3onedata

MES5200&MES5300-24GT4GS Series Layer 2 Industrial Ethernet Switch

CLI User Manual

Document Version: 01

Issue Date: 09/14/2023

Industrial Ethernet Communication Solution Expert **3onedata Co., Ltd.**

Trademark Statement

3onedata, 3onedata and 3One data are the registered trademarks owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Note

Purchased product, service or features should be constrained by 3onedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document is only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.

3onedata

3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen, 518108 China
Technology support:	support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86 0755-2670-3485
Website:	http://www.3onedata.com

Preface

Switch CLI user manual has introduced:

- CLI configuration interface login
- CLI configuration rule and method
- Introduction of command lines related to various network management functions

Audience

This manual applies to the following engineers:

- Network administrators responsible for network configuration and maintenance
- On-site technical support and maintenance personnel
- Network engineers

Text Format Convention

Format	Note
" "	Words with “” represent the interface words. Fox example: “Port number”.
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: ‘Light Blue’.
About this chapter	The section ‘about this chapter’ provides links to various sections of this chapter, as well as links to the Principles/Operations Section of this chapter.

Icon Convention

Format	Note
 Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.

Format	Note
 Notes	Make a necessary supplementary instruction for operation description.
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Port Convention

The port number in this manual is only an example, and does not represent the actual port with this number on the device. In actual use, the port number existing on the device shall prevail.

Revision Record

Version No.	Revision Date	Revision Note
01	2023-08-31	Product release

Contents

1 Login the Switch Configuration

1.1 Login the Switch Function Overview

There are two ways for users to manage devices: CLI and WEB.

- CLI
  After logging into the device through the Console port, Telnet, or SSH, use the command line provided by the device to manage and configure the device. This approach requires configuring the user interface for the corresponding login mode.
- WEB
  When the device acts as a server, users can log in to the device through the WEB administration. The device provides a graphical interface with the built-in WEB server to facilitate users to manage and maintain the device intuitively and conveniently. This method can only realize the management and maintenance part of functions of the device. If more complex or fine management of the device is needed, the CLI method is still needed.

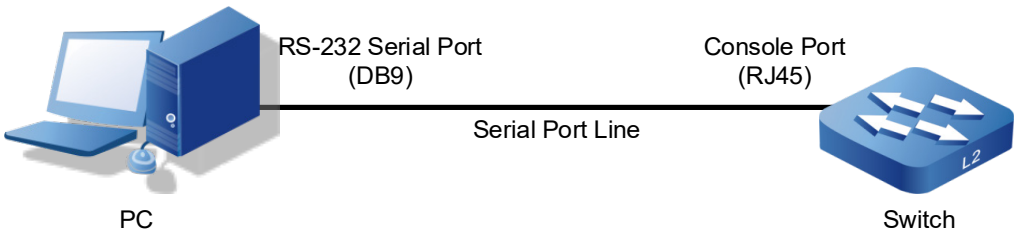
1.2 Login to the Switch

1.2.1 Login to the Switch via Serial Port

Logging in through the Console port is the basic way to log in a device, and is the basis for configuring a device logged in through other means. By default, users can log into the device directly through the serial port, and the switch baud rate is 115200bit/s. The PC can log in to the command line interface of the device by connecting to the Console port.

Operation steps

Step 1 Connect the serial port of the computer to the Console port of the device through the serial port line to establish a local configuration environment, as shown in the topology diagram below.

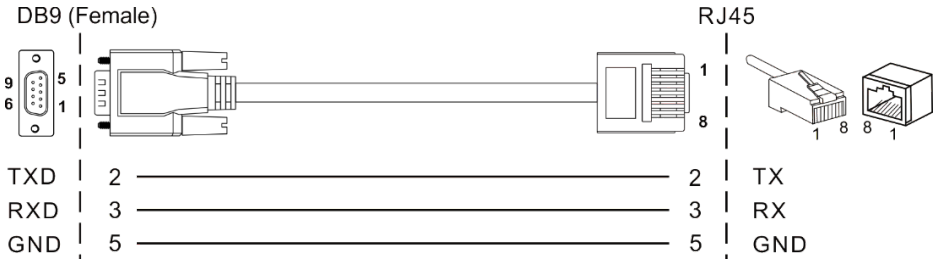


1 Connect DB9 at one end of serial port line to RS-232 serial port of PC.

2 Connect the RJ45 on the other end of the serial line to the Console port of the device.

Note:

Diagram of internal connection line of serial port line/communication cable is shown below.

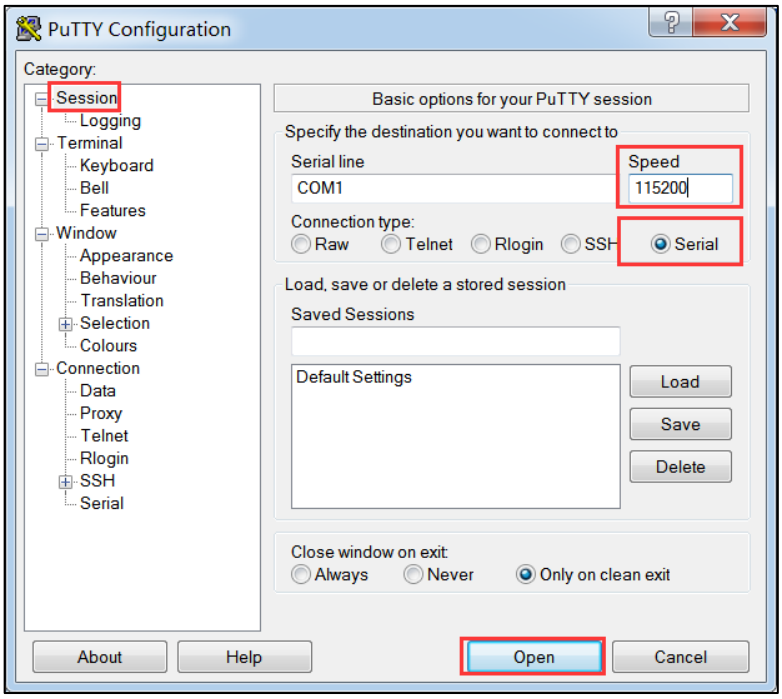


Step 2 Open the terminal simulation software on the PC, create a new connection, and set the interface and communication parameters of the connection. (Using PuTTY as an example here.)

1 Open PuTTY and click “Session” on the menu bar.

2 In the "Basic options for your PuTTY session" input box on the right, do the following:

- Select "Connection type" to "Serial".
- Enter "115200" in the "Speed" text box;
- Click “Open”.



3 The "COM1-PuTTY" command line edit dialog box pops up. Press enter key to enter user name and password. The user name and password is “admin123”, as shown in the following figure.

Step 3 End.

1.2.2 Login to the Switch via Telnet

Log into the switch by Telnet, and the device acts as Telnet-Server By default, the Telnet-Server function is enabled. Therefore, before using Telnet to log into the switch, it is necessary to configure the IP of the switch through serial port to ensure the normal communication between PC and DUT.

Telnet-Server Configuration

Operation	Command	Remark
Enter Configure Mode	**configure terminal**	-
Enable Telnet Server	**telnet-server enable**	Optional

Disable Telnet Server	`no telnet-server enable`	Optional

Notice

DUT acts as a Telnet server, if the logged client does not do any operation for a long time, it will automatically disconnect, i.e. timeout exit, and the function is enabled by default with 30m.

Through Telnet client login to the command line interface of the device, the client and the device should meet the following requires:

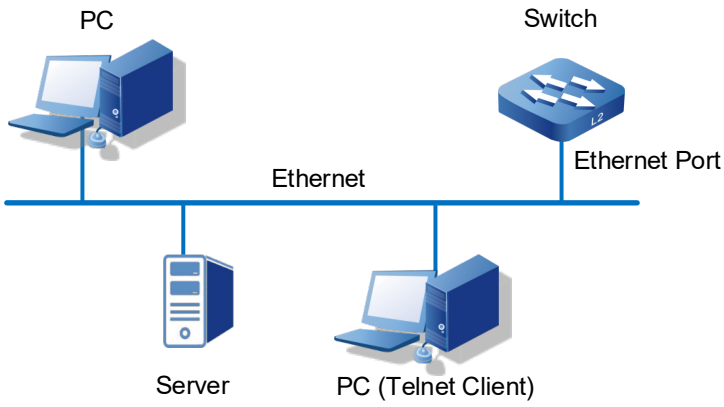
1 Configure the IP address of the switch correctly.

2 If the Telnet client and the device are in the same LAN, the IP address of the device and the client must be configured in the same network segment. Otherwise, the route between Telnet client and device must be accessible.

User can log in to the switch device through the Telnet client and configure the device if the two requires above are met.

Operation Steps

Step 1 As shown in the figure below, set up the configuration environment to connect the Ethernet port of the computer to the Ethernet port of the device through the LAN.

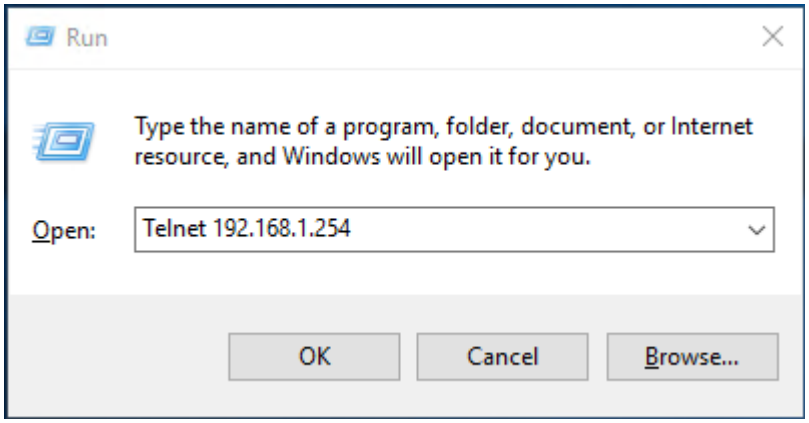


1 Run the Telnet client on the computer and input the administrative IP address of the Ethernet port connected the computer to the switch, as shown in the figure below.

2 Press "Win+R" to pop up the running window;

3 Enter “Telnet+ space + device IP address” in the “Open (O)” input box.

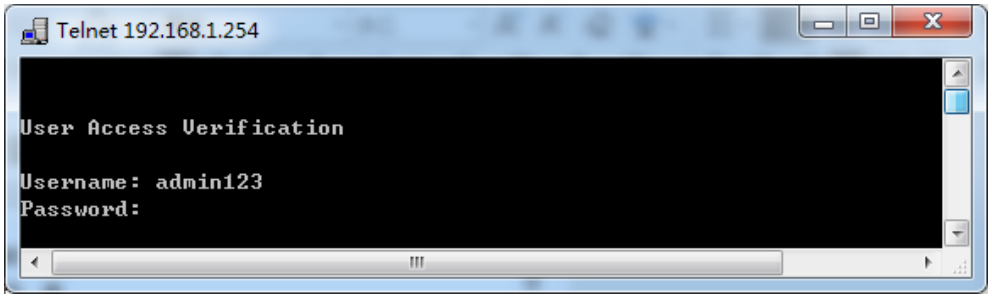
4 Click "OK” button.



