm event
Function: Show the event information of ULSM. The no operation disables showing ULSM events.
Parameter: None.
Default: None.
Command mode: Admin Mode.
Usage Guide: None.
Example: Show the event information of ULSM.
Switch# debug ulsm event
Downlink synchoronized with ULSM group, change state to Down.

6.5.2 show ulsm group

Command: show ulsm group [group-id]
Function: Show the configuration information of ULSM group.
Parameter: [group-id]: the ID of ULSM group.
Default: By default, show the information of all ULSM groups which have been configured.
Command mode: Admin Mode.
Usage Guide: None.
Example: Show the configuration information of ULSM group1.
Switch# show ulsm group 1
ULSM group 1 information:
ULSM group state: Down

Member	Role	State	Down by ULSM
ethernet1/0/1	UpLINK	Down	
ethernet1/0/2	DownLINK	Down	Yes

6.5.3 ulsm group

Command: ulsm group *<group-id>*
no ulsm group *<group-id>*

Function: Create a ULSM group. The no command deletes the ULSM group.

Parameter: <*group-id*> is the ID of ULSM group, range from 1 to 32.

Default: There is no ULSM group configured by default.

Command mode: Global Mode.

Usage Guide: None.

Example: Create ULSM group 10.

Switch(config)# ulsm group 10

6.5.4 ulsm group {uplink | downlink}

Command: ulsm group <*group-id*> {uplink | downlink}

no ulsm group <*group-id*>

Function: Configure the uplink/downlink ports of ULSM group. The no command deletes the uplink/downlink ports.

Parameter: <*group-id*>: The ID of ULSM group, the range from 1 to 32.

uplink: Configure the port as the uplink port.

downlink: Configure the port as the downlink port.

Default: The port does not belong to any ULSM group.

Command mode: Port Mode.

Usage Guide: Configure the uplink/downlink ports of ULSM group. Each ULSM group can configure 8 uplink ports and 16 downlink ports at most.

Example: Configure port1/0/3 as the uplink port of ULSM group10.

Switch(config)# interface ethernet 1/0/3

Switch(config-If-Ethernet1/0/3)# ulsm group 10 uplink

Chapter 7 Commands for Debugging and Diagnosis

7.1 Monitor and Debug

7.1.1 clear history all-users

Command: clear history all-users
Function: Clear the command history of all users saved by the switch.
Command Mode: Admin mode
Usage Guide: Using this command can clear the command history of all users.
Example:
Switch#clear history all-users

7.1.2 history all-users max-length

Command: history all-users max-length <count>
Function: Set the max command history of all users saved by the switch.
Parameter: <count>: the command history number can be saved, ranging from 100 to 1000
Command Mode: Global mode
Usage Guide: The system can save 100 recent command history of all users at best by default, using this command can set the max command history number.
Example:
Switch(config)#history all-users max-length 500

7.1.3 ping

Command: ping [[src *<source-address>*] { *<destination-address>* | host *<hostname>* }]
Function: Issue ICMP request to remote devices, check whether the remote device can be reached by the switch.
Parameters: ***<source-address>*** is the source IP address where the ping command is issued, with IP address in dotted decimal format. ***<destination-address>*** is the target IP address of the ping command, with IP address in dotted decimal format. ***<hostname>*** is the target host name of the ping command, which should not exceed 64 characters.
Default: 5 ICMP echo requests will be sent. The default packet size and time out is 56 bytes and 2 seconds.
Command Mode: Admin mode
Usage Guide: When the ping command is entered without any parameters, interactive configuration mode will be invoked. And ping parameters can be entered interactively.

Example:

Example 1: To ping with default parameters.

Switch#ping 10.1.128.160

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds.

...!!

Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms

In the example above, the switch is made to ping the device at 10.1.128.160. The command did not receive ICMP reply packets for the first three ICMP echo requests within default 2 seconds timeout. The ping failed for the first three tries. However, the last two ping succeeded. So the success rate is 40%. It is denoted on the switch "." for ping failure which means unreachable link, while "!" for ping success, which means reachable link.

Example 2: Use ping command with source address configuration, and leave other fields to default.

Switch#ping src 10.1.128.161 10.1.128.160

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 10.1.128.160, using source address 10.1.128.161, timeout is 2 seconds.

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

In the example above, 10.1.128.161 is configured as the source address of the ICMP echo requests, while the destination device is configured to be at 10.1.128.160. The command receives all the ICMP reply packets for all of the five ICMP echo requests. The success rate is 100%. It is denoted on the switch "." for ping failure which means unreachable link, while "!" for ping success, which means reachable link.

Example 3: Ping with parameters entered interactively.

Switch#ping

VRF name：

Target IP address：10.1.128.160

Use source address option[n]: y

Source IP address: 10.1.128.161

Repeat count [5]: 100

Datagram size in byte [56]：1000

Timeout in milli-seconds [2000]: 500

Extended commands [n]: n

Display Information	Explanation
VRF name	VRM name. If MPLS is not enabled, this field will be left empty.
Target IP address：	The IP address of the target device.
Use source address option[n]	Whether or not to use ping with source address.
Source IP address	To specify the source IP address for ping.

Repeat count [5]	Number of ping requests to be sent. The default value is 5.
Datagram size in byte [56]	The size of the ICMP echo requests, with default as 56 bytes.
Timeout in milli-seconds [2000]:	Timeout in milli-seconds, with default as 2 seconds.
Extended commands [n]:	Whether or to use other extended options.

7.1.4 ping6

Command: ping6 [<dst-ipv6-address> | host *<hostname>* / src *<src-ipv6-address>* {*<dst-ipv6-address* > / host *<hostname>*}]

Function: To check whether the destination network can be reached.

Parameters: ***<dst-ipv6-address>*** is the target IPv6 address of the ping command. ***<src-ipv6-address>*** is the source IPv6 address where the ping command is issued. ***<hostname>*** is the target host name of the ping command, which should not exceed 64 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.

7.1.5 show boot-files

Command: show boot-files
Function: Display the first and second IMG files and the CFG file enabled by switch.
Command Mode: Admin and Configuration Mode.
Usage Guide: After implementing this command, the booting sequence of IMG files in the corresponding storage device, which IMG file is currently used in booting, the configuration information of the CFG file in the storage device and the CFG file currently booted.
Example: Display the first and second IMG files and the CFG file enabled by switch.
Switch#show boot-files
Booted files on switch
The primary img file at the next boot time: flash:/nos.img
The backup img file at the next boot time: flash:/nos.img
Current booted img file: flash:/nos.img

The startup-config file at the next boot time: flash:/startup.cfg
Current booted startup-config file: flash:/startup.cfg

If the CFG file of the next booting is set as NULL, the CFG part mentioned above will be displayed as follows:
The startup-config file at the next boot time: NULL
Current booted startup-config file: flash:/startup.cfg

7.1.6 show debugging

Command: show debugging {l4 | lldp|pppoe | other | spanning-tree|erps|fulleaps}
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 l4 debug switch state.
Switch#show debugging l4
L4 debugging status ON mod:
Relative command: debug

7.1.7 show fan

This command is not supported by the switch.

7.1.8 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 ----

7.1.9 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 1/0/3
enable
dir
show ftp
```

7.1.10 show history all-users

Command: show history all-users [detail]
Function: Show the recent command history of all users.
Parameter: [detail] shows user name of the executing command. IP address of the user will be shown when logging in the executing command through Telnet or SSH.
Command Mode: Admin and configuration mode
Usage Guide: This command is used to show the recent command history of all users, including time, logging type, executing command, etc.
Notice: The user can only check the command history of other users whose purview should not be higher than oneself.
Example:

```
Switch(config)#show history all-users detail
Time              Type          User        Command
0w 0d 0h 2m    Telnet/SSH   admin      show history all-users detail 192.168.1.2:1419
0w 0d 0h 1m    Telnet/SSH   admin      show history all-users 192.168.1.2:1419
0w 0d 0h 1m    Console      Null        show history all-users
0w 0d 0h 1m    Console      Null        end
0w 0d 0h 1m    Console      Null        ip address 192.168.1.1 255.255.255.0
0w 0d 0h 0m    Console      Null        in v 1
0w 0d 0h 0m    Console      Null        telnet-server enable
```

7.1.11 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   *................*
```

7.1.12 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

7.1.13 show running-config current-mode

Command: show running-config current-mode

Function: Show the configuration under the current mode.

Command mode: All configuration modes.

Default: None.

Usage Guide: Enter into any configuration mode and input this command under this mode, it can show all the configurations under the current mode.

Example:

```
 Switch(config-if-ethernet1/0/1)#show run c
!
Interface Ethernet1/0/1
```

Diagnosis switchport access vlan 2
!

7.1.14 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.

7.1.15 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 1/0/1.
Switch#show switchport interface ethernet 1/0/1
Ethernet1/0/1
Type :Universal
Mac addr num : No limit
Mode :Trunk
Port VID :1
Trunk allowed Vlan :ALL

Displayed Information	Description
Ethernet1/0/1	Corresponding interface number of the Ethernet.
Type	Current interface type.
Mac addr num	Numbers of interfaces with MAC address learning ability.
Mode: Trunk	Current interface VLAN mode.
Port VID :1	Current VLAN number the interface belongs.
Trunk allowed Vlan :ALL	VLAN permitted by Trunk.

7.1.16 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.

7.1.17 show tcp ipv6

Command: show tcp ipv6

Function: Show the current TCP connection.

Command mode: Admin and configuration mode.

Example:

Switch#show tcp ipv6

LocalAddress	LocalPort	RemoteAddress	RemotePort	State	IF	VRF
::	*80*	::	0	LISTEN	0	0
::	23	::	0	LISTEN	0	0

Displayed Information	Explanation
LocalAddress	Local IPv6 address of TCP connection
LocalPort	Local port of TCP connection
RemoteAddress	Remote IPv6 address of TCP connection
RemotePort	Remote Port of TCP connection
State	The current state of TCP connection
IF	Local port index of TCP connection
VRF	Virtual route forward instance

7.1.18 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

7.1.19 show temperature

Command: show temperature

Function: Show the temperature of the CPU.

Parameters: None.

Command Mode: Any modes

Usage Guide: This command can be used to monitor the CPU temperature of the switch.

Example: Show the temperature of the CPU of the switch.

Switch(Config)#show temperature

Temperature: 47.0625 ℃

7.1.20 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

7.1.21 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.

7.1.22 show udp ipv6

Command: show udp ipv6

Function*:* Show the current UDP connection.

Command mode: Admin and configuration mode.

Example:

LocalAddress LocalPort RemoteAddress RemotePort State

:: 69 :: 0 CLOSED

:: 1208 :: 0 CLOSED

Displayed Information	Explanation
LocalAddress	Local IPv6 address of UDP connection
LocalPort	Local port of UDP connection
RemoteAddress	Remote IPv6 address of UDP connection
RemotePort	Remote Port of UDP connection
State	The current state of UDP connection

7.1.23 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

7.1.24 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.

7.1.25 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 passes by the data packets is 30, and timeout period is defaulted at 2000ms.
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

7.2 Logging

7.2.1 logging executed-commands

Command: logging executed-commands {enable | disable}
Function: Enable or disable the logging executed-commands.
Parameter: None.
Command Mode: Global mode.
Default: Disable state.
Usage Guide: After enable this command, the commands executed by user at the console, telnet or ssh terminal will record the log, so it should be used with the logging LOGHOST command.
Example: Enable the command and send the commands executed by user into log host (10.1.1.1)
Switch(Config)#logging 10.1.1.1

Diagnosis Switch(Config)#logging executed-commands enable

7.2.2 show logging executed-commands state

Command: show logging executed-commands state
Function: Show the state of logging executed-commands.
Parameter: None.
Command Mode: Admin mode.
Default: None.
Usage Guide: Use this command to display the state (enable or disable).
Example:
Switch#show logging executed-commands state
Logging executed command state is enable

7.2.3 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

7.2.4 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

7.2.5 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

7.2.6 logging source-ip

Command: logging source-ip { <A.B.C.D> | <X:X::X:X> }
Function: Appoint the source IP address of the log packet which is sent to the log server, the ipv4 or ipv6 addresses can be configured.
Command Mode: Global mode
Usage Guide: Appoint the source IP address of the log packet which is sent to the log server, the ipv4 or ipv6 addresses can be configured. After configured this command, the log information sent to the server has the IP address; if this command is not configured, the log information does not have the IP address.
Example: Configure the source IP address of the log packet which is sent to the log server.
switch(config)#logging source-ip 2010::10

7.2.7 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, and the valid range is 1-65535. When only display logging buffered information of the line card must be added range parameter, but the main control has not the request.
Command Mode: Admin and Configuration Mode.
Default: No parameter specified indicates all the critical log information will be displayed.
Usage Guide: Warning and critical log information is saved in the buffer zone. When displayed to the terminal, their display format should be: index ID time <level> module ID [mission name] log information.

Example 1: Display the critical log information in the log buffer zone channel and related to the main control with index ID between 940 and 946.
Switch#show logging buffered level critical range 940 946
Example 2: Display all the information which level is warning and above in the log buffer zone channel.
Switch#show logging buffered level warning

7.2.8 show logging executed-commands state

Command: show logging executed-commands state
Function: Show the state of logging executed-commands.
Parameter: None.
Command Mode: Admin mode.
Default: None.
Usage Guide: Use this command to display the state (enable or disable).
Example:
Switch#show logging executed-commands state
Logging executed command state is enable

7.2.9 show logging source

Command: show logging source mstp
Function: Show the log information source of MSTP module.
Parameters: None.
Default: None.
Command mode: Admin and configuration mode.
Usage Guide: Check the log information source (include information channel, the information severity level) by **show logging mstp** command.
Example: Show the log information source of MSTP.
Switch#show logging source mstp
system module log switch status:

Channel	Onoff	Severity
logbuff	on	warning
loghost	on	warning
terminal	on	warning

7.3 Reload Switch after Specified Time

7.3.1 reload after

Command: reload after {[*<HH:MM:SS>*] [days <*days*>]}

Function: Reload the switch after a specified period of time.

Parameters: ***<HH:MM:SS>*** the specified time, HH (hours) ranges from 0 to 23, MM (minutes) and SS (seconds) range from 0 to 59.

<days> the specified days, unit is day, range from 1 to 30.

time and day may be configured at the same time or configured solely.

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. After this command is configured, it will prompt the reboot information when user logging in the switch by telnet.

Example: Set the switch to automatically reload after 2 days, 10 hours and 1 second.

Switch#reload after 10:00:01 days 2

Process with reboot after? [Y/N] y

Related Commands: reload, reload cancel, show reload

7.3.2 reload cancel

Command: reload cancel

Function: Cancel the specified time period to reload the switch.

Parameters: None

Command Mode: Admin mode.

Usage Guide: With this command, users can cancel the specified time period to reload the switch, that is, to cancel the configuration of command “reload after”. This command will not be reserved.

Example: Prevent the switch to automatically reboot after the specified time.

Switch#reload cancel

Reload cancel successful.

Related Commands: reload, reload after, show reload

7.3.3 show reload

Command: show reload

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

Parameters: None.

Command Mode: Admin and configuration mode

Usage Guide: With this command, users can view the configuration of command “reload after”

and check how long a time is left before rebooting the switch.

Example: View the configuration of command “reload after”. In the following case, the user set the switch to be rebooted in 10 hours and 1 second, and there are still 9 hours 59 minutes and 48 seconds left before rebooting it.

Switch#show reload

The original reload after configuration is 10:00:01.

System will be rebooted after 09:59:48 from now.

Related Commands: reload, reload after, reload cancel

7.4 Debugging and Diagnosis for Packets Received and Sent by CPU

7.4.1 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

7.4.2 cpu-rx-limitnotify enable interval

This command is not supported by the switch.

7.4.3 cpu-rx-limitnotify protocol (all|WORD)(enable|disable)

This command is not supported by the switch.

7.4.4 cpu-rx-ratelimit channel

This command is not supported by the switch.

7.4.5 cpu-rx-ratelimit enhanced

This command is not supported by the switch.

7.4.6 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 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 ARP packets to 500pps.

Switch(config)#cpu-rx-ratelimit protocol arp 500

7.4.7 cpu-rx-ratelimit queue-length

This command is not supported by the switch.

7.4.8 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

7.4.9 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 turns 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

7.4.10 protocol filter

This command is not supported by the switch.

7.4.11 show cpu-rx protocol

Command: show cpu-rx protocol [*<protocol-type>*]

Function: Show the statistics of the CPU received packets of the specified protocol type.

Parameter: <*protocol- type*> is the protocol type of the packets, if do not input parameters, show all statistic packets.