Notes:

- Using the command line prompt interface of Win7/Win8/Win10 and other operating systems to configure the device needs to enable Telnet client in advance, user can check and enable Telnet client in the Windows function window under the path of "Control Panel > Program and Function > Enable or Disable Windows function", if Telnet client has been enabled, user can ignore this instruction.
- If the computer operating system does not support Telnet clients, a third party software PuTTY can be used as a Telnet client.
- The default IP address of the device is “192.168.1.254”.

Step 2 The "Telnet" dialog box pops up and user can enter user name and password according to the hint. The user name and password is “admin123”, as shown in the following figure.



Step 3 End.

1.2.3 Login to the Switch via SSH

The switch can be used as an SSH server, but can not be used as an SSH client.

By default, the SSH server function of the device is disabled. Therefore, before using SSH to log in to the device, it is necessary to log in to the device through the Console port first, and enable the SSH server function and other properties of the device for corresponding configuration, so as to ensure normal login to the device through SSH.

SSH Configuration

Operation	Command	Remark
Enter Configure Mode	**configure terminal**	-
Enable SSH server	**ssh-server enable**	Optional
Disable SSH server	**no ssh-server enable**	Optional

Notice

If using ssh login to DUT is needed, the simplest operations are:

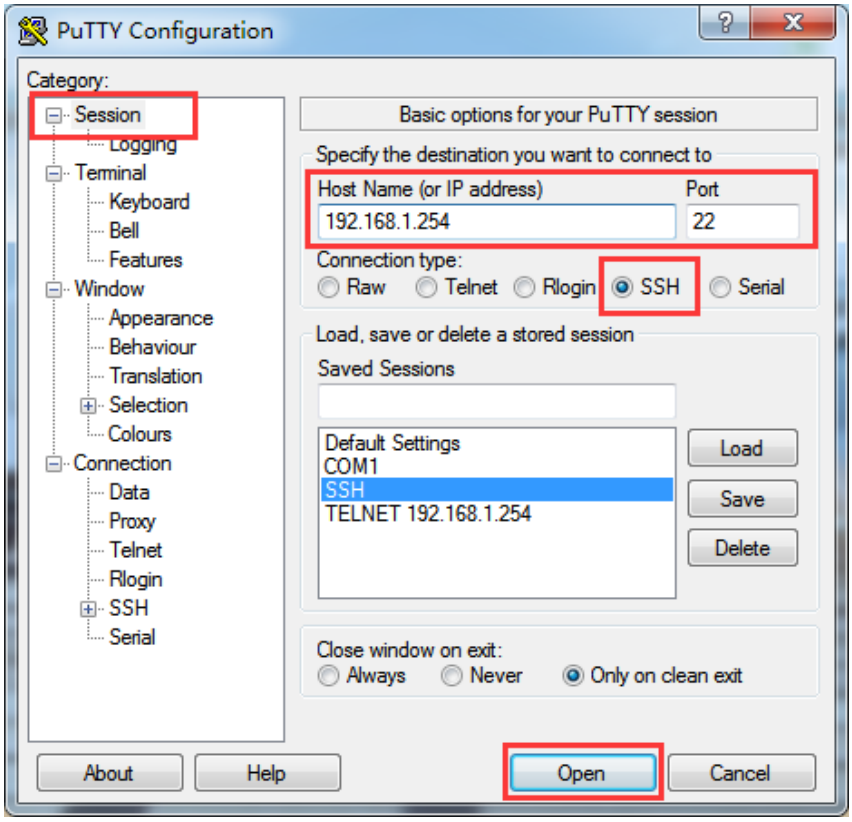
- Enable SSH;
- Configure SSH users, that is device users;
- Login the device

Operation Steps

Step 1 Using the Console port, enable SSH service using the "ssh-server enable" command.

```
switch> enable
switch# configure terminal
switch(config)# ssh-server enable
```

Step 2 Run the third-party PuTTY software on the PC host as an SSH client to establish a secure connection with the device, and fill in the following parameters:



1 Click “Session” in the “Category” bar;

2 Choose “SSH” in the “Connection type”;

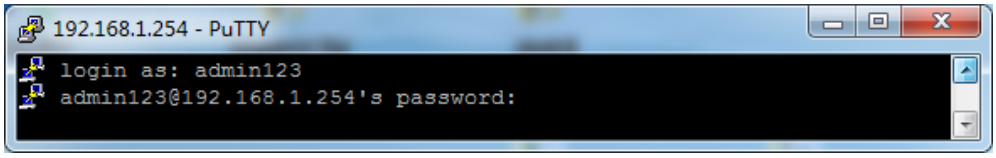
3 Enter the IP address "192.168.1.254" of the device in the "Host Name (or IP address)" text box.

4 “Port” port number defaults to 22.

5 (Optional) enter the session name in the "Saved Sessions", such as SSH; click "Save" to save the session;

6 Click "Open" button to enter the SSH configuration interface;

7 Enter the user account name of this device in the SSH client, such as the default user name and password is "admin123";



Note:

With SSH enabled, all users on the device support SSH encrypted login.

8 Access to the device through SSH is successful, end.

Step 3 End.

1.2.4 Login to the Switch via WEB

User can Login to the Switch via WEB.

By default, the switch is enabled as an HTTP server function. Before logging into the WEB, user needs to ensure that the client has a browser and corresponding IP address to ensure normal communication between the client and the HTTP server.

WEB Log in Configuration

Operation	Command	Remark
Enter global mode	**configure terminal**	Required
Enable HTTP server	**http-server enable**	Optional
Disable HTTP server	**no http-server enable**	Optional

Configuration Environment Requirements

Client requirements: IE browser 8.0 above, some versions of 360 browser may have problems, other browsers have not found any problem at present.

Login WEB Management Platform

The user enter http://X.X.X.X directly in the browser (default switch management IP is 192.168.1.254), press Enter key to enter the switch login interface, enter user name

and password and click login to enter the main interface.http://x.x.x.x/ The default user name and password of the device is “admin123”.

1.2.5 Manage the Switch via Network Management Software

The switch supports login management via network management software. By default, SNMP function is enabled, and can use the default community name. This only shows that the switch can be managed by SNMP. Please refer to the SNMP user manual for more detailed configuration.

SNMP login configuration

Operation	Command	Remark
Enter global mode	**configure terminal**	Required
Enable SNMP server	**snmp-server**	Required
Disable SNMP server	**no snmp-server**	Optional

1.3 Command Line

1.3.1 Command Analysis

Command consists of two parts: command word and command parameter. Commands are all lowercase, input is case-insensitive; command words come in many forms, including: capital letters, (), <>, *, etc.

For example: IP address A.B.C.D/M (secondary|), IP and address are command words, and A.B.C.D/M and (secondary|) are command parameters.

1.3.2 Command Line Mode

Here are four major command-line patterns:

- Exec Mode: it is also called "View Mode", a basic mode to enter the CLI. The prompt is ">", and only some simple commands can be executed, such as: show, enable, logout, etc. Users logged in with priority 0 are taken as reference users to enter the CLI exec mode, while users logged in with other priorities enter the CLI privileged mode. The "enable" command is used to elevate user privileges. Log in through the console port, and execute "enable" to enhance the user

authority; Through Telnet, ssh and other login methods, you need to configure the enable password to enhance the privilege.

- Privileged Exec Mode: also known as "Enable Mode" with the prompt of "#", in Exec Mode, entered by executing enable command, or switched from other modes. Basic commands such as: debug, show, reboot, copy can be executed.
- Configure Mode: also known as "Configure Terminal", the prompt is "(config)#". User can execute the configure terminal to enter this mode in Privileged Exec mode, or switch to this mode from another mode, and all Configure Mode commands can be executed.
- Interface Mode: prompt is "(config-IFNAME)#". User can enter "Interface IFNAME" in ConfigurE Mode or switch to this Mode from another mode. Configuration command for the specified Interface can be executed.

1.3.3 Shortcut Key

Only the commonly used command parameters are covered here.

Shortcut Key	Note
?	Help command, enter"?" to display Command help.
Tab	Command completion, "Tab" can prompt or complete the remaining characters to be input when typing part of the command word.
Ctrl+D	To exit the current mode, can exit to the upper level mode in any mode, such as Interface Mode to Configure Mode.
Ctrl+C	End up command input or execution. Or directly return to "Enable Mode".
Ctrl+W	Delete an input command word or delete an input command parameter.
Ctrl+U	Delete all characters from the current input command line.

【Instance】

"?" Help command. When using the command line, type“? ” to display the command help. Cases are as follows:

9 Type only "? "in a configuration mode, a list of all commands in the current mode will be displayed.

```
Switch#?
Exec commands:
  clear      Reset functions
  clock      Config clock time
```

```
  configure   Enter configuration mode
  copy        Copy file
  debug       Debugging functions (see also 'undebug')
  disable     Turn off privileged mode command
  enable      Turn on privileged mode command
  erase       erase file
  exit        End current mode and down to previous mode
  faults      Fault management command
  help        Description of the interactive help system
  logout      Exit from the EXEC
  loopback    config l2 interface loopback
  mstat       Show statistics after multiple multicast traceroutes
  mtrace      Trace multicast path from source to destination
  no          Negate a command or set its defaults
  ping        Send echo messages
  quit        Exit current mode and down to previous mode
  reboot      Halt and perform a cold restart
  rm          erase file
  show        Show running system information
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
  undebug     Disable debugging functions (see also 'debug')
  write         Write running configuration to memory, file or
terminal
```

10 All commands matching the current command word are displayed when partial command words are entered.

```
Switch#c?
  clear     Reset functions
  clock     Config clock time
  configure  Enter configuration mode
  copy      Copy file
```

1.4 Common Command

1.4.1 Password Verification

The configuration process for enabling password verification:

```
Switch>enable
Switch#configure terminal
Switch(config)#username admin password admin
```

```
Switch(config)#line vty 0
Switch(config-line_0)#login local
Disable password verification:
Switch(config-line_0)#no login local
```

1.4.2 Customization Display

Currently, there are four ways: exclude, include, grep and redirect:

- Exclude: only shows rows that do not contain the current string;
- Include: only displays the line that contains the current string;
- Grep: displays only the rows that conform to the current rule;
- Redirect: Redirect input to a system file.

Instance 1: show interface brief all

```
Switch#show interface brief all
Interface       IP-Address      Link    Protocol
lo              127.0.0.1       up      up
vlanif1         192.168.1.254   up      up

Interface       Link    Speed   Duplex  Type    PVID Description
ge1             down    auto    auto    access  1
ge2             down    auto    auto    access  1
ge3             down    auto    auto    access  1
ge4             down    auto    auto    access  1
ge5             down    auto    auto    access  1
ge6             down    auto    auto    access  1
ge7             down    auto    auto    access  1
ge8             down    auto    auto    access  1
ge9             down    auto    auto    access  1
ge10            down    auto    auto    access  1
ge11            down    auto    auto    access  1
ge12            down    auto    auto    access  1
ge13            down    auto    auto    access  1
ge14            down    auto    auto    access  1
ge15            down    auto    auto    access  1
ge16            down    auto    auto    access  1
ge17            down    auto    auto    access  1
ge18            down    auto    auto    access  1
ge19            down    auto    auto    access  1
ge20            down    auto    auto    access  1
ge21            down    auto    auto    access  1
```

```
ge22            up      100m(a) full(a) access  1
ge23            down    auto    auto    access  1
ge24            down    auto    auto    access  1
xe1             down    10g(a)  full(a) access  1
xe2             down    10g(a)  full(a) access  1
xe3             down    10g(a)  full(a) access  1
xe4             down    10g(a)  full(a) access  1
```

Instance 2: show interface brief all | exclude ge Does not show interfaces containing ge

```
Switch#show interface brief all | exclude ge
Interface       IP-Address      Link    Protocol
lo              127.0.0.1       up      up
vlanif1         192.168.1.254   up      up

Interface       Link    Speed   Duplex  Type    PVID Description
xe1             down    10g(a)  full(a) access  1
xe2             down    10g(a)  full(a) access  1
xe3             down    10g(a)  full(a) access  1
xe4             down    10g(a)  full(a) access  1
```

Instance 3: show interface brief all | include ge Only show interfaces containing ge

```
Switch#show interface brief all | include ge
ge1             down    auto    auto    access  1
ge2             down    auto    auto    access  1
ge3             down    auto    auto    access  1
ge4             down    auto    auto    access  1
ge5             down    auto    auto    access  1
ge6             down    auto    auto    access  1
ge7             down    auto    auto    access  1
ge8             down    auto    auto    access  1
ge9             down    auto    auto    access  1
ge10            down    auto    auto    access  1
ge11            down    auto    auto    access  1
ge12            down    auto    auto    access  1
ge13            down    auto    auto    access  1
ge14            down    auto    auto    access  1
ge15            down    auto    auto    access  1
ge16            down    auto    auto    access  1
ge17            down    auto    auto    access  1
ge18            down    auto    auto    access  1
ge19            down    auto    auto    access  1
```

```
ge20            down     auto    auto    access  1
ge21            down     auto    auto    access  1
ge22            up       100m(a) full(a) access  1
ge23            down     auto    auto    access  1
ge24            down     auto    auto    access  1
```

Instance 4: show interface brief all | grep ge*1 Show interfaces containing ge*1

```
Switch#show interface brief all | grep ge*1
ge1             down     auto    auto    access  1
ge10            down     auto    auto    access  1
ge11            down     auto    auto    access  1
ge12            down     auto    auto    access  1
ge13            down     auto    auto    access  1
ge14            down     auto    auto    access  1
ge15            down     auto    auto    access  1
ge16            down     auto    auto    access  1
ge17            down     auto    auto    access  1
ge18            down     auto    auto    access  1
ge19            down     auto    auto    access  1
```

Instance 5: show interface brief all | grep down Only show down interfaces

```
Switch#show interface brief all | grep down
ge1             down     auto    auto    access  1
ge2             down     auto    auto    access  1
ge3             down     auto    auto    access  1
ge4             down     auto    auto    access  1
ge5             down     auto    auto    access  1
ge6             down     auto    auto    access  1
ge7             down     auto    auto    access  1
ge8             down     auto    auto    access  1
ge9             down     auto    auto    access  1
ge10            down     auto    auto    access  1
ge11            down     auto    auto    access  1
ge12            down     auto    auto    access  1
ge13            down     auto    auto    access  1
ge14            down     auto    auto    access  1
ge15            down     auto    auto    access  1
ge16            down     auto    auto    access  1
ge17            down     auto    auto    access  1
ge18            down     auto    auto    access  1
ge19            down     auto    auto    access  1
```

```
ge20            down     auto    auto    access  1
ge21            down     auto    auto    access  1
ge23            down     auto    auto    access  1
ge24            down     auto    auto    access  1
xe1             down     10g(a)  full(a) access  1
xe2             down     10g(a)  full(a) access  1
xe3             down     10g(a)  full(a) access  1
xe4             down     10g(a)  full(a) access  1
```

1.4.3 Configuration Management

Command	Note
Switch#**show running-config**	Displays the configuration of the current system running
Switch#**show startup-config**	Displays the configuration of the system startup profile
Switch#**write**	Save command
Switch#**erase startup-config**	Restore factory settings
Switch#**copy tftp startup-config** 192.168.1.168 **Switch.conf**	Upload configuration file to switch
Switch#**copy flash startup-config** 192.168.1.168 **Switch.conf**	Download Configuration file from switch

Notice

If the configuration of the current system is inconsistent with the configuration of the system startup configuration file:

- After entering Configure Mode, the prompt is "*Switch";
- When performing a system reboot, it will prompt whether to save data or not.

1.4.4 System Upgrade

Suppose the upgrade package is "packetapp.bin", the IP address of the TFTP server is "192.168.1.168", and the command to upgrade the switch system is:

```
Switch#copy tftp package 192.168.1.168 packetapp.bin
```

Notes

The system upgrade must restart the switch to take effect.

The command to restart the system is: Switch#reboot.

After executing the restart, the screen will display as follows:

```
*Switch#reboot
save running config? (y/n): y
Building configuration...
[OK]
reboot system? (y/n): y
```

1.4.5 Debug Mode

1. Enter the debugging state of function module.

```
*Switch#debug ospf packet /*Enable receiving packet debug of ospf*/
*Switch(config)#log stdout /*Log output to serial port*/
2. Print message information:
Switch # debug PKT-filter tx/rx icmp     Enable the information
printing of received icmp messages or sent icmp messages.
Switch # no debug PKT-filter tx/rx icmp   Disable the information
printing of received icmp messages or sent icmp messages.
3. Check the detailed information such as the number of sending
and receiving packets of various messages:
Switch#show pkt-filter
```

1.4.6 Enable Modbus TCP

Enable Modbus TCP:

Operation	Command	Note
Enable Modbus TCP	**modbus-server** {enable|disable}	{enable| disable} • enable • disable

Configuration Instance

Enable the Modbus TCP function:

Switch(config)#modbus-server enable

Switch(config)#

2 User Configuration

2.1 Add User

【Command】

```
username WORD
username WORD password (8|) LINE
username WORD privilege <0-15>
username WORD privilege <0-15> password (8|) LINE
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

WORD: a user name, limited to 16 characters. And it cannot be numbers, characters, and characters other than @ # ￥%.

(8|) : 8 means password encryption. This function will only take effect when global encryption is turned on.

LINE: password, limited to 8 characters. And it cannot be numbers, characters, and characters other than @ # ￥%.

<0-15>: a total of 16 user privilege priorities, divided into four categories:

- 0: visit level; user can only view device version information and some simple configuration information.
- 1: view level; The configuration information of the device can be viewed, but the configuration of the device cannot be modified.
- 2: configuration level; User can view the configuration information of the device and configure some functional parameters of the device, but cannot manage the

device.

- 3-15: manage level, user has all privileges of the device, including downloading, uploading, rebooting, modifying device information and other operations.

【Description】

username WORD: this command adds a user name that has no password and priority defaults to 1.

Username WORD password (8|) LINE: this command can add or change passwords to users that have already been created, or add users with passwords.

username WORD privilege <015> : this command has setting permission of the user and the default priority for all new users is 15.

Username WORD privilege <015> password (8|) LINE: this command can create a new user, specify priority, and specify password.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#username admin123 privilege 15 password admin123
```

2.2 Delete User

【Command】

```
no username WORD
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

WORD: a user name, limited to 16 characters.

【Description】

Delete specified user

【Instance】

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#no username admin123
```

Notice

Deleted user names cannot be logged into the device, and when all user names have been deleted, the device only can be logged in through the Console port.

2.3 View Current Online Users

【Command】

show users

show logined users

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

None

【Description】

show logined users: view current online users

show users: view current users with lower priority.

【Instance】

```
Switch> enable
Switch#show Logined users
Line     User     Type    Idle     Host(s)    Uptimes      Location
 0     admin123  console   0                  01:36:08     console
```

2.4 Console Login Management

The Console user interface is used to manage and monitor users logging in through the Console port. The device provides a RJ45 type Console port of RS-232 serial port.

The terminal serial port of the user can connect directly with the device Console port to achieve local access to the device.

【Command】

```
line console <0-0>
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<0-0> : parameter "0", local Console configuration, supporting only one user.

【Description】

Line console <0-0> enters the Console user interface configuration view. The Console user interface can configure connection timeout, password validation, priority, and history command buffer sizes.

【Instance】

```
*Switch#configure terminal
*Switch(config)#line console 0
*Switch(config-console_0)#
```

2.5 Virtual Terminal Login Management

The VTY (Virtual Type Terminal) user interface is used to manage and monitor users logging in through VTY. After the user establishes a Telnet or SSH connection with the device through the terminal, a VTY channel is established. Currently each device supports up to 16 simultaneous VTY users. There is no fixed relationship between user interface and user. The user interface is assigned differently when the same user logs in different ways. Different user interfaces may be assigned for different login times for the same user.

【Command】

```
line vty <0-15>
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<0-15> : VTY user channel 0-15, supports 16 VTY users to access the device simultaneously.

【Description】

line vty <0-15>: enters the VTY user interface configuration view. The VTY user interface can configure connection timeout, password validation, priority, and history command buffer sizes.

【Instance】

```
*Switch#configure terminal
*Switch(config)#line vty 0
*Switch(config-vty_0)#
```

2.6 Timeout Logout

【Command】

exec-timeout <0-35791> <10-2147483>

【View】

Console/ VTY user interface configuration mode

【Default Level】

2: Configuration level

【Parameter】

<0-35791> : timeout minutes range.

<10-2147483> : timeout seconds range.

【Description】

exec-timeout <0-35791> <10-2147483> : this command disconnects idle connections within a set time. If the connection is always idle during the set time, the system will automatically disconnect the connection. By default, the timeout of user interface disconnection is 10 minutes.

【Instance】

The system is configured with a 10-minute timeout by default. If the user is configured with password authentication, the user needs to enter the username and password again after the timeout to enter the system.

Configuration process for modifying the timeout logout:

```
Switch>enable
Switch#configure terminal
Switch(config)#line vty 0
Switch(config-vty_0)#exec-timeout 0 600
```

3 Port Configuration

3.1 Enter Port Configuration Mode

【Command】

```
interface IFNAME
interface ge <1-24>
interface loopback <0-1>
interface po <1-12>
interface range (ge | xe)
interface sa <1-12>
interface vlanif <1-4094>
interface xe <1-4>
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

IFNAME: port name

ge: Gigabit port name.

loopback: loopback port name

po: dynamic aggregation group name.

range: supports range type port input. For example, interface range ge 1-10 is denoted as going into Gigabit port 1-10. Only Gigabit ports and 10 Gigabit ports are currently supported.

sa: static aggregation group name

vlanif : layer 3 interface

xe: 10 Gigabit port.

【Description】

This command is the mode navigation command that goes from Configure Mode to interface configuration mode. The next step is to modify the configuration of the corresponding interface.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface range ge 1-10
Switch(config-ge1-10)#
Enter 10 ports from ge1 to ge10.
```

3.2 Port Rate Limit

【Command】

bandwidth <64-10000000>

no bandwidth

【View】

fe (100M Ethernet) port view

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

sa (static aggregation group) port view

po (dynamic aggregation group) port view

【Default Level】

2: Configuration level

【Parameter】

<64-10000000> : the unit is kbps. For different ports, there are some restrictions on the parameters. The allowed input range of normal Gigabit ports is 64-1000000, and the allowed input range of 10 Gigabit ports is 64-10000000. If the input parameter is not in the specified range, the setting will not be successful and an error will be returned.