Command Mode: Admin and configuration mode

Default: None.

Usage Guide: This command is used to debug, it is supposed to be used with the help of the technical support.

Example: Show the statistics of CPU receiving ARP packets.

Switch(config)#show cpu-rx protocol arp

Type	Rate-limit	TotPkts	DropPkts	DelayCount	CurState
ARP	300	0	0	0	allowed

7.5 Mirror

7.5.1 monitor session source interface

Command: monitor session *<session>* source {interface *<interface-list>* | cpu} {rx| tx| both}
no monitor session *<session>* source {interface *<interface-list>* | cpu}

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 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. **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 1/0/1-4 and to mirror the datagram received by interface1/0/5

Switch(config)#monitor session 1 source interface ethernet 1/0/1-4 tx
Switch(config)#monitor session 1 source interface ethernet1/0/5 rx

7.5.2 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 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. In the moment, the command only IP ACL and MAC ACL.

Example: Configure the mirror interface 1/0/6 to filter with access list 120 in session 1.

Switch(config)#monitor session 1 source interface 1/0/6 access-list 120 rx

7.5.3 monitor session destination interface

Command: monitor session *<session>* destination interface *<interface-number>*

no monitor session *<session>* destination interface *<interface-number>*

Function: Specify the destination interface of the mirror. The no form command will disable this configuration.

Parameters: *<session>* is the session number of the mirror, which is currently limited to 1-4. ***<interface-number>*** is the destination interface of the mirror.

Default: None.

Command Mode: Global mode

Usage Guide: Only four 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 is removed, the mirror path configured will be removed at the same time. And if the destination interface is reconfigured, the interface, CPU 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 1/0/7 as the destination of the mirror.

Switch(config)#monitor session 1 destination interface ethernet 1/0/7

7.5.4 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.

Example:

Switch#show monitor

7.5.5 mirror sample rate

Command: monitor session *<session>* sample rate <num>

no monitor session *<session>* sample rate

Parameters: *<session>* is mirror session value, and it supports 1 to 4 at moment; **<num>**is sampled value, and ranges from 0 to 65535.

Function: It represents the how many packets mirror to destination port.

Command Mode: Global Mode.

Usage Guide: It represents how many packets mirror to destination port and it ranges from 0 to 65535, such as, when rate value equals 100, the first, 101, 201 packets can mirror destination port, when rate value equal 0, it does not configure samping rate, the default is notconfigured samping rate.

Example:

switch(config)#monitor session 1 sample rate 100

7.6 RSPAN

7.6.1 remote-span

Command: remote-span

no remote-span

Function: To configure VLAN to RSPAN VLAN. The no form of this command will delete the RSPAN VLAN.

Parameter: None.

Command Mode: VLAN Configuration Mode.

Default: Not configured.

Usage Guide: This command is used to configure the existing VLAN as RSPAN VLAN. Dedicated RSPAN VLAN should be configured before RSPAN can function. When configuring RSPAN VLAN, it should be made sure that specialized VLAN, such as the default VLAN, dynamic VLAN, private VLAN, multicast VLAN, and layer 3 interface enabled VLAN, should not be configured as RSPAN VLAN. If any existing sessions are still working when RSPAN is disabled, these sessions will be still working regardless the configuration change. However, if any layer 3 interface is configure in the VLAN after RSPAN is disable, the existing RSPAN session will be stopped.

Example:

Switch(Config-Vlan5)#remote-span

7.6.2 monitor session remote vlan

Command: monitor session <*session*> remote vlan <*vid*>

no monitor session <*session*> remote vlan

Function: To configure local mirror session to RSPAN. The no form of this command will restore the RSPAN to local mirror.

Parameter: <*session*>: session ID, range between 1~4. **<*vid*>:** The id of RSPAN VLAN.

Command Mode: Global Mode.

Default: Not configured.

Usage Guide: To configure local mirror session to RSPAN. The VLAN id is the RSPAN VLAN. The mirrored data grams will be attached with RSPAN tags.

Example:

Switch(config)#monitor session 1 remote vlan 5

7.6.3 monitor session reflector-port

Command: monitor session <*session*> reflector-port <*interface-number*>

no monitor session <*session*> reflector-port <*interface-number*>

Function: To configure reflector port, the no form of this command will delete the reflector port.

Parameter: <*session*>: Session ID, range between 1~4, **<*interface-number*>:** Interface number.

Command Mode: Global Mode.

Default: Not configured.

Usage Guide: This command configures the reflector port for the destination of mirror data grams, and disables the MAC learning function of the specified port. The configuration of reflector port is to change the mode of the local port from the destination port mode to be the reflector mode. Hence, the configuration of reflector port and the destination port are exclusive. The no command is used to restore the reflector port to normal port. The source port, in access or trunk mode, should not be added to RSPAN VLAN. When the reflector port is configured as springboard of CPU TX direction mirroring, it must be configured as TRUNK port and allows the RSPAN VLAN data passing, the Native VLAN should not be configured as RSPAN VLAN. After configured RSPAN, the vlan tag will be added on the packet of the egress mirror. It will cause the abort error frame on the reflection port, so the default MTU value of the switch should be modified.

Example:

Switch(config)#monitor session 1 reflector-port ethernet1/0/3

7.7 sFlow

7.7.1 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

7.7.2 sflow analyzer

Command: sflow analyzer sflowtrend

no sflow analyzer sflowtrend

Function: Configure the analyzer used by sFlow, the no command deletes the analyzer.

Parameter: sflowtrend is the analyzer of Inmon.

Command Mode: Global Mode

Default: Do not configure

Usage Guide: Configure this command when using sFlowTrend.

Example:

Switch(config)#sflow analyzer sflowtrend

7.7.3 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 e1/0/1 to 20 seconds.

Switch(Config-If-Ethernet1/0/1)#sflow counter-interval 20

7.7.4 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 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-Ethernet1/0/2)#sflow data-len 1000

7.7.5 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

7.7.6 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 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-Ethernet1/0/2)#sflow header-len 50

7.7.7 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 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

7.7.8 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 e1/0/1 to 10000 and the egress sample rate to 20000.

Switch(Config-If-Ethernet1/0/1)#sflow rate input 10000

Switch(Config-If-Ethernet1/0/1)#sflow rate output 20000

7.7.9 sflow version

Command: ***sflow version {4|5}***

no sflow version

Function: Configure the sFlow version number to switch the protocol versions supported by sFlow. The "no" form of this command is used to restore the default value. The sFlow agent-address command must not be configured when switching versions.

Parameter: 4: Indicates that the version number of current sFlow output message is 4.
5: Indicates that the version number of current sFlow output message is 5.
Command Mode: Global Mode.
Default: The default value is v4.
Usage Guide: Used to configure the version number of sFlow output message.
Example: Configure sFlow version number to 5.
Switch(Config)#sflow version 5

7.7.10 show sflow

Command: show sflow
Function: Display the sFlow configuration state.
Parameter: None.
Command Mode: All Modes.
Usage Guide: This command is used to acknowledge the operation state of sFlow.
Switch#show sflow
Sflow version 1.2
Agent address is 172.16.1.100
Collector address have not configured
Collector port is 6343
Sampler priority is 2
Sflow DataSource: type 2, index 194(Ethernet1/0/2)
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(Ethernet1/0/1)	One sample proxy data source of the sFlow is the interface e1/0/1 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 E1/0/1 interface is 192.168.1.200
Collector port is 6343	Default value of the port on E1/0/1 interface sampling proxy is 6343.

Counter interval is 20	The statistic sampling interval on e1/0/1 interface is 20 seconds
Sample rate is input 10000, output 0	The ingress traffic rate of e1/0/1 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 e1/0/1 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 e1/0/1 interface sampling proxy is 50
Sample version is 4	The datagram version of the sFlow group sent by the E1/0/1 interface sampling proxy is 4.

Chapter 8 Commands for Network Time Management

8.1 NTP

8.1.1 clock timezone

Command: clock timezone WORD {add | subtract} <0-23> [<0-59>]

no clock timezone WORD

Function: This command configures timezone in global mode, the no command deletes the configured timezone.

Parameters: WORD: timezone name, the length should not exceed 16

add | subtract: the action of timezone

<0-23>: the hour value

<0-59>: the minute value

Command Mode: Global mode

Default: None.

Usage Guide: The timezone name is invalid with the blank, the hour and minute value must be in the specific range.

Example: Configure the action as add for the eighth timezone globally.

Switch(config)#clock timezone aaa add 8

8.1.2 debug ntp adjust

Command: debug ntp adjust

no debug ntp adjust

Function: To enable/disable the debug switch of displaying local time adjust information.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable the debug switch of displaying local time adjust information.

Switch# debug ntp adjust

8.1.3 debug ntp authentication

Command: debug ntp authentication

no debug ntp authentication

Function: To display NTP authentication information, the no form command disabled the switch

of displaying NTP authentication information.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: To display NTP authentication information, if the switch is enabled, and if the packets schlepped authentication information when the packet in sending or receiving process, then the key identifier will be printed out.

Example: To enable the switch of displaying NTP authentication information.

Switch# debug ntp authentication

8.1.4 debug ntp events

Command: debug ntp events

no debug ntp events

Function: To enable/disable debug switch of displaying NTP event.

Parameter: None.

Default: Disable the debug switch of displaying NTP event.

Command Mode: Admin Mode.

Usage Guide: To enable debug switch of displaying NTP event, after that, if some server changed from available to unavailable or from unavailable to available, the received illegal packet events will be printed.

Example: To enable debug switch of displaying NTP event information.

Switch# debug ntp events

8.1.5 debug ntp packet

Command: debug ntp packet [send | receive]

no debug ntp packet [send | receive]

Function: To enable/disable the debug switch of displaying NTP packet information.

Parameter: send: The debug switch of sending NTP packet.

receive: The debug switch of receiving NTP packet.

If there is no parameter, that means should enable the sending and receiving switch of NTP packet in the same time.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable the debug switch of displaying NTP packet information.

Switch# debug ntp packet

8.1.6 debug ntp sync

Command: debug ntp sync

no debug ntp sync

Function: To enable/disable debug switch of displaying local time synchronization information.

Parameter: None.

Default: Disabled.

Command Mode: Admin Mode.

Usage Guide: None.

Example: To enable debug switch of displaying local time synchronization information.

Switch# debug ntp sync

8.1.7 ntp access-group

Command: ntp access-group server <*acl*>

no ntp access-group server <*acl*>

Function: To configure/cancel the access control list of NTP Server.

Parameter: <*acl*>: ACL number, range is from 1 to 99.

Default: Not configure the access control of NTP Server.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure access control list 2 on the switch.

Switch(config)#ntp access-group server 2

8.1.8 ntp authenticate

Command: ntp authenticate

no ntp authenticate

Function: To enable/cancel NTP authentication function.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To enable NTP authentication function.

Switch(config)#ntp authenticate

8.1.9 ntp authentication-key

Command: ntp authentication-key <*key-id*> md5 <*value*>

no ntp authentication-key <*key-id*>

Function: To enable/cancel NTP authentication function, and defined NTP authentication key.

Parameter: key-id: The id of key, range is from 1 to 4294967295.

value: The value of key, range between 1 to 16 of ascii code.

Default: The authentication key of NTP authentication is not configured by default.

Command Mode: Global Mode.

Usage Guide: None.

Example: To define the authentication key of NTP authentication, the key-id is 20, the md5 is abc.

Management Switch(config)# ntp authentication-key 20 md5 abc

8.1.10 ntp broadcast client

This command is not supported by the switch.

8.1.11 ntp broadcast server count

Command: ntp broadcast server count *<number>*

no ntp broadcast server count

Function: Set the max number of broadcast or multicast servers supported by the NTP client. The no operation will cancel the configuration and restore the default value.

Parameters: number： 1-100, the max number of broadcast servers.

Default: The default max number of broadcast servers is 50.

Command Mode: Global Mode.

Examples: Configure the max number of broadcast servers is 70 on the switch.

Switch(config)#ntp broadcast server count 70

8.1.12 ntp disable

Command: ntp disable

no ntp disable

Function: To disable/enable the NTP function on port.

Parameter: None.

Default: To enable NTP function on all ports.

Command Mode: vlan Configuration Mode.

Usage Guide: None.

Example: To disable the NTP function on vlan1 interface.

Switch(config)# interface vlan 1

Switch(Config-if-Vlan1)#ntp disable

8.1.13 ntp enable

Command: ntp enable

ntp disable

Function: To enable/disable NTP function globally.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To enable NTP function.

Switch(config)#ntp enable

8.1.14 ntp ipv6 multicast client

Command: ntp ipv6 multicast client

no ntp ipv6 multicast client

Function: Configure the specified interface to receive IPv6 NTP multicast packets, the no command will cancels the specified interface to receive IPv6 NTP multicast packets.

Parameter: None.

Command mode: vlan mode

Default: Interface does not receive IPv6 NTP multicast packets.

Usage guide: None.

Example: Enable the function for receiving IPv6 NTP multicast packets on vlan1 interface.

Switch(Config)# interface vlan 1

Switch(Config-if-Vlan1)#ntp ipv6 multicast client

8.1.15 ntp multicast client

Command: ntp multicast client

no ntp multicast client

Function: Configure the specified interface to receive NTP multicast packets, the no command will cancels the specified interface to receive NTP multicast packets.

Parameter: None.

Command mode: vlan mode

Default: Interface does not receive NTP multicast packets.

Usage guide: None.

Example: Enable the function for receiving NTP multicast packets on vlan1 interface.

Switch(Config)# interface vlan 1

Switch(Config-if-Vlan1)#ntp multicast client

8.1.16 ntp server

Command: ntp server {<*ip-address*> | <*ipv6-address*>} [version <*version_no*>] [key <*key-id*>]

no ntp server {<*ip-address*>|<*ipv6-address*>}

Function: To enable specified time server of time source, the no form of this command cancels the specified time server of time source.

Parameter: ip-address: IPv4 address of time server.

ipv6-address: IPv6 address of time server.

version: The version information configured for server.

version_no: The version number of server, range is from 1 to 4, default is 4.

key: To configure key for server.

key-id: The key id.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: None.

Example: To configure time server address as 1.1.1.1 on switch.
Switch(config)#ntp server 1.1.1.1

8.1.17 ntp syn-interval

Command: ntp syn-interval <1-3600>
no ntp syn-interval
Function: Configure the request packet sending interval of ntp client as 1s-3600s. The no command recovers to be the default value of 64s.
Default: 64s.
Command Mode: Global Mode.
Usage Guide: For responding the risk of ntp adjusting the system time under the high latency network, ntp client will select the time information with the smallest latency for the system time synchronization after sent 8 ntp time requisitions. So at the default configuration, ntp client sends the requisition packet once every 64s, after 8 times, it will adjust the time. It means to adjust the system time every 8 minutes. If user wants to configure the interval, such as one hour, user should adjust the packet sending interval as 450(3600/8) s.
Example: Configure to adjust the system time once an hour, and the packet sending time is 450s.
Switch(config)#ntp syn-interval 450

8.1.18 ntp trusted-key

Command: ntp trusted-key <*key-id*>
no ntp trusted-key <*key-id*>
Function: To configure the trusted key. The no command cancels the trusted key.
Parameter: key-id: The id of key, range is from 1 to 4294967295.
Default: Trusted key is not configured by default.
Command Mode: Global Mode.
Usage Guide: None.
Example: To configure the specified key 20 to trusted key.
Switch(config)# ntp trusted-key 20

8.1.19 show ntp status

Command: show ntp status
Function: To display time synchronization status, include synchronized or not, layers, address of time source and so on.
Parameter: None.
Default: None.
Command Mode: Admin and Configuration Mode.
Usage Guide: None.
Example:
Switch# show ntp status

Clock status: synchronized
Clock stratum: 3
Reference clock server: 1.1.1.2
Clock offset: 0.010 s
Root delay: 0.012 ms
Root dispersion: 0.000 ms
Reference time: TUE JAN 03 01:27:24 2006

8.1.20 show ntp session

Command: show ntp session [<*ip-address*> | <*ipv6-address*>]
Function: To display the information of all NTP session or one specific session, include server ID, server layer, and the local offset according to server. (The symbol * means this server is the selected local time source)
Parameter: ip-address: The IPv4 address of some specifics configured time server.
ipv6-address: The IPv6 address of some specifics configured time server.
If no parameter, the session relative information of all servers will be displayed (Include broadcast and multicast servers)
Default: None.
Command Mode: Admin and Configuration Mode.
Usage Guide: None.
Example:
(Switch)# show ntp session

	server	stream	type	rootdelay	rootdispersion	trustlevel
*	1.1.1.2	2	unicast	0.010s	0.002s	10
	2.2.2.2	3	unicast	0.005s	0.000s	10

8.2 SNTP

8.2.1 clock timezone

Command: clock timezone WORD {add | subtract} <0-23> [<0-59>]
no clock timezone WORD
Function: This command configures timezone in global mode, the no command deletes the configured timezone.
Parameters: WORD: timezone name, the length should not exceed 16
add | subtract: the action of timezone
<0-23>: the hour value
<0-59>: the minute value
Command Mode: Global mode
Default: None.
Usage Guide: The timezone name is invalid with the blank, the hour and minute value must be in

the specific range.

Example: Configure the action as add for the eighth timezone globally.

Switch(config)#clock timezone aaa add 8

8.2.2 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

8.2.3 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

8.2.4 sntp server

Command: sntp server {<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]

no sntp server {<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]

Function: Enable the specified time server as clock source, the no command deletes the specified time server.

Parameters: ip-address: IPv4 address of time server

ipv6-address: IPv6 address of time server

source: Specify the interface of the source address

vlan: Configure the virtual LAN

vlan no: Virtual LAN number, ranging from 1 to 4094

loopback: Configure loopback interface

loopback no: Loopback identifier, ranging from 1 to 1024

version: Configure the version for the server

version_no: Version number, ranging from 1 to 4, the default is 4

Default: Do not configure the time server.

Command Mode: Global mode

Usage Guide: None.

Example:

Configure the time server address as 1.1.1.1, specify the interface of the source address as vlan1:

Switch(config)#sntp server 1.1.1.1 source vlan 1

Delete the time server that the address is 1.1.1.1, the interface of the specified source address is vlan1:

Switch(config)#no sntp server 1.1.1.1 source vlan 1

8.2.5 show sntp

Command: show sntp

Function: Displays current SNTP client configuration and server status.

Parameters: N/A.

Command Mode: Admin and Configuration Mode.

Example: Displaying current SNTP configuration.

Switch#show sntp

SNTP server	Version	Last Receive
2.1.0.2	1	6

8.3 DNSv4/v6

8.3.1 clear dynamic-host

Command: clear dynamic-host {*<ip-address>* | *<ipv6-address>* | all}

Function: To delete the domain entry of specified address or all address in dynamic cache.

Parameter: ***<ip-address>*** is the IP address, in dotted decimal notation; ***<ipv6-address>*** is the IPv6 address; **all** is to delete the domain entry of all address in dynamic cache.

Command Mode: Admin Mode.

Default: Disabled.

Usage Guide: This command is used to manually delete the domain name and address entry in dynamic cache, this command is much useful when domain name have lived long time in cache.

Example: To delete the address of 202.108.22.5 of domain entry.

Switch# clear dynamic-host 202.108.22.5

8.3.2 debug dns

Command: debug dns {all | packet [send | recv] | events | relay}

no debug dns {all | packet [send | recv] | events | relay}

Function: To display the application debug information of DNS domain name resolution, the no form of this command disables the debug display.

Parameter: None.

Command Mode: Admin Mode.

Example:

Switch# debug dns all

Switch# ping host www.sina.com.cn

%Jan 01 00:03:13 2006 domain name www.sina.com.cn is to be parsed!

%Jan 01 00:03:13 2006 Dns query type is A!

%Jan 01 00:03:13 2006 Connect dns server 10.1.120.241 .....

ping www.sina.com.cn [202.108.33.32]

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 202.108.33.32, timeout is 2 seconds.

%Jan 01 00:03:15 2006 Host:www.sina.com.cn Address:202.108.33.32

.....

Success rate is 0 percent (0/5), round-trip min/avg/max = 0/0/0 ms

8.3.3 dns-server

Command: dns-server {*<ip-address>*|*<ipv6-address>*} [priority *<value>*]

no dns-server {*<ip-address>*|*<ipv6-address>*}

Function: To configure/delete DNS server.

Parameter: ***<ip-address>*** is the IP address, in dotted decimal notation, ***<ipv6-address>*** is the IPv6 address, ***<value>*** is the priority of DNS server, range between 0~255, 0 by default.

Command Mode: Global Mode.

Default: Not configuration.

Usage Guide: This command is used for configure or delete DNS server, when need to enable dynamic domain name mapping, the switch will sending a domain name search request packet to configured DNS server, the DNS server can be configured no more than 6. The priority is the optional parameter, if priority is configured, the DNS server must be organized according to the order of priority, from high to low. That is the switch sending domain name search request to the server which have the biggest priority, so some DNS server with quick search speed and used frequently can be configured to highest priority. If priority is not configured, to search DNS server must according to the configuration order. When the switch serves as a DNS SERVER, the queries to the DNS SERVER won't follow the above privilege rule; instead, the requests will be sent to all configured servers at the same time

Example: To configure the priority of DNS server as 200, the server's address is 10.1.120.241.

Switch(config)# dns-server 10.1.120.241 priority 200

8.3.4 dns lookup

Command: dns lookup {ipv4 | ipv6} *<hostname>*

Function: To enable DNS dynamic domain name resolution.

Parameter: {ipv4 | ipv6} means the IPv4 or IPv6 address look up, ***<hostname>*** is the resolute dynamic host name, less than 63 characters.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used to look up correspond address based on entered client name, it can look up both IPv4 and IPv6 address. This command only used for domain name mapping, it have no other application function. When command is running, interrupt is forbidding. If configured many servers and domain name suffix, longer time will be required for domain name mapping.

Example: To look up the IPv4 address of www.sina.com.

Switch(config)# dns lookup ipv4 www.sina.com

8.3.5 show dns name-server

Command: show dns name-server

Function: To display the information of configured DNS server.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

Switch# show dns name-server

DNS NAME SERVER:

Address	Priority
10.1.120.231	100
10.1.180.85	80
2001::1	20

8.3.6 show dns domain-list

Command: show dns domain-list

Function: To display the suffix information of configured DNS domain name.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

Switch# show dns domain-list

DNS DOMAIN LIST:

com.cn

edu.cn

8.3.7 show dns hosts

Command: show dns hosts

Function: To display the dynamic domain name information of resolute by switch.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

Switch# show dns hosts

Total number of dynamic host is 2

DNS HOST LIST：

Hostname	Address	Time to live	Type
www.sina.com.cn	202.108.33.32	168000	dynamic
www.ipv6.org	2001:6b0:1:	168060	dynamic

8.3.8 show dns config

Command: show dns config

Function: Display the configured global DNS information on the switch.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

Switch(config)#show dns config

ip dns server enable

ip domain-lookup enable

the maximum of dns client in cache is 3000, timeout is 5

dns client number in cache is 0

dns dynamic host in cache is 0

dns name server number is 1

dns domain-list number is 0

8.3.9 show dns client

Command: show dns client

Function: Display the DNS Client information maintained by the switch.

Parameter: None.

Command Mode: Admin and Configuration Mode.

Example:

Switch(config)#show dns client

DNS REQUEST LIST:

Total number of dns request is 2

Address	Request Id
192.168.11.141	1
192.168.11.138	2

8.3.10 ip domain-lookup

Command: ip domain-lookup

no ip domain-lookup

Function: To enable/disable DNS function, whether the switch will send dynamic DNS domain queries to the real DNS server or not.

Parameter: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used to enable or disable the switch DNS dynamic query function. If DNS dynamic query function is enabled, the DNS server will resolve the host name and domain name to the IPv4 or IPv6 address for requests from the clients. If DNS is disabled, client applications will not be able to send any DNS requests to the DNS server. In this situation, only the static address resolution is available. For the address mapping in the resolve cache, which is learnt through DNS before, will be invalid after aging.

Example: To enable DNS function, can resolve the domain name dynamic.

Switch(config)# ip domain-lookup

8.3.11 ip domain-list

Command: ip domain-list *<WORD>*

no ip domain-list *<WORD>*

Function: To configure/delete domain name suffix.

Parameter: ***<WORD>*** is the character string of domain name suffix, less than 63 characters.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used to configure or delete suffix of domain name, when the entered domain name is not integrity (such as sina), the switch can add suffix automatically, after that, address mapping can run, the domain name suffix can be configured no more than 6. The first configured domain name suffix will be added first.

Example: To configure domain name suffix of com.

Switch(config)# ip domain-list com

8.3.12 ip dns server

Command: ip dns server

no ip dns server

Function: Enable/disable DNS SERVER function.

Parameter: None.

Command Mode: Global Mode.

Default: Disabled by default.

Usage Guide: After the DNS SERVER function is enabled, the switch will be able to receive and handle DNS Requests from the clients by looking up locally or forward the request to the real DNS

server.

Example: Configure to enable the dns server function of the switch.

Switch(config)#ip dns server

8.3.13 ip dns server queue maximum

Command: ip dns server queue maximum <1-5000>

no ip dns server queue maximum

Function: Configure the max number of client information in the switch queue.

Parameter: <1-5000> the value can be 1—5000.

Command Mode: Global Mode.

Default: The default client number is 3000.

Usage Guide: When receiving a DNS Request from a client, the switch will cache the client's information. But the number of client information in the queue should not exceed the configured maximum number; otherwise the client's request won't be handled.

Example: Set the max number of client information in the switch queue as 2000.

Switch(config)#ip dns server queue maximum 2000

8.3.14 ip dns server queue timeout

Command: ip dns server queue timeout <1-100>

no ip dns server queue timeout

Function: Configure the timeout value of caching the client information on the switch.

Parameters: <1-100> the value can be1—100s.

Command Mode: Global Mode.

Default: The default timeout value is 5s.

Usage Guide: When receiving a DNS Request from a client, the switch will cache the client's information. But the time of maintaining the client information should not exceed the configured maximum timeout value; otherwise the client's information will be cleared out.

Example: Configure the maximum timeout value of caching the client information on the switch as 10s.

Switch(config)#ip dns server queue timeout 10

8.4 Summer Time

8.4.1 clock summer-time absolute

Command: clock summer-time <*word*> absolute <*HH:MM*> <*YYYY.MM.DD*> <*HH:MM*> <*YYYY.MM.DD*> [<*offset*>]

no clock summer-time

Function: Configure summer time range, the time in this range is summer time. The no command deletes the configuration.

Parameter: ***<word>*** is the time zone name of summer time; ***<HH:MM>*** is the start time, the format is hour (from 0 to 23):minute (from 0 to 59); ***<YYYY.MM.DD>*** is the start date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31); ***<HH:MM>*** is the end time, the format is hour (from 0 to 23):minute (from 0 to 59); ***<YYYY.MM.DD>*** is the end date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31); ***<offset>*** is the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes.

Default: There is no summer time range.

Command Mode: Global Mode

Usage Guide: This command sets the absolute start and end time for summer time. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. Note: the end time should be bigger than the start time for configuring summer time.

Example: Configure the time range of summer time at 12:10 from april 6th to augest 6th in 2010, offset value as 70 minutes, summer time is named as aaa.

Switch(config)#clock summer-time aaa absolute 12:10 2010.4.6 12:10 2010.8.6 70

8.4.2 clock summer-time recurring

Command: clock summer-time <*word*> recurring <*HH:MM*> <*MM.DD*> <*HH:MM*> <*MM.DD*> [<*offset*>]

no clock summer-time

Function: Configure the recurrent summer time range, the time in this range is summer time.

Parameter: ***<word>*** is the time zone name of summer time; ***<HH:MM>*** is the start time, the format is hour (from 0 to 23):minute (from 0 to 59); ***<MM.DD>*** is the start date, the format is month(from 1 to 12).date(from 1 to 31); ***<HH:MM>*** is the end time, the format is hour(from 0 to 23):minute(from 0 to 59); ***<MM.DD>*** is the end date, the format is month(from 1 to 12).date(from 1 to 31); ***<offset>*** is the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes.

Default: There is no summer time range.

Command Mode: Global Mode

Usage Guide: This command sets the start and the end time for the recurrent summer time. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. There is no relation between the recurrent summer time to the year, the system clock will be changed when it reaches to the start and the end time point of summer time year after year. This command supports the summer time of southern hemisphere.

Example: Configure the time range of summer time at 12:10 from april 6th to augest 6th year

after year, offset value as 70 minutes, summer time is named as aaa.
Switch(config)# clock summer-time aaa recurring 12:10 4.6 12:10 8.6 70

8.4.3 clock summer-time recurring

Command: clock summer-time <*word*> recurring <*HH:MM*> <*week*> <*day*> <*month*> < *HH:MM* > <*week*> <*day*> <*month*> [<*offset*>]

no clock summer-time

Function: Configure the recurrent summer time range, the time in this range is summer time.

Parameter: ***<word>*** is the time zone name of summer time; ***<HH:MM>*** is the start time, the format is hour(from 0 to 23):minute(from 0 to 59); ***<week>*** is the week from 1 to 4, first or last; ***<day>*** is the week value, the value as “Sun”, “Mon”, “Tue”, “Wed”, “Thu”, “Fri”, “Sat”; ***<month>*** is the month, the value as ”Jan”, “Feb”, “Mar”, “Apr”, “May”, ”Jun”, “Jul”, “Aug”, “Sep”, “Oct”, “Nov”, “Dec”; ***<HH:MM>*** is the end time, the format is hour(from 0 to 23):minute(from 0 to 59); ***<week>*** is the week from 1 to 4, first or last; ***<day>*** is the week value, the value as “Sun”, “Mon”, “Tue”, “Wed”, “Thu”, “Fri”, “Sat”; ***<month>*** is the month, the value as ”Jan”, “Feb”, “Mar”, “Apr”, “May”, ”Jun”, “Jul”, “Aug”, “Sep”, “Oct”, “Nov”, “Dec” ***<offset>*** is the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes.

Default: There is no summer time range.

Command Mode: Global Mode

Usage Guide: This command sets the start and end time for the recurrent summer time flexibly. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. There is no relation between the recurrent summer time to the year, the system clock will be changed when it reaches to the start and the end time point of summer time year after year. This command supports summer time of southern hemisphere.

Example: Configure summer time at 12:10 from the first Monday of april to the last Saturday of augest year after year, offset value as 70 minutes, summer time is named as aaa.
Switch(config)#clock summer-time aaa recurring 12:10 1 mon apr 12:10 last sat aug 70

Chapter 9 Commands for POE

9.1 POE

9.1.1 PoE

9.1.1.1 power inline enable (Global)

Command: power inline enable
no power inline enable
Function: Enable /disable global PoE.
Parameters: None.
Command Mode: Global Mode.
Default: Disable.
Usage Guide: With PoE globally disabled, there would be no power output no matter what the power state of a specified port is.
Example: Globally disable PoE.
Switch(Config)#no power inline enable

9.1.1.2 power inline enable (Port)

Command: power inline enable
no power inline enable
Function: Enable/disable PoE power supply.
Parameters: None.
Command Mode: Port Mode.
Default: Enable.
Usage Guide: Enabled: Automatically detect PD. In such a state, PSE will automatically detect and classify a PD, and provide power supply for it according to the classification. If a PD connection is detected, its specified output power will be satisfied as long as there is enough available power, after which the corresponding LED indicator will be updated. Otherwise, the power distribution rules will decide whether or not to implement this power supply. During a normal power supply process, if PD requires for an extra power which exceeds the max threshold value, the supply will be cut off and the corresponding LED indicator will be updated. When the PD is disconnected from the PSE normally, PSE will stop outputting power supply and update the corresponding LED indicator.

Disabled: Disable power supply. With the PSE power supply disabled, no power will be output regardless of the existence of PD connections, which means the port will act as a regular Ethernet data port without affecting data transmission.

When it is globally disabled, no power supply will be output regardless of the power supply is enabled or disabled on ports.

Examples: Disable power supply on ports1, 3, 4, 5, 6.

Switch(Config)# interface ethernet 1/0/1;3-6

Switch(Config-Port-Range)#no power inline enable

9.1.1.3 power inline power-up mode

Command: power inline power-up mode (af|high-inrush|pre-at|at)
no power inline power-up mode

Function: Modify the power-on mode of the port.

Parameters: af：IEEE 802.3af mode, generally, it is powered by PD supporting IEEE 802.3af mode；

high-inrush：Inrush current 700mA-1A, generally non-standard PD power supply;

pre-at：Pre-IEEE 802.3at mode，inrush current 400mA-450mA，switch to a higher current (700mA-1.0A) within 75 milliseconds after the port is powered up, typically for PDs that support Pre-IEEE 802.3at mode;

at：IEEE 802.3at mode, inrush current 700mA-1A, generally, it is powered by PD supporting IEEE 802.3at mode；

Command Mode: Port Mode.

Default: high-inrush mode.