【Description】

bandwidth: this command does not actually affect the bandwidth of an interface, but simply allows the user to inform the system the bandwidth standard of that interface. By default, the bandwidth of an Ethernet interface is determined by the rate of the actual port connection, and can be manually configured if necessary. The bandwidth is only a routing parameter and does not affect the real bandwidth of the interface of the physical link.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#bandwidth 128
```

3.3 Port Settings

3.3.1 Duplex Mode

【Command】

```
duplex ( auto | full | half )
no duplex
```

【View】

fe (100M Ethernet) port view

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

【Default Level】

2: Configuration level

【Parameter】

Auto: full duplex and half duplex self-adaption.

full: represents full duplex.

half: represents half duplex.

【Description】

duplex (auto | full | half) : this command is used to set the duplex mode of the port.

By default, duplex mode of all ports is auto.

When setting the normal port rate to Gigabit, the duplex mode of the port cannot be set to half-duplex. When setting 10 Gigabit fiber ports, the duplex mode of the port cannot be set to half duplex. Otherwise the setting will not take effect and an error will be returned.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#duplex full
```

3.3.2 Flow Control

【Command】

```
flowcontrol (both| receive | send)
flowcontrol send (on | off)
flowcontrol receive (on | off)
no flowcontrol
```

【View】

fe (100M Ethernet) port view

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

sa (static aggregation group) port view

po (dynamic aggregation group) port view

【Default Level】

2: Configuration level

【Parameter】

both: Data transmit and receive of the port are set to self-negotiate flow control.

receive (on | off) : only enable or disable flow control on data receiving of the ports.

send (on | off) : only enable or disable flow control on data transmission of the ports.

【Description】

flowcontrol: this command is used to enable or disable flow control of the ports.

By default, flow control on all ports is disabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#flowcontrol both
```

3.3.3 Max-Frame

【Command】

mtu <64-16360>

no mtu

【View】

fe (100M Ethernet) port view

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

sa (static aggregation group) port view

po (dynamic aggregation group) port view

vlanif (layer 3) port view

【Default Level】

2: Configuration level

【Parameter】

<64-16360> : the allowed setting range of mtu is 64-16360.

<128-1500> : the allowed setting range of mtu in a layer 3 interface is 128-1500.

【Description】

mtu: this command is used to set the maximum data frame length supported by the interface, that is, the maximum length of the data portion of the link.

By default, the maximum data frame length for all physical ports is set to 1518. The MTU for the virtual port, such as vlanif1, is set to 1500.

Notes

When setting up virtual ports such as vlanif1, the maximum MTU value allowed is 1500.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#mtu 1800
```

3.3.4 Interface Switch

【Command】

shutdown

no shutdown

【View】

fe (100M Ethernet) port view

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

sa (static aggregation group) port view

po (dynamic aggregation group) port view

vlanif (layer 3) port view

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

shutdown: for interfaces (Ethernet ports, converged ports, and switched virtual interfaces), the command is primarily to close the corresponding interface, but other configurations of the interface still exist, just do not work. no shutdown is to open the port.

By default, the administrative state of the interface is UP.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface sa1
Switch(config-sa1)#shutdown
```

3.3.5 Rate

【Command】

```
speed (auto | 10m | 100m | 1g | 10g)
speed (auto | 1g | 10g)
speed (auto | 10m | 100m | 1g )
no speed
```

【View】

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

sa (static aggregation group) port view

po (dynamic aggregation group) port view

【Default Level】

2: Configuration level

【Parameter】

auto: Indicates that the rate of the interface is self-adaptive.

10m: set the interface rate to 10Mbps.

100m: set the interface rate to 100Mbps.

1g: set the interface rate to 1Gbps.

10g: set the interface rate to 10Gbps.

(auto|10m|100m|1g|10g): port rate configuration of dynamic and static aggregation groups.

(auto|1g|10g): 10 Gigabit port speed configuration

(Auto|10m|100m|1g): Gigabit port speed configuration.

【Description】

speed: this command is used to set the rate of the port.

By default, the rate of the interface is self-adaptive (auto). The port rate cannot be set to 1g or above when setting the normal port duplex mode to half. The port rate is set to a minimum of 1g, when setting a 10 Gigabit fiber port.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
```

```
Switch(config-ge8)#speed 100m
```

3.4 Port Isolation

【Command】

port-isolate enable group <1-8>

no port-isolate enable

【View】

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

sa (static aggregation group) port view

po (dynamic aggregation group) port view

【Default Level】

2: Configuration level

【Parameter】

<1-8>: isolation group ID

【Description】

port-isolate: this command is used to add the current Ethernet ports to the isolation group.

no port-isolate： This command is used to remove the current Ethernet ports from the isolation group.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#port-isolate enable group 1
Switch(config-ge8)#no port-isolate enable
```

3.5 Storm Suppression

【Command】

storm-control (broadcast | dlf | multicast) level LEVEL

no storm-control (broadcast | dlf | multicast) level

【View】

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

sa (static aggregation group) port view

po (dynamic aggregation group) port view

【Default Level】

2: Configuration level

【Parameter】

broadcast: sets the limit of broadcast message traffic of the port

dlf: Destination look-up fail, which is to set unicast storm suppression.

multicast: sets the limit of multicast message traffic of the port

LEVEL: the percentage of restricted storm suppression, ranging from 0.00 to 100.00 to two decimal places.

【Description】

storm-control: this command is used to set the limit on unicast/multicast/broadcast messages traffic of the port.

no storm-control: this command is used to unconfigure restricted port messages.

After setting the upper limit of port message traffic, the port regularly detects the received unicast/multicast/broadcast message flow. Once the data flow of a certain type of message is detected to reach the storm control of the port, it would be considered as storm, then the port can block the forwarding of such message.

By default, the percentage of storm suppression is 100.00%.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#storm-control broadcast level 20.02
Switch(config-ge8)#no storm-control broadcast level
```

3.6 MAC Address

3.6.1 Clear Dynamic MAC address

【Command】

clear mac-address-table dynamic (MAC | address MACADDR| interface IFNAME | vlan VID)

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

MAC: means clear of the specified dynamic MAC address, in the format HHHH.HHHH.HHHH.

address: means clear the specified dynamic MAC address.

interface: means to clear all dynamic addresses of a specified interface.

vlan: means to clear all dynamic addresses of the specified vlan, ranging from 1-4094;

【Description】

clear mac-address-table dynamic: this command is used to clear the specified dynamic MAC address, or to clear all dynamic MAC addresses on the specified interface or VLAN.

【Instance】

```
Switch> enable
*Switch#clear mac-address-table dynamic interface ge1
```

3.6.2MAC Address Learning

【Command】

mac-address-learning (disable | enable)

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

disable: disable global MAC learning.

enable: enable global MAC learning.

【Description】

mac-address-learning: The function of this command is to disable the global MAC address learning ability, so that the global MAC address learning can not be carried out; Or enable the global MAC address learning ability, according to the port of the MAC address learning ability to take effect.

By default, the learning capability of the global MAC address is enabled.

When the MAC address learning ability is enabled, the MAC address learned by the port is a dynamic MAC address, and the aging time is determined by the user settings.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mac-address-learning disable
```

3.6.3MAC Address Aging-Time

【Command】

```
mac-address-ageingtime ( 0 | <10-1000000> )
no mac-address-ageingtime
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

ageing-time: set the aging time of the global MAC. The value range of dynamic address aging time is <10-1000000>, in seconds. 0 means to disable aging function.

【Description】

mac-address-ageingtime: command is to set the dynamic aging time of the MAC address table. When the user enters the 0 parameter, it means to disable the aging time of MAC.

no mac-address-ageingtime: MAC address aging time is restored to the default value. By default, the aging time is set to 300 seconds.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mac-address-ageingtime 500
```

3.6.4 Static MAC Address Filtering

【Command】

mac-address-table static MAC (discard | forward) IFNAME vlan VLAN

no mac-address-table static address MAC (vlan VLAN |)

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

Discard: set a MAC address for the port .Discard the packet if the packet's source MAC address is the same as the set MAC address.

Forward: sets a MAC address of the port. Forward the packet if the source MAC address is consistent with the set MAC address.

vlan: specifies the vlan corresponding to the table entry, with a range of <2-4094>. If there is no input, the default is vlan 1.

【Description】

mac-address-table static MAC forward IFNAME: this command is to set a static MAC address to the MAC table entry on the specified port. Static addresses, as opposed to dynamic ones, never aging and can only be manually configured and deleted. Static addresses will not lost even if the device is reset.

No static address is set by default.

Static addresses cannot be set to multicast addresses.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mac-address-table static 0.8.4 forward ge10 vlan 3
```

3.6.5 Multicast MAC Address Filtering

【Command】

```
mac-address-table multicast MAC ( discard | forward) IFNAMELIST vlan <2-4094>
no mac-address-table multicast address MAC interface IFNAME vlan <2-4094>
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

IFNAMELIST: multiple ports can be entered simultaneously. For example: ge1, ge2

vlan: specifies the vlan corresponding to the table entry, with a range of <2-4094>. If there is no input, the default is vlan 1.

【Description】

mac-address-table static MAC forward IFNAMELIST: this command is to set a static Multicast MAC address to the MAC table entry on the specified port. Static addresses, as opposed to dynamic protocol learned, never aging and can only be manually configured and deleted. Static addresses will not lost even if the device is reset.

no mac-address-table multicast: is used to remove static multicast table entries configured with command. The three commands of interface, mac and vlan can be randomly combined. That is, through the port to batch delete, can also delete a specific MAC specific VLAN under the specific port.

No static address is set by default.

 Notice

Currently only single port deletions are allowed when deleting configuration. Multiple port combination deletion is not allowed.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mac-address-table    multicast    0100.5e00.0001
forward ge10,ge11,ge12 vlan 3
```

3.6.6 Display MAC Address Table

【Command】

```
show mac-address-table
show mac-address-table ( multicast | dynamic | static | )
```

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

multicast: displays the table entry of multicast MAC address.

Dynamic: displays dynamic MAC address table entries.

static: displays dynamic MAC address table entries.

【Description】

show mac-address-table: this command displays the MAC table of the device. Without parameters, all MAC addresses are displayed, including user-configured static MAC addresses, dynamic MAC addresses learned by protocol, and multicast MAC addresses. With the relevant parameters, the corresponding MAC address is displayed, when with multicast, dynamic and static multicast MAC addresses are displayed.

【Instance】

```
Switch> enable
Switch#show mac-address-table
```

3.7 Mirror Command

3.7.1 Port Mirror Configuration

【Command】

mirror session <1-4> (both | receive | transmit) destination IFNAME source IFNAMELIST

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

session: mirror group number, value range: <1-4>.

TRAFFIC: messages direction of monitored port. That is to monitor the messages received or transmit.

- both: means both receiving and sending packets are monitored.
- transmit: stands for direction of transmit package.
- receive: stands for direction of receive package.

directions: means the destination port.

source: means the source port. Multiple ports can be input at the same time, separated by commas.

【Description】

Mirrors a message in the specified direction of the source port to the destination port.