Usage Guide: The power-on mode of the port needs to be selected according to the PD support.

Examples: Change the power-on mode of the port to IEEE 802.3at mode.

Switch(config)#interface ethernet 1/0/1;3-6

Switch(Config-If-Port-Range)#power inline power-up mode at

9.1.1.4 power inline high-inrush

Command: power inline high-inrush enable
no power inline high-inrush enable

Function: Enable the allowed high-inrush current when nonstandard PD is powered instantaneously, disable the allowed high-inrush current.

Parameter: None.

Command Mode: Global mode

Default: The allowed high-inrush current is not enabled.

Usage Guide: high-inrush current will be brought when nonstandard PD is powered instantaneously, it will result PSE self-protection to make PD power failure. Here, if this

nonstandard PD must be powered, it needs to allow the high-inrush current.

Example: Enable the allowed high-inrush current when nonstandard PD is powered instantaneously.

Switch(config)#power inline high-inrush enable

9.1.1.5 power inline legacy

Command: power inline legacy enable

no power inline legacy enable

Function: Set whether or not to provide power supply for non-standard IEEE PD.

Parameters: None.

Command Mode: Global Mode.

Default: Do not provide power supply for non-standard IEEE PD.

Usage Guide: With this function enabled, the switch will be compatible with and provide power supply for non-standard IEEE PD.

Examples: Set the switch to provide power supply for non-standard IEEE PD.

Switch(Config)#power inline legacy enable

9.1.1.6 power inline max (Global)

Command: power inline max *<max-wattage>*

no power inline max

Function: Set the global max output power of PoE.

Parameters: max-wattage: value of the max output power, in W. The ranging of DCRS-5960-52T-PoE and DCRS-5960-28T-PoE from 37 to 740W is valid.

Command: Global Mode.

Default: The global max output power of DCRS-5960-52T-PoE and DCRS-5960-28T-PoE is 740W. The **no power inline max** will resume the default configuration.

Usage Guide: Setting a global max output power can guarantee a secure power supply and an effective method to control the power consumed by connected subordinate devices.

Example: Set the global max output power to 50W.

Switch(Config)#power inline max 50

9.1.1.7 power inline max (Port)

Command: power inline max *<max-wattage>*

no power inline max

Function: Set the max output power of a specified port.

Parameters: max-wattage: the value of the max output power, in mW, ranging from 1 to 15400mW (802.3af)/1 to 3000mW (802.3at), with a granularity of 100mW. Any value less than 100mW will be taken as 100mW, that is, 1~100 equals 100, 15301~15400 equals 15400. But the

value set by users will be maintained without being rounded up.

Command Mode: Port Mode.

Default: The max output power of a port is 15400mW (802.3af)/3000mW (802.3at).

Usage Guide: This configuration will effectively control the output power of each port in cooperation with the global max power.

Example: Set the max output power of Port 1 to 0.8W.

Switch(Config)#interface ethernet 1/0/1

Switch(Config-Ethernet1/0/1)#power inline max 800

9.1.1.8 power inline police

Command: power inline police enable

no power inline police enable

Function: Enable/disable the power priority management policy mode.

Parameters: None.

Command Mode: Global Mode.

Default: The power priority management policy mode is disabled.

Usage Guide: Decide whether to use priority policy in power management policy. The “enable” command will make priority policy in effect, while “no” command will recover the first-come-first-served policy. With priority policy enabled, port priority can be configured individually.

In priority mode, when not enough PSE power is available, ports with low priority will be closed to satisfy the power supply for ports with high priority, no matter how long the access time of a PD is. If two ports have same priority, the one with smaller sequence number is higher privileged.

In first-come-first-served mode, new PDs will not get power supply if available PSE power is not enough.

Example: Enable the power priority policy mode.

Switch(Config)#power inline police enable

9.1.1.9 power inline priority

Command: power inline priority {critical | high | low}

Function: Set power supply priority of a port.

Parameters: critical: the highest-level priority. **high:** high-level priority. **low:** low-level priority.

Command Mode: Port Mode.

Default: Port priority is low.

Usage Guide: This command will take effect in the mode of “power inline police enable”. Without enough available power for newly connected PD, ports with higher priority will get power supply first.

Examples: Set the priority of Port 1 to high and that of Port 2 to critical.

Switch(Config)#interface ethernet 1/0/1

Switch(Config-Ethernet1/0/1)#power inline priority high

Switch(Config)#interface ethernet 1/0/2
Switch(Config-Ethernet1/0/2)#power inline priority critical

9.1.2 PoE Monitoring and Debugging

9.1.2.1 Monitoring and Debugging Information

9.1.2.1.1 show power inline

Command: show power inline
Function: Display global PoE configurations and status.
Parameters: None.
Command Mode: Admin Mode.
Default: None.
Usage Guide: The meanings of each field are listed in the following table:

Field	Description
Power Inline Status	The global PoE status: enabled or disabled
Power Available	The global max value of available power
Power Used	The global value of used power
Power Remaining	The global value of remaining power
Min Voltage	The global threshold of under-voltage
Max Voltage	The global threshold of over-voltage
Police	The power priority policy status: enabled or disabled
Legacy	The non-standard PD detection status: enabled or disabled
Disconnect	The PD disconnection mode
HW Version	The hardware version of the PoE module
SW Version	The software version of the PoE module
Mode	Power supply mode Signal: power supply over signal cables (Alternative A) spare: power supply over spare cables (sAlternative B)

Examples: Display the current global PoE status
Switch#show power inline
Power Inline Status: On
Power Available: 370 W
Power Used: 0 W
Power Remaining: 370 W
Min Voltage: 44 V
Max Voltage: 57 V
Police: Off
Legacy: Off

Disconnect: Ac

Mode: Signal

HW Version: 30

SW Version: 05.0.5

9.1.2.1.2 show power inline interface ethernet

Command: show power inline interface [ethernet <*interface-number*> | <*interface-name*>]

Function: Display the PoE configuration and status on specified ports.

Parameters: interface-list: a list of specified ports, specifying all ports by default.

Command Mode: Admin Mode.

Default: None.

Usage Guide: The meaning of each field is listed in the following table.

Field	Description
Interface	Ethernet port number
Status	Power supply status Enable: Power supply enabled Disable: Power supply disabled
Oper	Working status On: PD is normally connected and powered Off: PD is not connected faulty: PD detection failed deny: not enough available power or the required power is over the limit
Power	The power used by the port currently
Max	The max power allowed to be distributed to the port
Current	The present current of the port
Volt	The present voltage of the port
Priority	The Power supply priority Critical: the highest-level priority High: the high-level priority Low: the low-level priority
Class	Class Usage PD Input Power (W) 0 Default 0.44~12.95 1 Optional 0.44~3.84 2 Optional 3.84~6.49 3 Optional 6.49~12.95 4 Reserved treated as class 0 and reserved for future use It is impossible for a compatible PD to provide a class 4 signal

Examples: Display the current PoE status on port 1 to port 6.

Switch# show power inline interface ethernet 1/0/1-6

Interface Status Oper Power(mW) Max(mW) Current(mA) Volt(V) Priority Class

---------- ------- ------ --------- ------- ----------- ------- -------- -----

Ethernet1/0/1	enable	off	0	15400	0	0	high	0
Ethernet1/0/2	enable	off	0	15400	0	0	low	0
Ethernet1/0/3	enable	off	0	15400	0	0	low	0
Ethernet1/0/4	enable	off	0	15400	0	0	low	0
Ethernet1/0/5	enable	off	0	15400	0	0	low	0
Ethernet1/0/6	enable	off	0	15400	0	0	low	0

9.1.2.1.3 debug power inline

Command: debug power inline

no debug power inline

Function: Enable or disable the PoE debugging.

Parameters: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: With debugging enabled, relative information will be printed in the key processes while implementing commands, for further debugging reference whenever an error occurs. The “no” command will disable the debugging.

Examples: Enable PoE debugging.

Switch#debug power inline

Chapter 10 Commands for IPv6

10.1 DHCPv6

10.1.1 clear ipv6 dhcp binding

Command: clear ipv6 dhcp binding [*<ipv6-address>*] [pd <*ipv6-prefix* | *prefix-length*>]
Function: To clear one specified DHCPv6 assigned address binding record or all the IPv6 address binding records.
Parameter: ***<ipv6-address>*** is the specified IPv6 address with binding record; ***<ipv6-prefix| prefix-length>*** is the specified IPv6 prefix with binding record; To clear all IPv6 address binding record if there is no specified record.
Command Mode: Admin Configuration Mode.
Usage Guide: DHCPv6 IPv6 address binding information can be displayed through the command **show ipv6 dhcp binding**. If DHCPv6 client does not use the DHCPv6 allocated IPv6 address but when the life time of the IPv6 address does not end, the DHCPv6 server will not remove its bind for this address. In this situation, the address binding information can be removed manually through this command; and if no parameter is appended, this command will remove all the address binding information, then all addresses and prefix will be assigned again in the DHCPv6 address pool.
Example: To delete all binding record of IPv6 address and prefix.
Switch#clear ipv6 dhcp binding
Relative Command: show ipv6 dhcp binding

10.1.2 clear ipv6 dhcp conflict

Command: clear ipv6 dhcp conflict [*<address>*]
Function: Clear the address with the conflict record in address conflict log.
Parameter: ***<address>*** is the specified address with the conflict record, no specified address will clear all conflict records.
Command mode: Admin Mode
Usage Guide: With **show ipv6 dhcp conflict** command, the user can check the conflict in which IP addresses. With this command, the user can clears the conflict record of an address. If no specified address will clear the conflict record of all addresses in log. After the conflict records are cleared in log, these addresses can be used by DHCPv6 server again.
Example: When administrator checks the conflict logs, administrator discovers that address 2001::1 with the conflict record is not used, so its record will be cleared from address conflict files.
Switch#clear ipv6 dhcp conflict 2001::1

10.1.3 clear ipv6 dhcp statistics

Command: clear ipv6 dhcp statistics

Function: Clear the statistic records of DHCPv6 packets, the statistic counter of DHCPv6 packets is cleared.

Parameter: None.

Command mode: Admin Mode

Usage Guide: With **show ipv6 dhcp statistics** command, the user can check the statistic information of the counter for DHCPv6 packets, all statistic information is an accumulative value. With this command will clear the counter to check the debugging conveniently.

Example: Clear the counter of DHCPv6 packets.

Switch#clear ipv6 dhcp statistics

Relative Command: show ipv6 dhcp statistics

10.1.4 debug ipv6 dhcp client packet

Command: debug ipv6 dhcp client {event | packet}

no debug ipv6 dhcp client {event | packet}

Function: To enable the debugging messages for protocol packets of DHCPv6 prefix delegation client, the no form of this command will disable the debugging information.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch**#** debug ipv6 dhcp client packet

10.1.5 debug ipv6 dhcp detail

Command: debug ipv6 dhcp detail

no debug ipv6 dhcp detail

Function: To display the debug information of all kinds of packets received or sent by DHCPv6, the no form of this command disabled this function.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch# debug ipv6 dhcp detail

10.1.6 debug ipv6 dhcp relay packet

Command: debug ipv6 dhcp relay packet

no debug ipv6 dhcp relay packet

Function: To enable the debugging information for protocol packets of DHCPv6 relay, the no form of this command will disable the debugging.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch# debug ipv6 dhcp relay packet

10.1.7 debug ipv6 dhcp server

Command: debug ipv6 dhcp server { event | packet }

no debug ipv6 dhcp server { event | packet }

Function: To enable the debugging information of DHCPv6 server, the no form of this command will disable the debugging.

Parameter: event is to enable debugging messages for DHCPv6 server events, such as address allocation; packet is for debugging messages of protocol packets of DHCPv6 server.

Default: Disabled.

Command Mode: Admin Mode.

Example:

Switch#debug ipv6 dhcp server packet

10.1.8 dns-server

Command: dns-server *<ipv6-address>*

no dns-server *<ipv6-address>*

Function: To configure the IPv6 address of the DNS server for DHCPv6 client; the no form of this command will remove the DNS configuration.

Parameter: *<ipv6-address>* is the IPv6 address of DNS Server.

Default: No configured address pool of DNS Server by default.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Usage Guide: For each address pool, at most three DNS server can be configured, and the addresses of the DNS server must be valid IPv6 addresses.

Example: To configure the DNS Server address of DHCPv6 client as 2001:da8::1.

Switch(dhcp-1-config)#dns-server 2001:da8::1

10.1.9 domain-name

Command: domain-name *<domain-name>*

no domain-name *<domain-name>*

Function: To configure domain name of DHCPv6 client; the no form of this command will delete the domain name.

Parameter: *<domain-name>* is the domain name, less than 32 characters.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Default: The domain name parameter of address pool is not configured by default.

Usage Guide: At most 3 domain names can be configured for each address pool.

Example: To set the domain name of DHCPv6 client as test.com.cn

Switch(dhcp-1-config)#domain-name test.com.cn

10.1.10 excluded-address

Command: excluded-address *<ipv6-address>*

no excluded-address *<ipv6-address>*

Function: To configure the specified IPv6 address to be excluded from the address pool, the excluded address will not be allocated to any hosts; the no form of this command will remove the configuration.

Parameter: ***<ipv6-address>*** is the IPv6 address to be excluded from being allocated to hosts in the address pool.

Default: Disabled

Command Mode: DHCPv6 address pool configuration mode.

Usage Guide: This command is used to preserve the specified address from DHCPv6 address allocation.

Example: To configure to exclude 2001:da8:123::1 from DHCPv6 address allocation.

Switch(config)#excluded-address 2001:da8:123::1

10.1.11 ipv6 address

Command: ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>*

no ipv6 address *<prefix-name> <ipv6-prefix/prefix-length>*

Function: To configure the specified interface to use prefix delegation for address allocation. The no form of this command will disable the using of prefix delegation for address allocation.

Parameters: ***<prefix-name>*** is a string with its length no more than 32, designating or manual configuring the name of the address prefix defined in the prefix pool. ***<ipv6-prefix/prefix-length>*** is latter part of the IPv6 address excluding the address prefix, as well as its length.

Command Mode: Interface Configuration Mode.

Default: No global address is configured for interfaces by default.

Usage Guide: The IPv6 address of an interface falls into two parts: ***<prefix-name>*** and ***<ipv6-prefix>/<prefix-length>***. If routing advertisement has been enabled, the first 64 bits of the addresses will be advertised. The address generated by ***<prefix-name>*** and ***<ipv6-prefix/prefix-length>*** combination will be removed, and the advertising of the prefix will be disabled. Only one ***<ipv6-prefix/prefix-length>*** can be configured for one prefix name.

Example: If the prefix name my-prefix designates 2001:da8:221::/48, then the following command will add the address 2001:da8:221:2008::2008 to interface VLAN1.

Switch(Config-if-Vlan1)# ipv6 address my-prefix 0:0:0:2008::2008/64

10.1.12 ipv6 dhcp client pd

Command: ipv6 dhcp client pd *<prefix-name>* [rapid-commit]

no ipv6 dhcp client pd

Function: To configure DHCPv6 prefix delegation client for the specified interface. The no form of this command will disable the DHCPv6 prefix delegation client and remove the allocated address prefix.

Parameters: <*prefix-name*> is the string with its length no more than 32, which designates the name of the address prefix. If **rapid-commit** optional is specified and the prefix delegation server enables the rapid-commit function, then the prefix delegation server will reply the prefix delegation client with the REPLY message directly. And the prefix delegation request will be accomplished by exchanging messages once.

Command Mode: Interface Configuration Mode.

Default: DHCPv6 prefix delegation client is not enabled by default.

Usage Guide: This command is used to configure the prefix delegation client on the specified interface, an interface with prefix delegation client enabled will send SOLICIT packets to try to get address prefix from the server. If the prefix is retrieved correctly, the address prefix in the global address pool can be used by the **ipv6 address** command to generate a valid IPv6 address. This command is exclusive with **ipv6 dhcp server** and **ipv6 dhcp relay destination**. If the prefix delegation client is disabled for an interface, then the address prefix which is get from this interface through prefix delegation client, will be removed from the global address pool. Also the interface address which is generated by the prefix delegation client will be removed, and routing advertisement with the prefix will be disabled. If any general prefix has been configured by the **ipv6 general-prefix** command, the same prefix learnt from prefix delegation will be disagreed.

Example:

Switch(Config-if-Vlan1)#ipv6 dhcp client pd ClientA rapid-commit

10.1.13 ipv6 dhcp client pd hint

Command: ipv6 dhcp client pd hint <*prefix|prefix-length*>

no ipv6 dhcp client pd hint <*prefix|prefix-length*>

Function: Designate the prefix demanded by the client and its length. The no operation of this command will delete that prefix and its length from the specified interface.