Notice

- There is and can only be one destination port for mirroring, but multiple source ports can be configured simultaneously. And the destination port of one mirror group cannot be the source port for other mirror groups.
- The direction of the port mirroring cannot be covered, but only superimposed. When a

certain direction is not needed, the group needs to be deleted and reconfigured.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mirror session 1 both destination ge1 source ge2,ge3
```

3.7.2 Delete Port Mirror

【Command】

no mirror session <1-4> direction (both | receive | transmit) source IFNAME

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

session: mirror group number, value range: <1-4>.

TRAFFIC: messages direction of monitored port. That is to monitor the messages received or transmit.

- both: means both receiving and sending packets are monitored.
- transmit: stands for direction of transmit package.
- receive: stands for direction of receive package.

source: means the source port. Multiple ports can be input at the same time, separated by commas.

【Description】

Delete Mirror Configuration The three parameters in this instruction are optional, that is, user can only type session, or session and direction when deleting, or directly type no mirror without any parameters. And parameter position arbitrary swap, will not affect the execution of instructions.

【Instance】

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#no mirror session 1 source ge2
```

3.8 Link Aggregation Configuration

3.8.1 Dynamic Aggregation System Priority

【Command】

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

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<priority> : dynamic aggregation system priority, range is 1-65535

【Description】

lacp system-priority: this command is used for dynamical aggregate system priorities.

By default, the system priority is 32768.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#lacp system-priority 1
```

3.8.2 Dynamic Aggregation Port Priority

【Command】

```
lacp prot-priority <priority>
no lacp prot-priority
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

<priority> : dynamic aggregation port priority, range is 1-65535.

【Description】

lacp port-priority: this command is used for dynamic aggregation port priorities.

By default, the port priority is 32768.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#lacp port-priority 1
```

3.8.3 Dynamic Aggregation Port Timeout

【Command】

lacp timeout (short | long)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

Short: short timeout 3 seconds, the time threshold of neighborhood information aging.

Long: long timeout 90 seconds, the time threshold of neighborhood information aging.

【Description】

lacp timeout: this command is used for dynamic aggregate port timeout.

By default, it is long timeout.

【Instance】

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#interface ge8
Switch(config-ge8)#lacp timeout short
```

3.8.4 Add Dynamic Aggregation Group

【Command】

```
channel-group <id> mode (active | passive)
no channel-group
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

< id> : aggregation group number, the range is <1-12>.

Active: active mode, in which the switch actively initiates the aggregation negotiation process.

Passive: the mode in which the switch passively receives the aggregate negotiation process.

【Description】

channel-group: this command is used to add dynamic aggregation port members and configure the LACP mode for the ports.

When the first aggregation group member port is added, the corresponding aggregation group interface will be created. The interface name is Po + aggregation group number (the static aggregation group is sa+ aggregation group number). For example, a dynamic aggregation group interface named po100 with aggregation group number 100 is created by command channel-group 100 mode active.

When the last aggregation group member port is deleted, the corresponding aggregation group interface will be deleted.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#channel-group 1 mode active
```

3.8.5 Add Static LACP

【Command】

static-channel-group <id>

no static-channel-group

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

< id> : aggregation group number, the range is <1-12>.

【Description】

static-channel-group: this command is used to add static aggregate port members.

When the first aggregation group member port is added, the corresponding aggregation group interface will be created. The interface name is sa + aggregation group number (the dynamic aggregation group is po+ aggregation group number). For example, a static aggregation group interface named sa9 with aggregation group number 9 is created by command static-channel-group 9.

When the last aggregation group member port is deleted, the corresponding aggregation group interface will be deleted.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#static-channel-group 2
```

3.8.6 Link Aggregation Load Balance Mode

【Command】

port-channel load-balance (dst-ip | dst-mac | dst-port | src-dst-ip | src-dst-mac | src-dst-port | src-ip | src-mac | src-port)

no port-channel load-balance

【View】

Aggregation group interface view

【Default Level】

2: Configuration level

【Parameter】

dst-ip: Load balance mode based on destination IP;

src-ip: Load balance mode based on source IP;

src-dst-ip: Load balance mode based on source and destination IP;

dst-mac: Load balance mode based on destination MAC;

src-mac: Load balance mode based on source MAC.

src-dst-mac: Load balance mode based on source and destination MAC;

dst-port: the load balance mode is based on destination port, do not support currently.

src-port: the load balance mode is based on source port, do not support currently.

src-dst-port: the load balance mode is based on source and destination port, do not support currently.

【Description】

port-channel load-balance: this command is used to configure the load balance mode of the aggregate group.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#static-channel-group 2
Switch(config)#interface sa2
Switch(config-sa2)#port-channel load-balance dst-port
Switch(config-sa2)#exit
Switch(config)#interface ge7
Switch(config-ge7)#channel-group 1 mode active
Switch(config)#interface po1
Switch(config-po1)#port-channel load-balance src-mac
```

3.8.7 Displays Dynamic Aggregation Group

【Command】

show etherchannel {[<*id*>] | [detail] | [load-balance] | [summary]}

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

<id>: LACP aggregation group number

【Description】

show etherchannel: this command is used for LACP aggregation group related information.

【Instance】

```
Switch#show etherchannel
% Lacp Aggregator: po1
% Member:
   ge7
```

3.8.8 Displays Static Aggregation Group

【Command】

show static-channel-group

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show static-channel-group: this command is used for static aggregation group information.

【Instance】

```
Switch#show static-channel-group
% Static Aggregator: sa1
% Member:         state
   ge8            unbndl
```

3.9 Port Statistics

Port message statistics can be seen through the show interface IFNAME command. The following is the analysis of this instruction.

3.9.1 Display Port

【Command】

show interface IFNAME

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

IFNAME: port name.

【Description】

The display mainly includes port name, port number, port medium, port property, port MAC address, MTU, bandwidth, configuration rate, duplex mode, running time and port message statistics. Here is an explanation of the key words that appear in the statistics:

- "Input" refers to the message statistics received by the port, i.e., "receive". "output" means the number of packets transmitted by the port, i.e., "transmit".
- "TYPE" refer to the classification of statistical message types.

- "Total" represents the statistics of all types of messages in the corresponding direction (i.e. input or output), and the unit is bit.
- "Unicast" represents the statistics of the packets of Unicast in the corresponding direction, and the unit is packets.
- "Multicast" represents the statistics of the packets of packets in the corresponding direction, and the unit is packets.
- "Broadcast" represents the statistics of the number of packets Broadcast in the corresponding direction, and the unit is packets.
- "Dropped" represents the statistics of the packets lost in the corresponding direction, and the unit is packets.
- "Error" represents the statistics of the number of packets of errors in the corresponding direction, with the unit of packets.

- "RATE" refers to the rate in the corresponding direction (it should be noted that this rate refers to the average rate in the corresponding type and direction in a specific period of time. Port statistics cannot be updated in real time, with an interval of about 24 seconds). In the "Total" type, the rate is expressed in parentheses as the ratio of message bytes to the "defined bandwidth" of the port, not the set bandwidth. The "defined bandwidth" here refers to the maximum bandwidth corresponding to the port, that is, the bandwidth ratio of the Gigabit port is calculated by Gigabit, and the 10 Gigabit port is calculated by 10 Gigabit, having nothing to do with the actual bandwidth set by the user.
- "PEAK" refers to the PEAK value, which is the maximum speed from the start to the execution of the command. The following brackets represent the time point at which the peak occurs.
- "TOTAL" refers to the total number of corresponding "TYPE". That is to say, the number (or digits) of corresponding type and direction messages obtained from startup to execution of command are counted. The following brackets represent the unit conversion result of the corresponding TOTAL (that is, when the TOTAL is 1024, the brackets show 1K).

In addition, all unit conversion in the command is carried out in the form of 1K = 1024.

【Instance】

```
Switch> enable
Switch#show interface ge1
```

3.10 Link Flapping Protection Configuration

3.10.1 Enable Link Flapping Protection

【Command】

link-flap protection enable

no link-flap protection enable

【View】

Port view

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

The command is used to enable link flapping protection function.

By default, link flapping protection function is not enabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge2
Switch(config-ge2)#link-flap protection enable
```

3.10.2 Enable Link Flapping Auto-Recovery

【Command】

link-flap auto-recovery enable

no link-flap auto-recovery enable

【View】

Global configuration mode, port view

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

Command is used to enable link flapping auto-recovery of global or port. If link flapping auto-recovery is enabled, after the interface enters the link flapping protection state, it will be delayed for a certain time (configured recovery interval), and the interface will exit the link flapping protection state.

By default, link flapping auto-recovery of global or port is not enabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge2
Switch(config-ge2)# link-flap auto-recovery enable
```

3.10.3 Configure Recovery Interval of Link Flapping

【Command】

```
link-flap auto-recovery interval [value ]
no link-flap auto-recovery interval
```

【View】

Global configuration mode, port view

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

Command is used to configure the auto-recovery interval of global or port link flapping.

By default, the auto-recovery interval of link flapping is 3600 seconds.

Value: the auto-recovery interval of link flapping, and the value range is < 30-86400 >.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge2
Switch(config-ge2)#link-flap auto-recovery interval 3600
```

3.10.4 Configure Detection Interval of Link Flapping

【Command】

```
link-flap interval [value ]
no link-flap interval
```

【View】

Global configuration mode, port view

【Default Level】

2: Configuration level

【Parameter】

Value: the detection interval of link flapping, and the value range is < 10-100 >.

【Description】

The command is used to configure the detection interval of interface link flapping.

By default, the detection interval of interface link flapping is 20 seconds.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge2
Switch(config-ge2)#link-flap interval 20
```

3.10.5 Configure Time Threshold Value of Link Flapping

【Command】

```
link-flap threshold [value ]
no link-flap threshold
```

【View】

Global configuration mode, port view

【Default Level】

2: Configuration level

【Parameter】

Value: link flapping times, and the value range is <3-100>.

【Description】

The command is used to configure the times of interface link flapping.

By default, the time of interface link flapping is 5 times.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge2
Switch(config-ge2)# link-flap threshold 6
```

3.10.6 Check Link Flapping Protection Configuration

【Command】

show link-flap [interface interface-name]

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

None

【Description】

The command is used to view the configuration and status information of port link flapping protection.

interface-name: specifies the interface type and interface number. Check the information of all ports when no port is specified, and check the information of designated port when port is specified.

【Instance】

```
Switch> enable
Switch# show link-flap interface ge2
```

4 VLAN Configuration

4.1 Enter VLAN Configuration Mode

【Command】

vlan database

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

The vlan database command is used to enter VLAN configuration mode.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#vlan database
```

4.2 Add VLAN ID

【Command】

vlan <vlan-id> （name WORD | ）

vlan range VLANLIST

no vlan <vlan-id>

【View】

VLAN configuration view

【Default Level】

2: Configuration level

【Parameter】

<vlan-id> : VLAN ID value, range is 2-4094.

WORD: VLAN name.

range: set the static VLAN in batch.

VLANLIST: VLAN range to be set, user can input a single number, continuous range vlan or a combination of single and range, separated by commas, eg: 4, 10-20.