Parameters: <*prefix|prefix-length*> means the prefix demanded by the client and its length.

Command Mode: Interface Configure Mode.

Default Settings: There is no such configuration in the system by default.

Usage Guide: The system designates a prefix and its length on the interface for a client. If client prefix-proxy demanding function is enabled on the interface and hint function is enabled on the switch, the user will have prior claim to the prefix it demands and the prefix length when the server allocates them. Only one hint prefix is allowed in the system.

Examples:

Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48

10.1.14 ipv6 dhcp pool

Command: ipv6 dhcp pool <*poolname*>

no ipv6 dhcp pool <*poolname*>

Function: To configure the address pool for DHCPv6, and enter the DHCPv6 address pool configuration mode. In this mode, information such as the address prefix to be allocated, the DNS server addresses, and domain names, can be configured for the DHCPv6 client. The no form of

this command will remove the configuration of the address pool.

Parameter: ***< poolname>*** is the address pool name of DHCPv6 with its length no more than 32.

Default: Any DHCPv6 address pool are not configured by default.

Command Mode: Global Mode.

Usage Guide: This command should be launched in global configuration mode, and falls in DHCPv6 address pool configuration mode if launched successfully. To remove a configured address pool, interface bindings related to the address pool, as well as the related address bindings will be removed.

Example: To define an address pool, named 1.

Switch(config)#ipv6 dhcp pool 1

10.1.15 ipv6 dhcp relay destination

Command: ipv6 dhcp relay destination {[*<ipv6-address>*] [interface { *<interface-name>* | vlan *<1-4096>* }] }

no ipv6 dhcp relay destination { [*<ipv6-address>*] [interface { *<interface-name>* | vlan *<1-4096>* }] }

Function: To configure the destination to which the DHCPv6 relay forwards the DHCPv6 requests from the clients, the destination should be the address of an external DHCPv6 relay or the DHCPv6 server. The no form of this command will remove the configuration.

Parameters: ***<ipv6-address>*** is the address of the destination to which the DHCPv6 relay forwards; ***<interface-name>*** or VLAN is the interface name or VLAN id which is used for forwarding of DHCPv6 requests, ***<interface-name>*** should be a lay three VLAN name, and the VLAN id is limited between 1 and 4096. If ***<ipv6-addess>*** is a global unicast address, the **interface** parameter should not be configured; If ***<ipv6-address>*** is an local address, the **interface** parameter is required be configured; The destination address for the DHCPv6 server will be the multicast address of **ALL_DHCP_Servers (FF05::1:3)**, if the interface parameter is configured only.

Command Mode: Interface Configuration Mode.

Default: By default, destination address for DHCPv6 relay is not configured.

Usage Guide: This command is used to configure the DHCPv6 relay for the specified interface, the address should be the address of another DHCPv6 relay or the address DHCPv6 server. At most three relay addresses can be configured for an interface. To be mentioned, the DHCPv6 relay stops working only if all the relay destination address configurations have been removed. This command is mutually exclusive to "**ipv6 dhcp server**" and "**ipv6 dhcp client pd**" commands.

Example:

Switch(Config-if-Vlan1)#ipv6 dhcp relay destination 2001:da8::1

10.1.16 ipv6 dhcp server

Command: ipv6 dhcp server *<poolname>* [preference *<value>*] [rapid-commit] [allow-hint]

no ipv6 dhcp server *<poolname>*

Function: This command configures the address pool which will be allocated by the DHCPv6 server through the specified interface. The no form of this command will remove the address

pool configuration.

Parameters: <*poolname*> is a string with its length less than 32, which designates the name of the address pool which is associated with the specified interface. If the **rapid-commit** option has been specified, the DHCPv6 server send a REPLY packet to the client immediately after receiving the SOLICIT packet. If the **preference** option has been specified, **<*value*>** will be the priority of the DHCPv6 server, with its value allowed between 0 and 255, and with 0 by default, the bigger the preference value is, the higher the priority of the DHCPv6 server. If the **allow-hint** option has been specified, the client expected value of parameters will be appended in its request packets.

Command Mode: Interface Configuration Mode.

Default: DHCPv6 address pool based on port is not configured by default.

Usage Guide: This command configure the DHCPv6 address pool which is applied by the DHCPv6 server for the specified interface, as well as optional parameters. One VLAN can bind many DHCPv6 address pools and assign the address for DHCPv6 request packet from direct-link and relay delegation.

Example:

Switch(Config-if-Vlan1)#ipv6 dhcp server PoolA preference 80 rapid-commit allow-hint

10.1.17 ipv6 general-prefix

Command: ipv6 general-prefix *<prefix-name> <ipv6-prefix/prefix-length>*

no ipv6 general-prefix *<prefix-name>*

Function: To define an IPv6 general prefix. The no form of this command will delete the configuration.

Parameter: *<prefix-name>* is a character string less than 32 characters, to use as IPv6 general prefix name. ***<ipv6-prefix/prefix-length>*** is defined as IPv6 general prefix.

Command Mode: Global Mode.

Default: IPv6 general prefix is not configured by default.

Usage Guide: If IPv6 general prefix is configured, the interface will use the configured prefix for IPv6 address generating. Commonly, the general prefix is used for enterprise IPv6 prefix, and when entering an IPv6 address, users can simply add the address suffix of to the name of the general prefix. The configured address prefix will be reserved in the general address prefix pool. At most 8 general prefix can be configured at the same time. When trying to remove a configured general prefix name, the operation will fail if any interfaces used the configured prefix. Only one general prefix for a prefix name. The general prefix can not use the same prefix definition with prefixes learnt from prefix delegation.

Example: To set the prefix of 2001:da8:221::/48 to general prefix my-prefix.

Switch(config)# ipv6 general-prefix my-prefix 2001:da8:221::/48

10.1.18 ipv6 local pool

Command: ipv6 local pool *<poolname> <prefix/prefix-length> <assigned-length>*

no ipv6 local pool *<poolname>*

Function: To configure the address pool for prefix delegation. The no form of this command will

remove the IPv6 prefix delegation configuration.

Parameters: <*poolname*> is the name for the IPv6 address pool of the prefix delegation, the length name string should be less than 32. **<*prefix/prefix-length*>** is the address prefix and its length of the prefix delegation. **<*assigned-length*>** is the length of the prefix in the address pool which can be retrieved by the client, the assigned prefix length should be no less than the value of **<*prefix-length*>**

Command Mode: Global Mode.

Default: No IPv6 prefix delegation address pool is configured by default.

Usage Guide: This command should be used with the "**prefix delegation pool**" command to allocate address prefixes to the clients. If IPv6 prefix delegation is removed, the associated "**prefix delegation**" command will be in-effective either.

10.1.19 lifetime

Command: lifetime {<*valid-time*> | infinity} {<*preferred-time*> | infinity}

no lifetime

Function: To configure the life time for the addresses or the address prefixes allocated by DHCPv6. The no form of this command will restore the default setting.

Parameters: <*valid-time*> and <*preferred-time*> are the valid life time and preferred life time respectively for the allocated IPv6 addresses in the local address pool. Its value is allowed to be between 1 and 31536000 in seconds, and **<*preferred-time*>** should never be bigger than **<*valid-time*>**. The **infinity** parameter designates the maximum life time.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Default: The default valid life time and preferred life time are 2592000 seconds (30 days) and 604800 seconds (7 days) respectively.

Example: To configure the valid life time as 1000 seconds, and the preferred life time as 600 seconds.

Switch(config)#lifetime 1000 600

10.1.20 network-address

Command: network-address <*ipv6-pool-start-address*> {<*ipv6-pool-end-address*> | <*prefix-length*>} [eui-64]

no network-address

Function: To configure the DHCPv6 address pool; the no form of this command will remove the address pool configuration.

Parameters: <*ipv6-pool-start-adderss*> is the start of the address pool; **<*ipv6-pool-end-address*>** is the end of the address pool; **<*prefix-length*>** is the length of the address prefix, which is allowed to be between 3 and 128, and 64 by default, the size of the pool will be determined by **<*prefix-length*>** if it has been specified. **<*ipv6-pool-end-address*>** and **<*prefix-length*>** alternative options to determine the size of the IPv6 address pool. If **<*prefix-length*>** is 64 and the **eui-64** option has been configured, the DHCPv6 server will allocate IPv6 addresses according to the EUI-64 standard, or the DHCPv6 server will be allocating addresses sequentially.

Default: No address pool is configured by default.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Usage Guide: This command configures the address pool for the DHCPv6 server to allocate addresses, only one address range can be configured for each address pool. To be noticed, if the DHCPv6 server has been enabled, and the length of the IPv6 address prefix has been configured, the length of the prefix in the address pool should be no less than the length of the prefix of the IPv6 address of the respective layer three interfaces in the switch. If ***<ipv6-pool-end-address>*** is bigger than ***<ipv6-pool-start-address>***, this command returns at once.

Example: To configure the address range for address pool as 2001:da8:123::100-2001:da8:123::200.

Switch(dhcp-1-config)#network-address 2001:da8:123::100 2001:da8:123::200

Relative Command: excluded-address

10.1.21 prefix-delegation

Command: prefix-delegation *<ipv6-prefix/prefix-length> <client-DUID>* [iaid *<iaid>*] [lifetime <valid-time> <preferred-time>]

no prefix-delegation *<ipv6-prefix/prefix-length> <client-DUID>* [iaid *<iaid>*]

Function: To configure dedicated prefix delegation for the specified user. The no form of this command will remove the dedicated prefix delegation.

Parameters: *<ipv6-prefix/prefix-length>* is the length of the prefix to be allocated to the client. ***<client-DUID>*** is the DUID of the client. DUID with the type of DUID-LLT and DUID-LL are supported, the DUID of DUID-LLT type should be of 14 characters. ***<iaid>*** is the value to be appended in the IA_PD field of the clients' requests. ***<valid-time>*** and ***<preferred-time>*** are the valid life time and the preferred life time of the IPv6 address allocated to the clients respectively, in seconds, and its value is allowed between 1 and 31536000. However ***<preferred-time>*** should be less than ***<valid-time>***. If not configured, the default ***<valid-time>*** will be 2592000, while ***<preferred-time>*** will be 604800.

Command Mode: DHCPv6 Address Pool Configuration Mode.

Default: Disabled.

Usage Guide: This command configures the specified IPv6 address prefix to bind with the specified client. If no IAID is configured, any IA of any clients will be able get this address prefix. At most eight static binding address prefix can be configured for each address pool. For prefix delegation, static binding is of higher priority than the prefix address pool.

Example: The following command will allocate 2001:da8::/48 to the client with DUID as 0001000600000005000BBFAA2408, and IAID as 12.

Switch(dhcp-1-config)#prefix-delegation 2001:da8::/48 0001000600000005000BBFAA240812

10.1.22 prefix-delegation add static route

Command: prefix-delegation add static route

no prefix-delegation add static route

Function: DHCPv6 issues a ipv6 static route according to assigned prefix, client link address and interface vlan when DHCPv6 server distribute ipv6 prefix.

Parameters: None.

Default: Do not issues static route by default.

Command Mode: Ipv6 address pool configuration Mode.

Usage Guide: The command is configured on address pool mode and it must have associated ipv6 local pool namely prefix address pool at the same time.

Example: Configure static route function on dhcpv6 server.

Switch(config)# service dhcpv6

Switch(config)# ipv6 local pool client-prefix-pool 2001:da8:1800::/40 48

Switch(config)# ipv6 dhcp pool dhcp-pool

Switch(dhcpv6- dhcp-pool-config)#dot1x enable

Switch(dhcpv6- dhcp-pool-config)# prefix-delegation pool client-prefix-pool

Switch(dhcpv6- dhcp-pool-config)#prefix-delegation add static route

10.1.23 prefix-delegation pool

Command: prefix-delegation pool *<poolname>* [lifetime *<valid-time>* *<preferred-time>*]

no prefix-delegation pool *<poolname>*

Function: To configure prefix delegation name used by DHCPv6 address pool. The no form of this command deletes the configuration.

Parameters: ***<poolname>*** is the name of the address prefix pool, the length name string should be less than 32. ***<valid-time>*** and ***<preferred-time>*** are the valid life time and the preferred life time of the IPv6 address allocated to the clients respectively, in seconds, and its value is allowed between 1 and 31536000.However ***<preferred-time>*** should be less than ***<valid-time>***, if not configured, the default ***<valid-time>*** will be 2592000, while ***<preferred-time>*** will be 604800.

Command Mode: DHCPv6 address pool configuration mode.

Default: The prefix delegation name used by DHCPv6 address pool is not configured.

Usage Guide: This command configures the name of the address prefix pool for address allocation. If configured, the addresses in the prefix address pool will be allocated to the clients. This command can be used in association with the **ipv6 local pool** command. For one address pool, only one prefix delegation pool can be bound. When trying to remove the prefix name configuration, the prefix delegation service of the server will be unavailable, if both the address pool is not associated with the prefix delegation pool and no static prefix delegation binding is enabled.

Example:

Switch(dhcp-1-config)#prefix-delegation pool abc

10.1.24 service dhcpv6

Command: service dhcpv6

no service dhcpv6

Function: To enable DHCPv6 server function; the no form of this command disables the configuration.

Parameter: None.

Default: Disabled.

Command Mode: Global Mode.

Usage Guide: The DHCPv6 services include DHCPv6 server function, DHCPv6 relay function, DHCPv6 prefix delegation function. All of the above services are configured on ports. Only when DHCPv6 server function is enabled, the IP address assignment of DHCPv6 client, DHCPv6 relay and DHCPv6 prefix delegation functions enabled can be configured on ports.

Example: To enable DHCPv6 server.

Switch(config)#service dhcpv6

10.1.25 show ipv6 dhcp

Command: show ipv6 dhcp

Function: To show the enable switch and DUID of DHCPv6 service.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show the enable switch and DUID of DHCPv6 service, server identifier options only use DUID of DUID-LLT type.

Example:

Switch#show ipv6 dhcp

DHCPv6 is enabled

LLT DUID is <00:01:00:01:43:b7:1b:81:00:03:0f:01:5f:9d>

LL DUID is <00:03:00:01:00:03:0f:01:5f:9d>

10.1.26 show ipv6 dhcp binding

Command: show ipv6 dhcp binding [*<ipv6-address>*| pd *<ipv6-prefix|prefix-length>*|count]

Function: To show all the address and prefix binding information of DHCPv6.

Parameter: ***<ipv6-address>*** is the specified IPv6 address; **count** show the number of DHCPv6 address bindings.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show all the address and prefix binding information of DHCPv6, include type, DUID, IAID, prefix, valid time and so on.

Example:

Switch#show ipv6 dhcp binding

Client: iatype IANA, iaid 0x0e001d92

DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83

IANA leased address: 2001:da8::10

Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds

Lease obtained at %Jan 01 01:34:44 1970

Lease expires at %Jan 31 01:34:44 1970 (2592000 seconds left)

The number of DHCPv6 bindings is 1

10.1.27 show ipv6 dhcp conflict

Command: show ipv6 dhcp conflict

Function: Show the log for the address that have a conflict record.

Command mode: Admin and Configuration Mode.

Example:

Switch# show ipv6 dhcp conflict

10.1.28 show ipv6 dhcp interface

Command: show ipv6 dhcp interface [<*interface-name*>]

Function: To show the information for DHCPv6 interface.

Parameter: ***<interface-name>*** is the name and number of interface, if the***<interface-name>*** parameter is not provided, then all the DHCPv6 interface information will be shown.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show the information for DHCPv6 interface, include Port Mode (Prefix delegation client、DHCPv6 server、DHCPv6 relay) , and the relative conformation information under all kinds of mode.

Example:

Switch#show ipv6 dhcp interface vlan10

Vlan10 is in server mode

Using pool: poolv6

Preference value: 20

Rapid-Commit is disabled

10.1.29 show ipv6 dhcp pool

Command: show ipv6 dhcp pool [<*poolname*>]

Function: To show the DHCPv6 address pool information.

Parameter: ***<poolname>*** is the DHCPv6 address pool name which configured already, and the length less than 32 characters. If the ***<poolname>*** parameter is not provided, then all the DHCPv6 address pool information will be shown.

Command Mode: Admin and Configuration Mode.

Usage Guide: To display the configuration and dynamic assignment information for DHCPv6 address pool, include the name of DHCPv6 address pool, the prefix of DHCPv6 address pool, excluded address, DNS server configuration, relative prefix information and so on. To display assigned address binding number of address pool that is used as address assignment server. To display assigned prefix number of address pool that is used as prefix delegation server.

Example:

Switch#show ipv6 dhcp pool poolv6

10.1.30 show ipv6 dhcp statistics

Command: show ipv6 dhcp statistics

Function: To show the statistic of all kinds of DHCPv6 packets by DHCPv6 server.

Command Mode: Admin and Configuration Mode.

Example:

Switch#show ipv6 dhcp server statistics

Address pools	1
Active bindings	0
Expiried bindings	0
Malformed message	0

Message	Recieved
DHCP6SOLICIT	0
DHCP6ADVERTISE	0
DHCP6REQUEST	0
DHCP6REPLY	0
DHCP6RENEW	0
DHCP6REBIND	0
DHCP6RELEASE	0
DHCP6DECLINE	0
DHCP6CONFIRM	0
DHCP6RECONFIGURE	0
DHCP6INFORMREQ	0
DHCP6RELAYFORW	0
DHCP6RELAYREPLY	0

Message	Send
DHCP6SOLICIT	0
DHCP6ADVERTISE	0
DHCP6REQUEST	0
DHCP6REPLY	0
DHCP6RENEW	0
DHCP6REBIND	0
DHCP6RELEASE	0
DHCP6DECLINE	0
DHCP6CONFIRM	0
DHCP6RECONFIGURE	0
DHCP6INFORMREQ	0
DHCP6RELAYFORW	0
DHCP6RELAYREPLY	0

Show information	Explanation

Address pools	To configure the number of DHCPv6 address pools;
Active bindings	The number of auto assign addresses;
Expiried bindings	The number of expiried bindings;
Malformed message	The number of malformed messages;
Message Recieved	The statistic of received DHCPv6 packets.
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST	The number of DHCPv6 REQUEST packets.
DHCP6REPLY	The number of DHCPv6 REPLY packets.
DHCP6RENEW	The number of DHCPv6 RENEW packets.
DHCP6REBIND	The number of DHCPv6 REBIND packets.
DHCP6RELEASE	The number of DHCPv6 RELEASE packets.
DHCP6DECLINE	The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets.
DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets.
DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets.
DHCP6RELAYREPLY	The number of DHCPv6 RELAYREPLY packets.
Message Send	The statistic of sending DHCPv6 packets
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.
DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets.
DHCPv6REQUEST	The number of DHCPv6 REQUEST packets.
DHCP6REPLY	The number of DHCPv6 REPLY packets.
DHCP6RENEW	The number of DHCPv6 RENEW packets.
DHCP6REBIND	The number of DHCPv6 REBIND packets.
DHCP6RELEASE	The number of DHCPv6 RELEASE packets.
DHCP6DECLINE	The number of DHCPv6 DECLINE packets.
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets.
DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets.
DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets.
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets.

10.1.31 show ipv6 general-prefix

Command: show ipv6 general-prefix

Function: To show the IPv6 general prefix pool information.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show the IPv6 general prefix pool information, include the prefix number in general prefix pool, the name of every prefix, the interface of prefix obtained, and the prefix value.

Example:

Switch#show ipv6 general-prefix

10.1.32 show ipv6 local pool

Command: show ipv6 local pool

Function: To show the statistic information of DHCPv6 prefix pool.

Command Mode: Admin and Configuration Mode.

Usage Guide: To show the statistic information of DHCPv6 prefix pool, include the name of prefix pool, the prefix and prefix length as well as assigned prefix length, the number of assigned prefix and information in DHCPv6 address pool.

Example:

Switch#show ipv6 local pool

Pool	Prefix	Free	In use
a	2010::1/0/48	65536	0

10.2 DHCPv6 option37, 38

10.2.1 Commands for DHCPv6 option37, 38

10.2.1.1 address range

Command: address range <*start-ip*> <*end-ip*>

no address range <*start-ip*> <*end-ip*>

Function: This command is used to set address range for a DHCPv6 class in DHCPv6 address pool configuration mode, the no command is used to remove the address range. The prefix/plen form is not supported.

Parameters: start-ip, defines the start address of the address pool

end-ip, defines the end address of the address pool

Default: None.

Command Mode: DHCPv6 address pool class configuration mode

Usage Guide: It is necessary to check the address range assigned to class in order to make sure that it doesn't exceed the address range of relevant address pool. A class is assigned a single address range and the address range assigned to different class in the same address pool can overlap. If you do not use this command to assign address range for a DHCPv6 class, then the range for it will be the whole subnet of the address pool by default.

Example: Associate a DHCPv6 class named CLASS1 to dhcpv6 pool 1 and assign the address range from 2001:da8:100:1::2 to 2001:da8:100:1::30 for CLASS1.

Switch(Config)#ipv6 dhcp pool 1

Switch(dhcp-1-config)#class CLASS1

Switch(dhcp-1-class-CLASS1-config)#address range 2001:da8:100:1::2 2001:da8:100:1::30

10.2.1.2 prefix range

Command: prefix range <start-prefix> <end-prefix>

no prefix range <start-prefix> <end-prefix>

Function: This command is used to set prefix address range for a DHCPv6 class in DHCPv6 address pool configuration mode, the no command is used to remove the prefix address range.

Parameters: start-prefix, defines the start prefix address of the prefix address pool

end-prefix, defines the end prefix address of the prefix address pool

Default: None.

Command Mode: DHCPv6 address pool class configuration mode

Usage Guide: It is necessary to check the prefix address range assigned to class in order to make sure that it doesn't exceed the prefix address range of relevant prefix address pool. A class is assigned a single prefix address range. If you do not use this command to assign prefix address range for a DHCPv6 class, then the range for it will be the whole range of the prefix address pool by default.

Example: Assign the prefix address range from 2001:da8:1800:1120::/64 to 2001:da8:1800:1130::/64 for CLASS1.

Switch(Config)#ipv6 dhcp pool 1

Switch(dhcp-1-config)#class CLASS1

Switch(dhcp-1-class-CLASS1-config)# prefix range 2001:da8:1800:1120::/64 2001:da8:1800:1130::/64

10.2.1.3 class

Command: class <*class-name*>

no class <*class-name*>

Function: This command associates class to address pool in DHCPv6 address pool configuration mode and enters class configuration mode in address pool. Use the no command to remove the link.

Parameters: class-name, the name of DHCPv6 class.

Default: None.

Command Mode: DHCPv6 address pool configuration mode

Usage Guide: It is recommended to define this class first using global command of IPv6 DHCP class. No class will be created if you input a class name which doesn't exist.

Example: Associate the DHCPv6 class named CLASS1 to dhcpv6 pool 1.

Switch(Config)#ipv6 dhcp pool 1

Switch(dhcp-1-config)#class CLASS1

10.2.1.4 ipv6 dhcp class

Command: ipv6 dhcp class <*class-name*>

no ipv6 dhcp class <*class-name*>

Function: This command defines a DHCPv6 class and enters DHCPv6 class configuration mode, the no operation of this command removes this DHCPv6 class.

Parameters: class-name, the name of DHCPv6 class which is a string with a length of less than 32

Default: None.

Command Mode: Global configuration mode

Usage Guide: Configure a group of option 37 or option 38, or configure option 37 and option 38 simultaneously in a DHCPv6 class. This command can be used when the server supports DHCPv6 class only.

Example: Define a DHCPv6 class named CLASS1.

Switch(Config)# ipv6 dhcp class CLASS1

10.2.1.5 ipv6 dhcp relay remote-id

Command: ipv6 dhcp relay remote-id <*remote-id*>

no ipv6 dhcp relay remote-id

Function: This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which <remote-id> is the remote-id in user-defined option 37 and it is a string with a length of less than 128. The no operation of this command restores remote-id in option 37 to enterprise-number together with vlan MAC address.

Parameters: remote-id, user-defined content of option 37.

Default: Using vlan MAC address as remote-id content by default such as “00-01-ac-12-23” with ‘-’ hyphen.

Command Mode: Interface configuration mode

Usage Guide: Because the option 37 information added by switch may associate with third-party DHCPv6 servers, users can specify the remote-id content based on server condition when default remote-id of the switch cannot satisfy the demand of server. The enterprise-number together with vlan MAC address is used as the remote-id by default.

Example: Enable abc as the remote-id of DHCPv6 option 37.

Switch(Config-if-vlan1)# ipv6 dhcp relay remote-id abc

10.2.1.6 ipv6 dhcp relay remote-id option

Command: ipv6 dhcp relay remote-id option

no ipv6 dhcp relay remote-id option

Function: This command enables switch relay to support the option 37, the no form of this command disables it.

Parameters: None.

Default: Disable the relay option 37.

Command Mode: Global configuration mode

Usage Guide: Only after this command is configured, DHCPv6 relay agent can add option 37 in DHCPv6 request packets before sending it to server or next relay agent. Make sure that DHCPv6

service has been enabled before execute this command.

Example: Enable the switch relay to support option 37.

Switch(Config)#service dhcpv6

Switch(Config)#ipv6 dhcp relay remote-id option

10.2.1.7 ipv6 dhcp relay subscriber-id

Command: ipv6 dhcp relay subscriber-id <subscriber-id>

no ipv6 dhcp relay subscriber-id

Function: This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which <subscriber-id> is the subscriber-id in user-defined option 38 and it is a string with a length of less than 128. The no operation of this command restores subscriber-id in option 38 to vlan name together with port name such as "Vlan2+Ethernet1/0/2".

Parameters: subscriber-id, user-defined content of option 38

Default: Set subscriber-id in option 38 to vlan name together with port name.

Command Mode: Interface configuration mode

Usage Guide: Because the option 38 information added by switch may associate with third-party DHCPv6 servers, users can specify the subscriber-id content based on server condition when standard subscriber-id of the switch cannot satisfy the demand of server. The vlan name together with physical port name is used as the subscriber-id in option 38 by default.

Example: Enable abc as the subscriber-id of DHCPv6 option 38.

Switch(Config-if-vlan1)# ipv6 dhcp relay subscriber-id abc

10.2.1.8 ipv6 dhcp relay subscriber-id option

Command: ipv6 dhcp relay subscriber-id option

no ipv6 dhcp relay subscriber-id option

Function: This command enables switch relay to support the option 38, the no form of this command disables it.

Parameters: None.

Default: Disable the relay option 38.

Command Mode: Global configuration mode

Usage Guide: Only after this command is configured, DHCPv6 relay agent can add option 38 in DHCPv6 request packets before sending it to server or next relay agent. Make sure that DHCPv6 service has been enabled before execute this command. The option 38 of switch relay is disabled by default.

Example: Enable the switch relay to support option 38.

Switch(Config)#service dhcpv6

Switch(Config)#ipv6 dhcp relay subscriber-id option

10.2.1.9 ipv6 dhcp relay subscriber-id select delimiter

Command: ipv6 dhcp relay subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter

WORD |)

no ipv6 dhcp relay subscriber-id select delimiter

Function: Configures user configuration options to generate subscriber-id. The no form of this command restores to its original default configuration, i.e. vlan name together with port name.

Parameters: (**sp | sv | pv | spv**): a selection in combinations of slot, port and vlan, among which **sp** represents slot and port, **sv** represents slot and vlan, **pv** represents port and vlan, and **spv** represents slot, port and vlan.

WORD: the delimiter between slot, port and vlan which ranges among (#|.|,|;|:|/|space). Note that there're two **delimiter WORDs** here, of which the former is the delimiter between slot and port and the latter is the one between port and vlan.

Default: Null.

Command Mode: Global configuration mode

Usage Guide: The command has no effect on ports with self-defined subscriber-id. If user redefines the subscriber-id of the port after using the command, the user-defined one prevails. This configuration is null by default.

Example:

Switch(config)# ipv6 dhcp relay subscriber-id select sp delimiter #

10.2.1.10 ipv6 dhcp server remote-id option

Command: ipv6 dhcp server remote-id option

no ipv6 dhcp server remote-id option

Function: This command enables DHCPv6 server to support the identification of option 37, the no form of this command disables it.

Parameters: None.

Default: Do not support option 37.

Command Mode: Global configuration mode

Usage Guide: Configure this command if option 37 options is expected to be identified and processed by DHCPv6 server, otherwise they will be ignored. Option 37 is not supported by default.

Example: Enable the DHCPv6 server to support option 37.

Switch(Config)# ipv6 dhcp server remote-id option

10.2.1.11 ipv6 dhcp server select relay-forw

Command: ipv6 dhcp server select relay-forw

no ipv6 dhcp server select relay-forw

Function: This command enables the DHCPv6 server to support selections when multiple option 37 or option 38 options exist and the option 37 and option 38 of relay-forw in the innermost layer are selected. The no operation of it restores the default configuration, i.e. selecting option 37 and option 38 of the original packets.

Parameters: None.

Default: Selecting option 37 and option 38 of the original packets.

Command Mode: Interface configuration mode

Usage Guide: Make sure that the server has been enabled to support option 37 and option 38 before use this command. The system selects option 37 and option 38 of the original packets by default.

Example: Configure that the vlan1 interface of DHCPv6 server selects option 37 and option 38 of relay-forw in the innermost layer.

Switch(Config-if-vlan1)# ipv6 dhcp server select relay-forw

10.2.1.12 ipv6 dhcp server subscriber-id option

Command: ipv6 dhcp server subscriber-id option

no ipv6 dhcp server subscriber-id option

Function: This command enables DHCPv6 server to support the identification of option 38, the no operation of this command disables it.

Parameters: None.

Default: Do not support option 38.

Command Mode: Global configuration mode

Usage Guide: Configure this command if option 38 is expected to be identified and processed by DHCPv6 server, otherwise they will be ignored. option 38 is not supported by default.

Example: Enable DHCPv6 server to support option 38.

Switch(Config)# ipv6 dhcp server subscriber-id option

10.2.1.13 ipv6 dhcp snooping information option remote-id format

Command: ipv6 dhcp snooping information option remote-id format {hex | acsii }

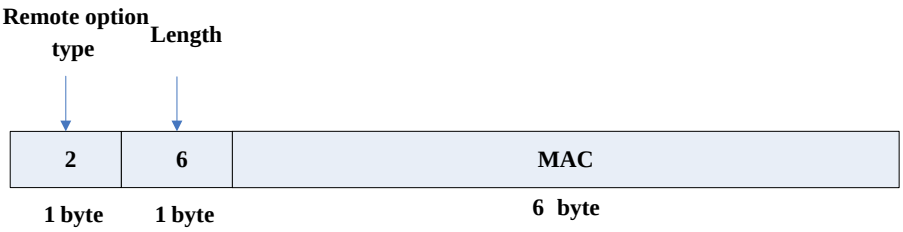
Function: This command can configure the remote-id format of the switch relay agent's DHCPv6 option37.

Parameters: default means that the remote-id is the VLAN MAC address of the hexadecimal switch. acsii means that the remote-id is the VLAN MAC address of the acsii format switch.

Default: The default remote-id format of option37 is acsii.

Command Mode: Global configuration mode.

Usage Guide: The hexadecimal remote-id format's definition is as below:



The MAC is the VLAN MAC address of the switch.

Example: Configure the default remote-id format of the switch relay agent's DHCPv6 option37.

Switch(config)#ipv6 dhcp snooping information option remote-id format acsii

10.2.1.14 ipv6 dhcp snooping information option subscriber-id format

This command is not supported by the switch.

10.2.1.15 ipv6 dhcp snooping remote-id

Command: ipv6 dhcp snooping remote-id <*remote-id*>

no ipv6 dhcp snooping remote-id

Function: This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which <remote-id> is the content of remote-id in user-defined option 37 and it is a string with a length of less than 128. The no form of this command restores remote-id in option 37 to enterprise-number together with vlan MAC address.

Parameters: remote-id, user-defined content of option 37.

Default: Using vlan MAC address as remote-id content by default such as "00-01-ac-12-23" with '-' hyphen.

Command Mode: Port mode

Usage Guide: Because option 37 information added by switch may associate with third-party DHCPv6 servers, users can specify remote-id content based on server condition when standard remote-id of the switch cannot satisfy the demand of server. The enterprise-number together with vlan MAC address is used as the remote-id by default.

Example: Enable abc as remote-id of DHCPv6 option 37.

Switch(Config-if-Ethernet1/0/1)# ipv6 dhcp snooping remote-id abc

10.2.1.16 ipv6 dhcp snooping remote-id option

Command: ipv6 dhcp snooping remote-id option

no ipv6 dhcp snooping remote-id option

Function: This command enables DHCPv6 SNOOPING to support option 37, the no form of this command disables it.

Parameters: None.

Default: Disable.