【Description】

vlan: this command is used to create a static VLAN and configure the VLAN name.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
```

4.3 Port Type

【Command】

switchport mode (access| hybrid | trunk)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

Access: set the link type of the port to access type.

Hybrid: set the link type of the port to hybrid type.

trunk: set the link type of the port to trunk type.

【Description】

switchport mode: this command is used to configure the link type of the port.

By default, the link type of all ports are access.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#switchport mode trunk
```

4.4 Port Default VLAN

【Command】

```
switchport (access| hybrid ) vlan <vlan-id>
no switchport (access| hybrid ) vlan
switchport trunk native vlan <vlan-id>
no switchport trunk native vlan
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

access vlan: set the default vlan for a port in access mode to <2-4094>.

hybrid vlan: sets the default vlan for a port in hybrid mode to <2-4094>.

<2-4094> : VID allowed setting range is 2-4094.

Native vlan: set the local VLAN and classify the unmarked traffic through the Layer 2 interface, that is, set the PVID of the port.

【Description】

switchport (access | hybrid) vlan: this command is to reset the default VLAN of the port. For example, enter the configuration mode of port ge1, the port ge1 is in hybrid mode, and enter “switchport hybrid vlan 3”. The default VLAN ID for port ge1 becomes 3.

switchport trunk native vlan: this command specifies a native VLAN for a trunk port. As a Trunk port, it must belong to a native VLAN. The native VLAN refers to UNTAG

messages sent and received on the interface, which are all considered to belong to the VLAN. Obviously, the default VLAN ID of the interface (i.e., PVID in IEEE 802.1Q) is the VLAN ID of the native VLAN. At the same time, if native VLAN frames are sent in Trunk port, UNTAG must be adopted.

By default, the default VLAN ID of the port is 1.

 Notice

When setting the VLAN ID, the port mode parameter of the command must be consistent with the current mode of the setting port to ensure the setting takes effect, otherwise an error will be returned.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#switchport access vlan 2
```

4.5 Classify VLAN Based on Port

【Command】

```
switchport hybrid allowed vlan add (tag| untag )<vlan-id>
switchport hybrid allowed vlan remove <vlan-id>
switchport hybrid allowed vlan (all | none)
switchport trunk allowed vlan (add |except | remove) <vlan-id>
switchport trunk allowed vlan (all | none)
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

<vlan-id> : VLAN ID, range is 1-4094.

add: add the port to the VLAN.

all: add ports to all VLANS.

except: adds a port to all VLANS except the one specified.

none: delete the port from all VLANS except PVID.

remove: delete the port from the specified VLAN.

tag: the port will add a VLAN tag when forwarding a VLAN message.

untag: the port will remove the VLAN Tag when forwarding a VLAN message.

【Description】

switchport (hybrid | trunk) allowed vlan: this command is used to configure the port to be added to or removed from a specified VLAN.

Notice

- When adding hybrid or trunk ports to a VLAN, the port should be set to the appropriate type.
- Hybrid or trunk ports are untag in the VLAN to which PVID belongs, and trunk ports are tag in VLAN except PVID.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#switchport hybrid allowed vlan add tag 2
```

4.6 Display VLAN Information

【Command】

show vlan all

show vlan brief

show vlan <2-4094>

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

<2-4094>: VLAN ID range is 2-4094.

【Description】

show vlan all: displays all vlan information.
show vlan brief: displays vlan information of all Bridges.
show vlan <2-4094> : displays the specified vlan information.

【Instance】

```
Switch> enable
Switch# show vlan 2
```

4.7 Port Receive Frame Type

【Command】

switchport acceptable-frame-type (all | tagged | untagged)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

All: there is no restriction on whether the received message with tag.

Tagged: only allow the port to receive tagged message, that is, stop the port to receive untagged message.

untagged: only allow the port to receive untagged message, stop the port to receive tagged message.

【Description】

The switchport accept-frame-type command is used to restrict whether the port is allowed to accept message with tags.

By default, the accepted frame type of the port is set to all, which means that the port does not by default restrict whether or not it can receive packets with tags. However, if the accepted frame type of the port is set to tagged, the port can only allow tagged message to pass, and other packets will be discarded.

【Instance】

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#interface ge8
Switch(config-ge8)#switchport acceptable-frame-type tagged
```

4.8 Port Entry Filtering

【Command】

```
switchport ingress-filter ( enable | disable )
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

enable: only messages from the VLAN to which the port belongs are allowed to be received.

disable: allows to receive messages from VLANs that do not belong to the port.

【Description】

The ingress filter function of the device defaults to enable, that is, any port only allows packets belonging to its VLAN to pass through. Other message will be discarded. However, when the ingress filter function of the port is set to disable, the port will allow to receive messages not belonging to the VLAN of the port and forward the message to the specified VLAN.

For example, set port entry filtering on port ge1 to disable. Port ge1 belongs to vlan10. The message is sent to ge2 belonging to vlan20. After ge1 receives the message, the port will receive the message and forward the message to the specified vlan. In other words, the message will be forwarded to ge2 belonging to vlan20 instead of discarding the message.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#switchport ingress-filter disable
```

4.9 VLAN Classifer Function

4.9.1 VLAN Classifier Function Introduction

The VLAN classifier is similar to PVID in that it assigns a default VLAN ID to packets entering the switch port. It provides MAC-based, subnet-based and protocol-based assignment. If a packet matches all of the three, only one rule will take effect. The priority of the rules is: MAC-based, subnet-based, and protocol-based. For example, if MAC-based rules are matched first, neither subnet-based nor protocol-based VLAN assignment rules will take effect. If none of the three rules match, VLAN ID are assigned according to PVID rule.

4.9.2 Rule Configuration

4.9.2.1 Classify VLAN Based on Sub-network

【Command】

vlan classifier rule <1-256> ipv4 A.B.C.D/M vlan <1-4094>

【View】

Global Configuration

【Default Level】

2: Configuration level

【Parameter】

<1-256>: group number.

A.B.C.D/M: sub-network segment.

<1-4094>: represents the VLAN ID assigned by the matching rule.

【Description】

Configure subnet-based VLAN rules.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#vlan classifier rule 1 ipv4 192.168.2.0/24 vlan 2
```

4.9.2.2 Classify VLAN Based on MAC Address

【Command】

```
vlan classifier rule <1-256> mac WORD vlan <1-4094>
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<1-256>: group number.

MAC: MAC address.

<1-4094>: represents the VLAN ID assigned by the matching rule.

【Description】

Configure MAC-based VLAN rules.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#vlan classifier rule 1 mac 0.0.2 vlan 3
```

4.9.2.3 Classify VLAN Based on Protocol

【Command】

```
vlan classifier rule <1-256> proto
(ip|ipv6|ipx|x25|arp|rarp|atalkddp|atalkaarp|atmmulti|atmtrans
port|pppdiscovery|pppsession|xeroxpup|xeroxaddrtrans|g8bpqx25|
ieeepup|ieeeaddrtrans|dec|decdnadumpload|decdnaremoteconsole|d
ecdnarouting|declat|decdiagnostics|deccustom|decsyscomm|<0-655
35>) encap (ethv2|snapllc|nosnapll) vlan <1-4094>
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<1-256>: group number.

proto: Ethernet protocol type; enter ip, ipv6, ipx, x25, arp, rarp, atalkddp, atalkaarp, atmmulti, atmtransport, pppdiscovery, pppsession, xeroxpup, xeroxaddrtrans, g8bpqx25, ieeepup, ieeeaddrtrans, dec, decdnadumpload, decdnaremoteconsole, decdnarouting, declat, decdiagnostics, deccustom, decsyscomm or enter protocol number <0-65535>

encap: Ethernet Encapsulation Type；ethv2，snapllc，nosnapll.

<1-4094>: represents the VLAN ID assigned by the matching rule.

【Description】

Configure protocol-based VLAN rules.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#vlan classifier rule 1 proto ip encap ethv2 vlan
3
```

4.9.2.4 Delete VLAN Rule

【Command】

no vlan classifier rule <1-256>

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<1-256>: group number.

【Description】

Delete a rule.

【Instance】

```
Switch> enable
```

```
Switch#configure terminal
Switch(config)#no vlan classifier rule 1
```

4.9.3 Group Configuration

【Command】

```
vlan classifier group <1-16> (add | delete) rule <1-256>
no vlan classifier group <1-16>
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<1-16>: group number.

add: add a rule to a group.

delete: delete a rule from a group.

<1-256> : rule number;

【Description】

vlan classifier group: group configuration.

no vlan classifier group: delete group.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#vlan classifier group 1 add rule 2
Switch(config)#no vlan classifier group 2
```

4.9.4 Interface Configuration Command

【Command】

```
vlan classifier activate <1-16>
no vlan classifier activate <1-16>
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

<1-16> : reference group number;

【Description】

vlan classifier activate: interface reference group.

no vlan classifier activate: delete interface reference group.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#vlan classifier activate 1
Switch(config-ge1)#no  vlan classifier activate 2
```

5 Ring Configuration

Ring is made up of the company independent research and development, professional link redundancy backup for the needs of high reliability of industrial control network application and development of the design of Ethernet rapid spanning tree algorithm, its design concept is completely in accordance with international standards (STP and RSTP) implementation, and do the necessary for industrial control application optimization, with Ethernet link redundancy, fault fast automatic recovery ability, when a network interruption or network failure, Ring can ensure that the user network automatic recovery link communication within 20 ms.

5.1 Global Ring Enable

【Command】

```
[no ] ring
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

ring: this command is used to enable the global Ring function.

no ring: this command is used to disable the global Ring function and delete all Ring groups.

By default, the global Ring function is disabled.

【Instance】

```
Switch> enable
Switch# configure terminal
Switch(config)# ring
```

5.2 Create Ring NetworkGroup

【Command】

```
ring <group-id> id <ring-id> port1 <ifname> port2 <ifname> type
0 hello <hello-time> (master | slave)
ring <group-id> id <ring-id> port1 <ifname> port2 <ifname> type
<type-id> hello <hello-time>
no ring <group-id>
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

group-id: ring group ID, range is 1-4.

ring-id : ring loop ID, range is 0-255.

ifname: ring port name, the port can be a physical port or a static aggregation group, and the port cannot enable spanning tree or ERPS.

type-id: ring loop type, range 0-3, corresponding to Single Ring, Coupling Ring, Chain, Dual Homing.

hello-time: hello request packet sending period, range 0-300(*100ms), 0 means to do not send.

Master | slave: ring network master device selection, no master station if all are masters, only ring type is Single ring can be configured.

【Description】

ring <group-id> : this command is used to configure the ring group.

no ring <group-id> : this command is used to delete the ring group.

By default, no ring group is configured.

Ring Type Description

A Single Ring is a basic ring networking structure in which all devices are connected in a ring. When the network is working normally, the algorithm running on the device will automatically block a link as a backup link to ensure the normal operation of the network. When the network has a link failure, the algorithm will automatically start the backup link and resume data communication within 20 ms.

Coupling Ring is a redundant structure introduced to connect two separate networks. The Coupling Ring provides additional security by enabling the coupling of two ports on different switches. For some systems, users can also create single rings for devices from different regions and also integrate multiple single rings through the Coupling Ring to create a larger redundant network.

Chain refers to connecting multiple switch devices in series and connecting both ends of the Chain to Ethernet network. Chain has strong channel selection ability. When the network is working properly, the algorithm automatically blocks one link in the Chain as a backup link, forcing all devices to access the Ethernet network from the unblocked end of the link. When Chain link failure occurs, the algorithm will automatically start the backup link within 20ms and quickly guide the device access the Ethernet network through the side that do not has a link failure.

Dual Homing is a special case of the Chain, in which users can host the same switch on two different networks or two different switching devices on the same network. The algorithm will automatically select one link for data communication according to the link condition. When the link in the communication state fails, the other link will start to work within 20ms.