Command Mode: Global configuration mode

Usage Guide: Only after this command is configured, DHCPv6 SNOOPING can add option 37 in DHCPv6 packets before sending it to server or relay agent. Make sure that DHCPv6 SNOOPING has been enabled before execute this command. The system disables option 37 of DHCPv6 SNOOPING by default.

Example: Enable option 37 in DHCPv6 SNOOPING.

Switch(Config)#ipv6 dhcp snooping enable

Switch(Config)#ipv6 dhcp snooping remote-id option

10.2.1.17 ipv6 dhcp snooping remote-id policy

Command: ipv6 dhcp snooping remote-id policy {drop | keep | replace}

no ipv6 dhcp snooping remote-id policy

Function: This command is used to configure the reforward policy of the system when receiving DHCPv6 packets with option 37, among which the **drop** mode means that the system simply discards it with option 37, **keep** mode means that the system keeps option 37 unchanged and forwards the packets to the server and **replace** mode means that the system replaces option 37 of current packets with its own before forwarding it to the server. The no operation of this command sets reforward policy of DHCPv6 packets with option 37 as replace.

Parameters: None.

Default: Using replace mode to replace option 37 of current packets with system's own.

Command Mode: Global configuration mode

Usage Guide: Since DHCPv6 client packets may already include option 37 information, corresponding processing policy of DHCPv6 SNOOPING is required to develop. If the forwarding policy is set as **replace**, option 37 has to be enabled in advance. Use replace mode to replace option 37 of current packets with system's own by default.

Example: Configure the reforward policy of DHCPv6 packets with option 37 as keep for DHCPv6 SNOOPING.

Switch(Config)# ipv6 dhcp snooping remote-id policy keep

10.2.1.18 ipv6 dhcp snooping subscriber-id

Command: ipv6 dhcp snooping subscriber-id <subscriber-id>

no ipv6 dhcp snooping subscriber-id

Function: This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which <subscriber-id> is the content of subscriber-id in user-defined option 38 and it is a string with a length of less than 128. The no operation of this command restores subscriber-id in option 38 to vlan name together with port name such as "Vlan2+Ethernet1/0/2".

Parameters: subscriber-id, user-defined content of option 38

Default: Set subscriber-id in option 38 to vlan name together with port name.

Command Mode: Port mode

Usage Guide: Because option 38 information added by switch may associate with third-party DHCPv6 servers, users can specify subscriber-id content based on server condition when standard subscriber-id of the switch cannot satisfy the demand of server. The vlan name together with physical port name is used as subscriber-id in option 38 by default.

Example: Enable abc as subscriber-id of DHCPv6 option 38.

Switch(Config-if-Ethernet1/0/1)#ipv6 dhcp snooping subscriber-id abc

10.2.1.19 ipv6 dhcp snooping subscriber-id option

Command: ipv6 dhcp snooping subscriber-id option

no ipv6 dhcp snooping subscriber-id option

Function: This command enables DHCPv6 SNOOPING to support option 38, the no form of this command disables it.

Parameters: None.

Default: Disable option 38 of DHCPv6 SNOOPING.

Command Mode: Global configuration mode

Usage Guide: Only after this command is configured, DHCPv6 SNOOPING can add option 38 in DHCPv6 packets before sending it to server or relay agent. Make sure that DHCPv6 SNOOPING has been enabled before executing this command. The system disables option 38 of DHCPv6 SNOOPING by default.

Example: Enable option 38 in DHCPv6 SNOOPING.

Switch(Config)#ipv6 dhcp snooping enable

Switch(Config)#ipv6 dhcp snooping subscriber-id option

10.2.1.20 ipv6 dhcp snooping subscriber-id policy

Command: ipv6 dhcp snooping subscriber-id policy {drop | keep | replace}

no ipv6 dhcp snooping subscriber-id policy

Function: This command is used to set the reforward policy of the system when receiving DHCPv6 packets with option 38, among which the **drop** mode means that the system simply discards it with option 38, **keep** mode means that the system keeps option 38 unchanged and forwards the packets to the server and **replace** mode means that the system replaces option 38 of current packets with its own before forwarding it to the server. The no operation of this command sets the reforward policy of DHCPv6 packets with option 38 as replace.

Parameters: None.

Default: Using replace mode to replace option 38 of current packets with system's own.

Command Mode: Global configuration mode

Usage Guide: Since DHCPv6 client packets may already include option 38 information, corresponding processing policy of DHCPv6 SNOOPING is requested to develop. If the reforward policy is set as **replace**, option 38 has to be enabled in advance. The system disables option 38 of DHCPv6 SNOOPING by default.

Example: Set the reforward policy of DHCPv6 packets with option 38 as keep for DHCPv6 SNOOPING.

Switch(Config)# ipv6 dhcp snooping subscriber-id policy keep

10.2.1.21 ipv6 dhcp snooping subscriber-id select delimiter

Command: ipv6 dhcp snooping subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD |)

no ipv6 dhcp snooping subscriber-id select delimiter

Function: Configure user configuration options to generate subscriber-id. The no form of this command restores to its original default configuration, i.e. vlan name together with port name.

Parameters: (**sp | sv | pv | spv**), a selection from combinations of slot, port and vlan, among which **sp** represents slot and port, **sv** represents slot and vlan, **pv** represents port and vlan, and **spv** represents slot, port and vlan.

WORD, the delimiter between slot, port and vlan which ranges among (#|.|,|;|:|/|space). Note that there're two delimiter WORDs here, of which the former is the delimiter between slot and port while the latter is that between port and vlan.

Default: Null.

Command Mode: Global configuration mode

Usage Guide: This command has no effect on ports with self-defined subscriber-id. If a user redefines subscriber-id of the port after configuring the command, the user-defined one prevails. This configuration is null by default.

Example:

Swithc(config)# ipv6 dhcp snooping subscriber-id select sv delimiter #

10.2.1.22 ipv6 dhcp use class

Command: ipv6 dhcp use class

no ipv6 dhcp use class

Function: This command enables DHCPv6 server to support DHCPv6 class during address assignment, the no operation of this command disables it without removing the relative DHCPv6 class information that has been configured.

Parameters: None.

Default: DHCPv6 server supports DHCPv6 class during address assignment.

Command Mode: Global configuration mode

Usage Guide: By default, DHCPv6 servers support DHCPv6 class during address assignment and the no form of this command doesn't remove DHCPv6 class information that has been configured. Make sure that DHCPv6 service has been enabled before using this command. DHCPv6 server supports DHCPv6 class during address assignment by default.

Example: Configure DHCPv6 server to support DHCPv6 class during address assignment.

Switch(Config)# ipv6 dhcp use class

10.2.1.23 remote-id subscriber-id

Command: {remote-id [*] <remote-id> [*] | subscriber-id [*] <subscriber-id> [*]}

no {remote-id [*] <remote-id> [*] | subscriber-id [*] < subscriber-id> [*]}

Function: This command configures option 37 and option 38 that match the class in IPv6 DHCP class configuration mode.

Parameters: <remote-id>, a string with a length ranging from 1 to 128 bytes is used to match remote-id in option 37.

<subscriber-id>, a string with a length ranging from 1 to 128 bytes is used to match subscriber-id in option 38.

[*****], match zero or more characters.

Default: None.

Command Mode: IPv6 DHCP Class configuration mode

Usage Guide: This command configures a mode which matches with the already-defined DHCPv6 class, and a DHCPv6 class may configure multiple commands. If this command is ignored and no mode configured in IPv6 DHCP Class mode, any remote-id or subscriber-id is considered to match with the DHCPv6 class, however, remote-id or subscriber-id must exist in DHCPv6 packet.

Example: Configure some remote-id or subscriber-id belonging to DHCPv6 class named CLASS1.

```
Switch(Config)# ipv6 dhcp class CLASS1
Switch(Dhcpv6-class)#remote-id abc* subscriber-id bcd*
Switch(Dhcpv6-class)#remote-id edf*
Switch(Dhcpv6-class)#subscriber *mmn
```

10.2.2 Commands for Monitoring and Debugging

10.2.2.1 debug ipv6 dhcp detail

Command: debug ipv6 dhcp detail

Function: Display the debug about detailed content of various packets sent and received by DHCPv6. If packets with option 37 and option 38, they will also be displayed. This command is applied in the server side as well as the relay side.

Parameters: None.

Command Mode: Admin mode

Usage Guide: Enable/disable the display of detailed debug about packets sent and received by DHCPv6.

Example:

```
Switch# debug ipv6 dhcp detail
%Jan 01 01:38:45 2006 DHCPv6 DETAILS: contents of SOLICIT packet
%Jan 01 01:38:45 2006       transaction-ID: 0x00b2d47c
%Jan 01 01:38:45 2006    elapsed time option(8), option-len 2
%Jan 01 01:38:45 2006       elapsed time: 0
%Jan 01 01:38:45 2006    client ID option(1), option-len 14
%Jan 01 01:38:45 2006       DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83
%Jan 01 01:38:45 2006    identity association option(3), option-len 12
%Jan 01 01:38:45 2006       IANA: 0x0e001d92, T1 0, T2 0
%Jan 01 01:38:45 2006    vendor class option(16), option-len 14
%Jan 01 01:38:45 2006       enterprise number : 311
%Jan 01 01:38:45 2006    option request option(6), option-len 6
%Jan 01 01:38:45 2006       requested-option: domain search list
%Jan 01 01:38:45 2006       requested-option: DNS server list
%Jan 01 01:38:45 2006       requested-option: vendor specific info
%Jan 01 01:38:45 2006    remote-id option(37), option-len 14
%Jan 01 01:38:45 2006       remote-id : 0x0a0b0c
%Jan 01 01:38:45 2006    subscriber-id option(38), option-len 16
%Jan 01 01:38:45 2006       subscriber-id : 0x0a0b0c0d
```

10.2.2.2 debug ipv6 dhcp relay packet

Command: debug ip dhcp relay packet

Function: Display the information of relay packet processing.

Parameters: None.

Command Mode: Admin mode

Usage Guide: This command is used to display the process of relay packet processed by relay agent together with the action information of option 37 and option 38.

Example:

Switch# debug ip dhcpv6 relay packet

%May 19 16:45:34 2010 DHCPv6 RELAY PACKET: received msg0 from <fe80::211:22ff:fe33:4455> on <Vlan8>

%May 19 16:45:34 2010 DHCPv6 RELAY PACKET: add subscriber-id option “Vlan8+Ethernet1/0/12”

10.2.2.3 debug ipv6 dhcp snooping packet

Command: debug ipv6 dhcp snooping packet

Function: Debug the packets of DHCPv6 SNOOPING. Corresponding information will also be displayed when adding or deleting option 37 and option 38.

Parameters: None.

Command Mode: Admin mode

Usage Guide: Enable/disable the information of DHCPv6 packets processed by DHCPv6 Snooping, including the type of received packet, source MAC and destination MAC, client DUID, i.e. the client identification, IA address, preferred lifetime, valid lifetime, and packet discard and so on.

Example:

switch#debug ipv6 dhcp snooping packet

dhcpv6 snooping packet debug is on

switch#%Jan 05 00:26:40 2006 DHCP6SNP EVENT: Parse packet SOLICIT from fe80::200:ff:fe00:1

src MAC 00-00-00-00-00-01 interface Ethernet1/0/23 vlan 24

%Jan 05 00:26:40 2006 DHCP6SNP PACKET: Receive DHCPv6 packet SOLICIT from fe80::200:ff:fe00:1

src MAC 00-00-00-00-00-01, dst MAC 33-33-00-01-00-02,

interface Ethernet1/0/23 vlan 24,

transaction-ID 6137412, smac host flag 0, dmac host flag 0

%Jan 05 00:26:40 2006 DHCP6SNP PACKET: Forward packet SOLICIT (protocol 0x37)

%Jan 05 00:26:40 2006 DHCP6SNP PACKET: to vlan 24 except port Ethernet1/0/23 (designPort flag 0)

%Jan 05 00:26:40 2006 DHCP6SNP PACKET: and return packet to network stack

switch#

10.2.2.4 show ipv6 dhcp relay option

Command: show ipv6 dhcp relay option

Function: Display the configuration of system relay agent, including the enable switch for option 37 and option 38.

Parameters: None.

Command Mode: Admin mode

Usage Guide: Use this command to check relay agents' configuration status for option 37 and option 38.

Example:

Switch#show ipv6 dhcp relay option
remote-id option enable
subscriber-id option enable
Interface Vlan 1: remote-id option configure "abc"

10.2.2.5 show ipv6 dhcp snooping option

Command: show ipv6 dhcp snooping option

Function: Display the configuration information of system snooping, including the enable switch for option 37 and option 38.

Parameters: None.

Command Mode: Admin mode

Usage Guide: Use this command to check snooping configuration status for option 37 and option 38.

Example:

Switch#show ipv6 dhcp snooping option
remote-id option enable
subscriber-id option enable
The slot port vlan select option is : port and vlan
The delimiter is : #

10.3 IPv6 Multicast Protocol

10.3.1 MLD Snooping

10.3.1.1 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.

Parameters: <1-4094> the specific VLAN ID; X:X::X:X the specific group address.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete all groups.

Switch#clear ipv6 mld snooping vlan 1 groups

Relative Command: show ipv6 mld snooping vlan <1-4094>

10.3.1.2 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.

Parameters: <1-4094> the specific VLAN ID; ethernet the Ethernet port name; IFNAME the port name.

Command Mode: Admin Configuration Mode

Usage Guide: Use show command to check the deleted group record.

Example: Delete the mrouter port in vlan 1.

Switch# clear ipv6 mld snooping vlan 1 mrouter-port

Relative Command: show ipv6 mld snooping mrouter-port

10.3.1.3 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.

10.3.1.4 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: MLD Snooping disabled on the switch by default

Usage Guide: Enable global MLD Snooping on the switch, namely allow every VLAN to be configured with MLD Snooping; the “no” form of this command will disable MLD Snooping on all

the VLANs as well as the global MLD snooping

Example: Enable MLD Snooping under global mode.

Switch (config)#ipv6 mld snooping

10.3.1.5 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

10.3.1.6 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

10.3.1.7 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

10.3.1.8 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

10.3.1.9 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 ethernet1/0/13

10.3.1.10 ipv6 mld snooping vlan mrouter-port learnpim6

Command: ipv6 mld snooping vlan <*vlan-id*> mrouter-port learnpim6

no ipv6 mld snooping vlan <*vlan-id*> mrouter-port learnpim6

Function: Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets), the no command will disable the function.

Parameter: <*vlan-id*>: The specified VLAN ID, ranging from 1 to 4094.

Command Mode: Global Mode

Default: Enable

Usage Guide: Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets). After a port received pimv6 packets, it will be set to mrouter port for implementing the automatic learning.

Example: Disable the function that vlan 100 learns mrouter-port (according to pimv6 packets).

Switch(config)#no ipv6 mld snooping vlan 100 mrouter-port learnpim6

10.3.1.11 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

10.3.1.12 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

10.3.1.13 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

10.3.1.14 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

10.3.1.15 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 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 1/0/1

10.3.1.16 ipv6 mld snooping vlan suppression-query-time

Command: ipv6 mld snooping vlan <*vlan-id*> suppression-query-time <*value*>

no ipv6 mld snooping vlan <*vlan-id*> suppression-query-time

Function: Configure the suppression query time; the "no" form of this command restores the default value.

Parameter: ***vlan-id*****:** VLAN ID, valid range: <1-4094>

value**:** valid range: <1-65535>secs.

Command Mode: Global Mode

Default: 255s

Usage Guide: This command can only be configured on L2 general querier. The Suppression-query-time represents the period the suppression state maintains when general querier receives queries from layer 3 MLD within the segment. To use this command, the query-intervals in different switches within the same segment must be in accordance. It is recommended to use the default value.

Example:

Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270

10.3.1.17 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)	Ethernet1/0/8	00:04:14	V2
	(2000::2)	Ethernet1/0/8	00:04:14	V2

Mld snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/0/2

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

time	status.
MLD Snooping Connect Group Membership	Group membership of the VLAN, namely the correspondence between the port and （S,G）.
Mld snooping vlan 1 mrouter port	Mrouter port of the VLAN, including both static and dynamic.

10.4 IPv6 Security RA

10.4.1 ipv6 security-ra enable

Command: ipv6 security-ra enable

no ipv6 security-ra enable

Function: Globally enable IPv6 security RA function, all the RA advertisement messages will not be forwarded through hardware, but only sent to CPU to handle. The no operation of this command will globally disable IPv6 security RA function.

Parameters: None.

Command Mode: Global Configuration Mode.

Default: The IPv6 security RA function is disabled by default.