Notice:

1. RING loop ports can be normal physical ports or static aggregation groups.

2. The RING loop port cannot enable other layer 2 protocols (MSTP, ERPS, etc.) at the same time.

【Instance】

```
Switch> enable
Switch# configure terminal
Switch(config)# ring 1 id 1 port1 ge1 port2 ge3 type 1 hello 1
```

5.3 Display Ring Network Information

【Command】

show ring [<*group-id*>]

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

group-id : ring group ID, range is 1- 4

【Description】

show ring: this command is used to show ring information.

【Instance】

```
Switch(config)#interface ge3
Switch(config-ge3)#spanning-tree disable
*Switch(config-ge3)# exit
*Switch(config)#interface ge4
*Switch(config-ge4)#spanning-tree disable
*Switch(config-ge4)#exit
*Switch(config)#ring 1 id 1 port1 ge3 port2 ge4 type 0 hello 0 master
*Switch#show ring
ring global : Enable
ring list:
ring GROUP: 1
ring ID: 1
ring PORT1: ge3
ring PORT1 state: block
ring PORT2: ge4
ring PORT2 state: block
ring TYPE: Single
ring HELLOTIME: 0
ring : master
```

6 MSTP Configuration

6.1 Global Spanning-tree Enablement

【Command】

spanning-tree (enable | disable)

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree enable: this command is used to enable the global spanning tree protocol.

spanning-tree disable: this command is used to disable the spanning tree protocol.

By default, the global spanning tree protocol is enabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree disable
```

6.2 Enter MSTP Instance Configuration View

【Command】

spanning-tree mst configuration

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree mst configuration: this command is used to enter the MSTP instance configuration view.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
```

6.3 Create MSTP Instance

【Command】

instance < instance -id> vlan <vlan-id>
no instance < instance -id> [vlan <vlan-id>]

【View】

MST configuration view

【Default Level】

2: Configuration level

【Parameter】

<instance-id>: the number of MSTI in the range 0-16.

<vlan-id> : VLAN ID value, the range is 1-4094.

【Description】

instance: This command is used to create MSTP instance.

no instance: this command is used to delete the MSTP instance.

instance instance_id vlan vlan_id: this command is used to configure the mapping between vlan and MSTP instances. If the Instance does not exist, it will be created first.

By default, all VLANS map to CIST (that is, MSTI 0).

Notice

- Different MSTI cannot be mapped to the same VLAN. If a VLAN that has been mapped to one MSTI is remapped to another MSTI, the original mapping relationship will be canceled.
- When adding a VLAN mapping, it is recommended to configure the VLAN first.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 1 vlan 2
```

6.4 MSTP Revision Level

【Command】

revision <level>

【View】

MST configuration view

【Default Level】

2: Configuration level

【Parameter】

<level> : revision level, range 0-255.

【Description】

revision: this command is used to configure the MSTP revision level for the MST domain.

By default, the MSTP revision level for the MSTP domain is 0.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#revision 1
```

6.5 MST Domain Name

【Command】

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

【View】

MST configuration view

【Default Level】

2: Configuration level

【Parameter】

<name> : the domain name of the MST domain.

【Description】

region <name>: this command is used to configure the domain name for the MST domain.

By Default, the MST domain name is Default.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#region test
```

6.6 Device Priority

【Command】

```
spanning-tree [instance <instance_id>] priority <priority>
```

no spanning-tree [instance <instance_id>] priority

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<priority> : device priority (multiple of 4094), <0- 61440>

【Description】

spanning-tree priority: this command is used to configure the device priority of CIST.

no spanning-tree priority: this command is used to restore the device priority of CIST to the default value.

spanning-tree instance priority: this command is used to configure the device priority of the MSTI.

no spanning-tree instance priority: this command is used to restore the device priority of MSTI to the default value.

By default, the device priority is 32768.

CIST refers to spanning tree instance 0, and MSTI refers to creating spanning tree instance, with instance range 1- 16.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree priority 4096
```

6.7 Spanning-tree Protocol Version

【Command】

spanning-tree force-version <version>

no spanning-tree force-version

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<version>: spanning tree protocol version number, range is 0- 3, 0 is STP compatibility mode, 2 is RSTP mode, 3 is MSTP mode, 1 is unsupported.

【Description】

spanning-tree force-version: this command is used to configure the version of the spanning tree protocol.

no spanning-tree force-version: this command restores the version of the spanning tree protocol to the MSTP protocol.

By default, the working mode of MSTP is MSTP mode.

MSTP and RSTP can recognize each other's protocol messages and are compatible with each other. STP cannot recognize MSTP messages, in order to realize mixed networking with STP equipment and complete compatibility with RSTP, there are three operating modes have been set: STP compatibility mode, RSTP mode and MSTP mode.

- In STP compatibility mode, each port of the device will send out STP BPDU messages.
- In the RSTP mode, each port of the device will send out RSTP BPDU messages. When it is found to be connected with the device running STP, the port will automatically switch to the STP compatibility mode.
- In MSTP mode, each port of the device will send out MSTP BPDU messages. When it is found that it is connected with the device running STP, the port will automatically switch to STP compatibility mode.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree force-version 2
```

6.8 Spanning Tree Timer Parameter

【Command】

```
spanning-tree (hello-time | forward-time | max-age) <seconds>
no spanning-tree hello-time
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<seconds> : hello-time range <1-10>, forward-time range <4-30>, max-age range <6-40>, all in seconds

【Description】

spanning-tree hello-time: the command is used to configure the hello-time.

no spanning-tree hello-time: this command is used to restore the hello-time to default value.

By default, hello-time is 2 seconds, forward-time is 15 seconds, and max-age is 20 seconds.

The values of the three time parameters of the root bridge hello-time, forward-time and max-age should meet the following formula, otherwise will cause the network oscillation frequently:

2 ×（forward-time - 1）≥ max-age

max-age ≥ 2 ×（hello-time + 1）

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree hello-time 3
```

6.9 The Maximum Hop of Spanning-tree

【Command】

spanning-tree max-hops <hops>

no spanning-tree max-hops

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<hops> : the maximum hops of MST domain are in the range <1-40>.

【Description】

spanning-tree max-hops: this command is used to configure the maximum number of hops of the MST domain.

no-spanning -tree max-hops: this command restores max-hops as the default.

By default, the max-hops is 20.

Starting from the root bridge of spanning tree in MST domain, every time configuration message in domain (namely BPDU message) is forwarded by a device, the hop number is reduced by 1; Devices discard configuration messages with 0 hops received, preventing devices outside the maximum hops from participating in the spanning tree calculation, limiting the size of the MST domain.

If the current device becomes the root bridge of CIST in MST domain or the root bridge of MSTI, the maximum hop number of this device configuration will become the network diameter of this spanning tree, limiting the scale of this spanning tree in the current MST domain. Devices that do not generate root Bridges in the MST domain will use the maximum number of hops set by the root bridge.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree max-hops 24
```

6.10 The Rate that the Spanning Tree Sends a BPDU

【Command】

spanning-tree transmit-holdcount <count>

no spanning-tree transmit-holdcount

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<count> : maximum number of message sent per second, range is <1-10>.

【Description】

spanning-tree transmit-holdcount: this command is used to configure the maximum rate of sending the BPDU of the port.

no spanning-tree transmit-holdcount: this command is used to restore the maximum rate of sending the BPDU of the port to default value.

By default, transmit-holdcount is 3.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree transmit-holdcount 10
```

6.11 Compatible with Cisco MSTP Mode

【Command】

spanning-tree cisco-interoperability (enable | disable)

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree cisco-interoperability enable: this command is used to enable compatibility with the cisco MSTP pattern.

By default, cisco MSTP mode is not compatible.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree cisco-interoperability enable
```

6.12 Global Edge Port BPDU Filtering

【Command】

```
spanning-tree portfast bpdu-filter
no spanning-tree portfast bpdu-filter
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree portfast bpdu-filter: this command is used to enable the global portfast bpdu-filter function.

no-spanning -tree portfast bpdu-filter: this command disables the global portfast bpdu-filter function.

By default, global portfast bpdu-filter is disabled.

The portfast features (bpdu-filter and bpdu-guard) both need to be valid on the portfast port (see related command spanning-tree portfast). The portfast feature can be enabled in configure mode or under the port (see the relative commands under the port). There are only enable and disable two state in configure mode, while there are enable, disable and default three states under the port. When the configured portfast feature of the port is default, the actual running portfast feature of the port will be the same as the portfast feature in configure mode. When the portfast feature configured of the port is enable or disable, the actual running portfast feature of the port will be consistent with the portfast feature configured on the port. Use the show spanning-tree interface command to view relative details.

By default, the global portfast bpdu-filter function is disabled.

The portfast function is mainly used to connect devices such as terminals or servers, which needs fast convergence ports, similar to edgeport. Portfast must be enabled if the port needs to use the portfast feature.

Bpdu-filter function is used for portfast port, after enabling it, the port will not send and receive bpdu messages.

bpdu-guard function is used for portfast port. Once enabled, when the port receives bpdu message, the port will change into error-disable state (shutdown), which can be restored by errdisable-timeout function.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree portfast bpdu-filter

*Switch#show spanning-tree interface ge6
% Default: Bridge up - Spanning Tree Enabled  - topology change
detected
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge
Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit
Hold Count 6 - Max-hops 20
% Default: CIST Root Id 800000b25f5f0003
% Default: CIST Reg Root Id 800000b25f5f0003
% Default: CIST Bridge Id 800000b25f5f0003
% 0: 1 topology change(s)  - last topology change Thu Jan  1 08:00:29
1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard enabled
% Default: portfast errdisable timeout enabled
% Default: portfast errdisable timeout interval 300 sec
%   ge6: Port Number 910 - Ifindex 5006 - Port Id 838e - Role Disabled
- State Discarding
%   ge6: Designated External Path Cost 0 -Internal Path Cost 0
%   ge6: Configured Path Cost 20000  - Add type Explicit ref count
1
%   ge6: Designated Port Id 0 - CIST Priority 128  -
%   ge6: Message Age 0 - Max Age 0
%   ge6: CIST Hello Time 0 - Forward Delay 0
%   ge6: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 -
topo change timer 0
%   ge6: forward-transitions 0
%   ge6: Version Multiple Spanning Tree Protocol - Received None
- Send MSTP
%   ge6: No portfast configured - Current  portfast off
```

```
%    ge6: portfast bpdu-guard   default   - Current portfast
bpdu-guard on
%    ge6: portfast bpdu-filter default   - Current portfast
bpdu-filter off
%   ge6: no root guard configured    - Current root guard off
%     ge6: Configured Link Type point-to-point  - Current
point-to-point
%   ge6: No auto-edge configured - Current port Auto Edge off
```

6.13 Global Edge Port BPDU Protection

【Command】

spanning-tree portfast bpdu-guard
no spanning-tree portfast bpdu-guard

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree portfast bpdu-guard: this command is used to enable the global portfast bpdu-guard function.
no spanning-tree portfast bpdu-guard: this command is used to disable the global portfast bpdu-guard function.
By default, global portfast bpdu-guard is disabled.

The portfast features (bpdu-filter and bpdu-guard) both need to be valid on the portfast port (see related command spanning-tree portfast). The portfast feature can be enabled in configure mode or under the port (see the relative commands under the port). There are only enable and disable two state in configure mode, while there are enable, disable and default three states under the port. When the portfast feature configured under the port is default, the actual running portfast feature under the port will be the same as the global portfast feature. When the portfast feature configured of the port is enable or disable, the actual running portfast feature of the port will be

consistent with the portfast feature configured on the port. Use the show spanning-tree interface command to view relative details.