Usage Guide: Only after enabling the global security RA function, the security RA on a port can be enabled. Globally disabling security RA will clear all the configured security RA ports. The global security RA function and the global IPv6 SAVI function are mutually exclusive, so they can not be enabled at the same time.

Example: Globally enable IPv6 security RA.

Switch(config)#ipv6 security-ra enable

10.4.2 ipv6 security-ra enable

Command: ipv6 security-ra enable

no ipv6 security-ra enable

Function: Enable IPv6 security RA on a port, causing this port not to forward the received RA message. The **no ipv6 security-ra enable** will disable the IPv6 security RA on a port.

Parameters: None.

Command Mode: Port Configuration Mode.

Default: IPv6 security RA function is disabled by default.

Usage Guide: Only after globally enabling the security RA function, can the security RA on a port be enabled. Globally disabling security RA will clear all the configured security RA ports.

Example: Enable IPv6 security RA on a port.

Switch(Config-If-Ethernet1/0/2)#ipv6 security-ra enable

10.4.3 show ipv6 security-ra

Command: show ipv6 security-ra [interface *<interface-list>*]

Function: Display all the interfaces with IPv6 RA function enabled.

Parameters: No parameter will display all distrust ports, entering a parameter will display the corresponding distrust port.

Command Mode: Admin and Configuration Mode.

Example:

Switch# show ipv6 security-ra

IPv6 security ra config and state information in the switch

Global IPv6 Security RA State: Enable

Ethernet1/0/1

IPv6 Security RA State: Yes

Ethernet1/0/3

IPv6 Security RA State: Yes

10.4.4 debug ipv6 security-ra

Command: debug ipv6 security-ra

no debug ipv6 security-ra

Function: Enable the debug information of IPv6 security RA; the no operation of this command will disable the debug information of IPv6 security RA.

Command Mode: Admin Mode.

Parameters: None.

Usage Guide: Users can check the proceeds of message handling of IPv6 security RA, which will help investigate the causes to problems if there is any.

Example: Enable the debug information of IPv6 security RA.

Switch#debug ipv security-ra

10.5 SAVI

10.5.1 Commands for SAVI

10.5.1.1 ipv6 cps prefix

Command: ipv6 cps prefix *<ipv6-address>* vlan *<vid>*

no ipv6 cps prefix<*ipv6-address*>

Function: Configure IPv6 address prefix of the link manually, no command deletes IPv6 address prefix.

Parameter: ipv6-address: the address prefix of link, like 2001::/64;

vid: vlan ID of the current link.

Command Mode: Global Mode.

Default: None.

Usage Guide: Users should configure local address prefix: fe80::/64 of the link before enable the function of matching address prefix of the link, it accepts the packets of which source addresses are the local addresses of the link.

Example: Configure the address prefix of the link to 2001::/64.

Switch(config)#ipv6 cps prefix 2001::/64

10.5.1.2 ipv6 cps prefix check enable

Command: ipv6 cps prefix check enable

no ipv6 cps prefix check enable

Function: Enable SAVI address prefix check function, no command will disable this function.

Parameter: None.

Command Mode: Global Mode.

Default: Disable SAVI address prefix check function.

Usage Guide: After enable the prefix check function, if the IPv6 address prefix of the packets does not accord with the link prefix, then do not establish the corresponding IPv6 address binding. If users enable the matched address prefix of the link, configure the local address prefix of fe80::/64 first to accept the packets with the source address as local link address. Disable address prefix check function by default.

Example: Enable SAVI address prefix check function.

Switch(config)#ipv6 cps prefix check enable

10.5.1.3 ipv6 dhcp snooping trust

Command: ipv6 dhcp snooping trust

no ipv6 dhcp snooping trust

Function: Configure the port as dhcpv6 trust port, it does not establish dynamic DHCPv6 binding again and allows all DHCPv6 protocol packets to pass; no command deletes the port trust function.

Parameter: None.

Command Mode: Port Mode.

Default: Disable.

Usage Guide: Set the port as dhcpv6 trust attribute, enable uplink port of the switch with SAVI function for connecting dhcpv6 server or dhcpv6 relay generally.

Example: Set ethernet1/0/1 to be DHCP trust port.

Switch(config)#interface ethernet1/0/1

Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust

10.5.1.4 ipv6 nd snooping trust

Command: ipv6 nd snooping trust

no ipv6 nd snooping trust

Function: Configure the port as slaac trust and RA trust port, this port will not establish dynamic slaac binding any more and forwards RA packets. The no command deletes the port trust function.

Parameter: None.

Command Mode: Port Mode.

Default: Disable port trust function.

Usage Guide: If the port disables ipv6 nd snooping trust function, it is considered to untrust RA packets port and discards all RA packets. Setting the port as trust attribute, enable the uplink port of the switch with SAVI or the conjoint port between switches with SAVI generally.

Example: Set the port ethernet1/0/1 to be nd trust port.

Switch(config)#interface ethernet1/0/1

Switch(config-if-etherne1/0/1)#ipv6 nd snooping trust

10.5.1.5 savi check binding

Command: savi check binding <*simple | probe*> mode

no savi check binding mode

Function: Configure the check mode for conflict binding, the no command deletes the check mode.

Parameter: simple mode: only check the port state for conflict binding, if the state is up, keep the conflict binding and do not set new binding. If the state is down, delete the conflict binding to set a new one

probe mode: besides checking the port state for conflict binding, it will send NS packets to probe the usability of the corresponding user when the port state is up. If receiving the responded NA packets from users, it will keep the current conflict binding and does not set new binding, otherwise delete the conflict binding to set new one.

Command Mode: Global Mode.

Default: Disable the conflict binding check mode by default. It will adopt the mode that delete the conflict binding directly to set new one.

Usage Guide: It is recommended to configure probe mode to prevent the attack that the spurious address conflict binding deletes the legal user binding.

Example: Configure the conflict binding check mode to probe mode.

Switch(config)#savi check binding probe mode

10.5.1.6 savi enable

Command: savi enable

no savi enable

Function: Enable the global SAVI function, the no command disables this global function.

Parameter: None.

Command Mode: Global Mode.

Default: Disable the global SAVI function.

Usage Guide: Command configuration can be processed for SAVI function after enabling the global SAVI function. Because SAVI function has already contained security RA function, global SAVI function and security RA function are mutually exclusive in the global mode.

Example: Enable SAVI function.

Switch(config)#savi enable

10.5.1.7 savi ipv6 binding num

Command: savi ipv6 binding num <*limit-num*>

no savi ipv6 binding num

Function: Configure the number of the corresponding binding with the port, no command restores the default value.

Parameter: limit-num: set the range from 0 to 65535, the default value of the port binding number is 65535.

Command Mode: Port Mode.

Default: 65535.

Usage Guide: The configured binding number only include the dynamic binding type of slaac, dhcp. If the binding sum exceeds the configured number, this port does not create new dynamic binding any more, if the configured number is 0, this port does not create any dynamic binding.

Example: Configure the binding number to be 100 for port ethernet1/0/1.

Switch(config)#interface ethernet1/0/1

Switch(config-if-ethernet1/0/1)# savi ipv6 binding num 100

10.5.1.8 savi ipv6 check source binding

Command: savi ipv6 check source binding ip <*ip-address*> mac <*mac-address*> interface <*if-name*> {type [slaac | dhcp] lifetime <*lifetime*> | type static}

no savi ipv6 check source binding ip <*ip-address*> interface <*if-name*>

Function: Configure the static or dynamic binding function manually; the no command deletes the configured binding.

Parameter: ip-address: is the unicast IPv6 address, including local link and global unicast address

mac-address: is the mac address of Ethernet

if-name: is the port name, like interface ethernet 1/0/1

slaac|dhcp: slaac means create the dynamic binding for slaac type, **dhcp** means create the dynamic binding for dhcp type

lifetime: configure the lifetime period for the dynamic binding, the unit is second.

static: create the binding of the static type.

Command Mode: Global Mode.

Default: None.

Usage Guide: After the dynamic binding configured by handwork is overtime, the corresponding binding will be deleted but the configuration is still be kept, so the binding still be shown. If the binding needs to take effect again, it should delete it first and configure a new binding again.

When the binding type is static type, do not configure lifetime period, the lifetime period is infinite.

Example: Configure the dynamic binding of slaac type for SAVI manually.

Switch(config)#savi ipv6 check source binding ip 2001::10 mac 00-25-64-BB-8F-04 Interface ethernet1/0/1 type slaac lifetime 2010

Configure the static binding for SAVI manually.

Switch(config)#savi ipv6 check source binding ip 2001::20 mac 00-25-64-BB-8F-04
Interface ethernet1/0/1 type static

10.5.1.9 savi ipv6 check source ip-address mac-address

Command: savi ipv6 check source [ip-address mac-address | ip-address | mac-address]
no savi ipv6 check source

Function: Enable the control authentication function for the packets of the port, no command disables this function.

Parameter: None.

Command Mode: Port Mode.

Default: Disable the control filtering function of the port.

Usage Guide: The global SAVI function must be enabled before configuring this command.

Example: Enable the control filtering function of the packets on port ethernet1/0/1.

Switch(config)#interface ethernet1/0/1
Switch(config-if-ethernet1/0/1)# savi ipv6 check source ip-address mac-address

10.5.1.10 savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Command: savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable
no savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Function: Enable SAVI application scene function, no command disables the function.

Parameter: dhcp-only: dhcp-only application scene
slaac-only: slaac-only application scene
dhcp-slaac: combination application scene of dhcp-only and slaac-only

Command Mode: Global Mode.

Default: Disable SAVI application scene.

Usage Guide: dhcp-only application scene only detects DHCPv6 packets and DAD NS packets of link-local ipv6 address to be IPv6 address with target field, it does not detect DAD NS packets of non-link-local address. slaac-only application scene detects DAD NS packets of all types. dhcp-slaac combination application scene detects all DHCPv6 and DAD NS packets. Disable all

kinds of application scene detection function for SAVI by default.

Example: Enable the specified dhcp-only application scene for SAVI.

Switch(config)#savi ipv6 dhcp-only enable

10.5.1.11 savi ipv6 mac-binding-limit

Command: savi ipv6 mac-binding-limit <*limit-num*>

no savi ipv6 mac-binding-limit

Function: Configure the dynamic binding number of the same MAC address, no command restores the default value.

Parameter: limit-num: set the ranging from 1 to 10, the default dynamic binding number is 32 for the same MAC address.

Command Mode: Global Mode.

Default: 32.

Usage Guide: This command is used to prevent the exhaust attack of the dynamic binding entry for SAVI.

Example: Set the dynamic binding number to be 5 for the same MAC address.

Switch(config)#isavi ipv6 mac-binding-limit 5

10.5.1.12 savi max-dad-dalay

Command: savi max-dad-delay <*max-dad-delay*>

no savi max-dad-delay

Function: Configure the dynamic binding at DETECTION state and send lifetime period of DAD NS packet detection, no command restores the default value.

Parameter: max-dad-delay: set the ranging between 1 and 65535 seconds, its default value is 1 second.

Command Mode: Port Mode.

Default: 1 second.

Usage Guide: It is recommended to use the default value.

Example: Set the detection lifetime as 2 seconds.

Switch(config)#savi max-dad-delay 2

10.5.1.13 savi max-dad-prepare-delay

Command: savi max-dad-prepare-delay <*max-dad-prepare-delay*>

no savi max-dad-prepare-delay

Function: Configure lifetime period of redetection for the dynamic binding, no command restores the default value.

Parameter: max-dad-prepare-delay: set the ranging between 1 and 65535 seconds, its default value is 1 second.

Command Mode: Global Mode.

Default: 1 second.

Usage Guide: It is recommended to user the default value.

Example: Set the redetection lifetime as 2 seconds.

Switch(config)#savi max-dad-prepare-delay 2

10.5.1.14 savi max-slaac-life

Command: savi max-slaac-life *<max-slaac-life>*

no savi max-slaac-life

Function: Configure lifetime period of slaac dynamic binding at BOUND state, no command restores the default value.

Parameter: max-slaac-life: set the ranging between 1 and 31536000 seconds, its default value is 4 hours.

Command Mode: Global Mode.

Default: 4 hours.

Usage Guide: None.

Example: Configure lifetime period of slaac binding type as 2010 seconds at BOUND state.

Switch(config)#savi max-slaac-life 2010

10.5.1.15 savi timeout bind-protect

Command: savi timeout bind-protect *<protect-time>*

no savi timeout bind-protect

Function: Configure the bind-protect lifetime period for a port after its state from up to down, no command restores the default value.

Parameter: protect-time: set the ranging between 1 and 300 seconds, its default value is 30 seconds.

Command Mode: Global Mode.

Default: 30 seconds.

Usage Guide: After the configured lifetime period is overtime, the port is still at down state, the binding of this port will be deleted. If the port state is changed from down to up state during the configured lifetime period, the binding of the port will reset it as lifetime period of BOUND state. If the configured parameter is 0 second, all binding of the port will be deleted immediately.

Example: Set bind-protect lifetime period to be 20 seconds.

Switch(config)#savi timeout bind-protect 20

10.5.2 Commands for Monitor and Debug

10.5.2.1 Monitor and Debugg

10.5.2.1.1 debug ipv6 dhcp snooping binding

Command: debug ipv6 dhcp snooping binding

no debug ipv6 dhcp snooping binding

Function: Enable binding debug of dhcp type for SAVI, no command disables the debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable this function, the relative binding of dhcp type or static type create the print information for misarranging. The no command disables this function.

Example: Enable the binding debug of dhcp type.

Switch#debug ipv6 dhcp snooping binding

10.5.2.1.2 debug ipv6 dhcp snooping event

Command: debug ipv6 dhcp snooping event

no debug ipv6 dhcp snooping event

Function: Enable event debug of dhcp type for SAVI, no command disables the debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable event debug, the relative event information of dhcp type will be print for misarranging. The no command disables this function.

Example: Enable binding event debug of dhcp type.

Switch#debug ipv6 dhcp snooping event

10.5.2.1.3 debug ipv6 dhcp snooping packet

Command: debug ipv6 dhcp snooping packet

no debug ipv6 dhcp snooping packet

Function: Enable the debug of DHCPv6 packets, no command disables the debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable packets debug, the relative DHCPv6 packtets will be print for misarranging. The no command disables this function.

Example: Enable the debug of DHCPv6 packets.

Switch#debug ipv6 dhcp snooping packet

10.5.2.1.4 debug ipv6 nd snooping binding

Command: debug ipv6 nd snooping binding

no debug ipv6 nd snooping binding

Function: Enable the binding debug of slaac type for SAVI, no command disables the binding debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable binding debug, the relative binding of slaac type will create the print information for misarranging. The no command disables this function.

Example: Enable binding debug of slaac type.

Switch#debug ipv6 nd snooping binding

10.5.2.1.5 debug ipv6 nd snooping event

Command: debug ipv6 nd snooping event

no debug ipv6 nd snooping event

Function: Enable the event debug of slaac type for SAVI, no command disables the event debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable event debug, the relative event information of slaac type will be print for misarranging. The no command disables this function.

Example: Enable the event debug of slaac type.

Switch#debug ipv6 nd snooping event

10.5.2.1.6 debug ipv6 nd snooping packet

Command: debug ipv6 nd snooping packet

no debug ipv6 nd snooping packet

Function: Enable ND packets debug, no command disables ND packets debug.

Parameter: None.

Command Mode: Admin Mode.

Default: None.

Usage Guide: After enable packets debug, the relative ND packets will be print for misarranging. The no command disables this function.

Example: Enable ND packets debug.

Switch#debug ipv6 nd snooping packet

10.5.2.1.7 show savi ipv6 check source binding

Command: show savi ipv6 check source binding [interface<*if-name*>]

Function: Show the global SAVI binding entry list.

Parameter: if-name: port name such as interface ethernet 1/0/1.

Command Mode: Admin Mode.

Default: None.

Usage Guide: Descriptions of each field are as below:

Field	Description
MAC	The bound MAC address
IP	The bound IP address

Vlan	The binding VLAN belongs to
Port	The binding port belongs to
Type	Binding type
State	Binding state
Expires	The bound lifetime period

Example: Show the global binding state of SAVI.

Switch(config)#show savi ipv6 check source binding

Static binding count: 0

Dynamic binding count: 3

Binding count: 3

MAC	IP	VLAN	Port	Type	State	Expires
00-25-64-bb-8f-04	fe80::225:64ff:febb:8f04	1	Ethernet1/0/5	slaac	BOUND	14370
00-25-64-bb-8f-04	2001::13	1	Ethernet1/0/5	slaac	BOUND	14370
00-25-64-bb-8f-04	2001::10	1	Ethernet1/0/5	slaac	BOUND	14370