By default, the global portfast bpdu-filter function is disabled.

The portfast function is mainly used to connect devices such as terminals or servers, which needs fast convergence ports, similar to edgeport. Portfast must be enabled if the port needs to use the portfast feature.

Bpdu-filter function is used for portfast port, after enabling it, the port will not send and receive bpdu messages.

Bpdu-guard function is used for portfast port. Once enabled, when the port receives bpdu message, the port will change into error-disable state (shutdown), which can be restored by errdisable-timeout function.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree portfast bpdu-guard
```

6.14 Port error-disable Timeout Recover

【Command】

```
spanning-tree errdisable-timeout (enable | disable)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree errdisable-timeout enable: this command is used to configure the error-disable timeout recovery function of the port.

spanning-tree errdisable-timeout disable: this command is used to disable the error-disable timeout recovery function of the port.

By default, the port error-disable timeout recovery function is enabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree errdisable-timeout enable
```

6.15 Port error-disable Recovery Interval

【Command】

spanning-tree errdisable-timeout interval <seconds>

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<seconds>: the recover interval of error-disable, in the range <10-1000000>.

【Description】

spanning-tree errdisable-timeout interval: this command is used to configure the time interval for recovery after error-disable of the port .

no spanning-tree errdisable-timeout interval: this command is used to restore the time interval for recovery after error-disable of the port to default.

errdisable-timeout interval is 300 seconds by default.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#spanning-tree errdisable-timeout interval 400
```

6.16 Edge Port

【Command】

spanning-tree portfast

no spanning-tree portfast

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree portfast: this command is used to enable the portfast function of the port.

no spanning-tree portfast: this command is used to disable the portfast function.

By default, port portfast is disabled.

The portfast function is mainly used to connect terminals or servers and other devices, requiring fast convergence of the port. Portfast must be enabled if the port needs to use the portfast feature.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree portfast
```

6.17 BPDU Filter of Edge Port

【Command】

spanning-tree portfast bpdu-filter (enable | disable | default)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree portfast bpdu-filter: this command is used to configure the mode of the portfast bpdu-filter feature under the port, enable, disable, default respectively.
By default, the port portfast bpdu-filter is in default.

The portfast features (bpdu-filter and bpdu-guard) both need to be valid on the portfast port (see related command spanning-tree portfast). The portfast feature can be enabled in configure mode or under the port (see the relative commands under the port). There are only enable and disable two state in configure mode, while there are enable, disable and default three states under the port. When the portfast feature configured under the port is default, the actual running portfast feature under the port will be the same as the global portfast feature. When the portfast feature configured of the port is enable or disable, the actual running portfast feature of the port will be consistent with the portfast feature configured on the port. Use the show spanning-tree interface command to view relative details.
By default, the global portfast bpdu-filter function is disabled.
The portfast function is mainly used to connect devices such as terminals or servers, which needs fast convergence ports, similar to edgeport. Portfast must be enabled if the port needs to use the portfast feature.
Bpdu-filter function is used for portfast port, after enabling it, the port will not send and receive bpdu messages.
bpdu-guard function is used for portfast port. Once enabled, when the port receives bpdu message, the port will change into error-disable state (shutdown), which can be restored by errdisable-timeout function.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree portfast bpdu-filter enable
```

6.18 BPDU Filter of Edge Port

【Command】

spanning-tree portfast bpdu-guard (enable | disable | default)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree portfast bpdu-guard: this command is used to configure the modes of the portfast bpdu-guard feature of the port, they are enable, disable, default.
By default, the port portfast bpdu-guard is in default.

The portfast features (bpdu-filter and bpdu-guard) both need to be valid on the portfast port (see related command spanning-tree portfast). The portfast feature can be enabled in configure mode or under the port (see the relative commands under the port). There are only enable and disable two state in configure mode, while there are enable, disable and default three states under the port. When the portfast feature configured under the port is default, the actual running portfast feature under the port will be the same as the global portfast feature. When the portfast feature configured of the port is enable or disable, the actual running portfast feature of the port will be consistent with the portfast feature configured on the port. Use the show spanning-tree interface command to view relative details.
By default, the global portfast bpdu-filter function is disabled.
The portfast function is mainly used to connect devices such as terminals or servers, which need fast convergence ports, similar to edgeport. Portfast must be enabled if the port needs to use the portfast feature.
Bpdu-filter function is used for portfast port, after enabling it, the port will not send and receive bpdu messages.
bpdu-guard function is used for portfast port. Once enabled, when the port receives bpdu message, the port will change into error-disable state (shutdown), which can be restored by errdisable-timeout function.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
```

```
Switch(config-ge8)#spanning-tree portfast bpdu-guard enable
```

6.19 Automatical Switching Edge Port

【Command】

```
spanning-tree autoedge
no spanning-tree autoedge
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree autoedge: this command is used to configure ports to automatically switch to edge ports.

no spanning-tree autoedge: this command conjures ports that cannot be automatically switched to non-edge ports.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree autoedge
```

6.20 Root Port Protection

【Command】

```
spanning-tree guard root
no spanning-tree guard root
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree guard root: this command is used to configure the root port protection function.

no spanning-tree guard root: this command concatenates the port to not enable root port protection.

By default, root port guard is not enabled.

guard root is a mandatory root protection that stops accidental (or illegal) switches becoming root Bridges in the network. when the guard root port (designated ports) is opened and receives better BPDU packets, the port will enter a Listening (STP) or discarding state (RSTP, MSTP).

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree guard root
```

6.21 Port Spanning-tree Enablement

【Command】

spanning-tree (enable | disable)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

spanning-tree enable: this command is used to enable the spanning tree function of the port.

spanning-tree disable: this command is used to disable the spanning tree function of the port.

By default, the port spanning tree function is enabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree enable
```

6.22 Port Hello-time

【Command】

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

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

<seconds> : hello-time，range is 1-10.

【Description】

spanning-tree hello-time: this command is used to configure the hello-time of the port.

no spanning-tree hello-time: this command is used to restore the hello-time of the port to its default value.

By default, the hello-time of the port is 2.

It is better to use global configuration commands for hello-time.

【Instance】

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree hello-time 3
```

6.23 Port Connection Type

【Command】

spanning-tree link-type (auto | point-to-point | shared)

no spanning-tree link-type

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

Auto: automatically determines the connection type, point-to-point or shared, based on duplex mode.

Point-to-point: specifies the port type as point-to-point.

Shared: specifies the port type as shared.

【Description】

spanning-tree link-type: this command is used to modify the link type of the port.

no spanning-tree link-type: this command is used to restore the link type of the port to the default value.

By default, the link type of the port is auto.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree link-type point-to-point
```

6.24 Port Priority

【Command】

spanning-tree [instance <instance_id>] priority <priority>

no spanning-tree instance <instance_id> priority

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

<instance-id>: the number of MSTI in the range 0-16.

<priority> : port priority, the range is 0-240.

【Description】

spanning-tree priority: this command is used to configure the port priority.

no spanning-tree priority: this command is used to restore the port priority to the default.

By default, the port priority is 128.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree priority 32
```

6.25 Cost

【Command】

```
spanning-tree [instance <instance_id>] path-cost <cost>
no spanning-tree instance <instance_id> path-cost
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

<instance-id>: the number of MSTI in the range 0-16.

<cost> : means the cost value of the port, ranging from 1-200000000.

【Description】

spanning-tree path-cost: this command is used to configure the port cost.

no spanning-tree path-cost: this command is used to restore the port cost as the default.

By default, the port cost is 20000000.

When the port cost is the default value, the actual cost of link up port is converted according to the port rate, the rate of 10M corresponds to the cost of 2000000, and 100M corresponds to the cost of 200000.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree path-cost 1000
```

6.26 Port Restricted Election

【Command】

```
spanning-tree [instance <instance_id>] restricted-role
no spanning-tree instance <instance_id> restricted-role
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

<instance-id> : the number of MSTI in the range 0-16.

【Description】

spanning-tree restricted-role: the command is used to configure ports to restrict elections so that ports cannot be elected as root ports.

no spanning-tree restricted-role: the command is used to cancel port restricted elections.

By default, the port does not restrict elections.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree restricted-role
```

6.27 Port Restriction TC

【Command】

spanning-tree [instance <instance_id>] restricted-tcn

no spanning-tree instance <instance_id> restricted-tcn

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

<instance-id>: represents the number of MSTI in the range 0-16.

【Description】

spanning-tree restricted-tcn: the command is used to configure port restriction processing for receiving TC bits in BPDU message.

no spanning-tree restricted-tcn: the command is used to cancel the port restriction processing of the TC bit in the received BPDU message.

By default, no restriction on the port.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#spanning-tree restricted-tcn
```

6.28 Display Spanning-tree Detail Information

【Command】

show spanning-tree (*interface IFNAME* |)

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

Interface IFNAME: displays status information of the specified port.

【Description】

show spanning-tree: this command is used to display the details of spanning-tree.

【Instance】

```
Switch#show spanning-tree
% Default: Bridge up - Spanning Tree Disabled
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge
Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit
Hold Count 6 - Max-hops 20
% Default: CIST Root Id 800000226f0100a3
% Default: CIST Reg Root Id 800000226f0100a3
% Default: CIST Bridge Id 800000226f0100a3
% 0: 0 topology change(s)  - last topology change Thu Jan  1 08:00:00
1970

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
%   ge1: Port Number 1 - Ifindex 5001 - Port Id 8001 - Role Disabled
- State Discarding
%   ge1: Link down - Spanning Tree Disabled
%   ge1: Designated External Path Cost 0 -Internal Path Cost 0
%   ge1: Configured Path Cost 20000000  - Add type Explicit ref count
1
```

```
%   ge1: Designated Port Id 0 - CIST Priority 128  -
%   ge1: Message Age 0 - Max Age 0
%   ge1: CIST Hello Time 0 - Forward Delay 0
%   ge1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 -
topo change timer 0
%   ge1: forward-transitions 0
%   ge1: Version MSTP - Received None - Send MSTP
%   ge1: Auto edge - On
%   ge1: Portfast - Off
%   ge1: Edge port - False
%   ge1: Bpdu Guard  - Disabled (Config - default)
%   ge1: Bpdu filter - Disabled (Config - default)
%   ge1: Link Type - point-to-point (Config - auto)
%   ge1: Root Guard - Off
```

6.29 Display the Basic Information of the Spanning Tree

【Command】

show spanning-tree (*instance* <*instance-id*>|) brief

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

<instance-id>: represents the number of MSTI in the range 0-16.

【Description】

The show spanning-treebrief command is used to show information for spanning-tree.

【Instance】

```
Switch#show spanning-tree brief
MST  Port           Role        State
0    ge10           Designated   Forwarding
```

7 ERPS Configuration

7.1 Enter ERPS Instance Configuration View

【Command】

erps instance config

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

erps instance config: this command is used to enter the ERPS instance configuration view.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
```

7.2 Create ERPS Instance Name

【Command】

erps creat erps-name <*NAME*>

no erps creat erps-name <*NAME*>

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name

【Description】

erps creat erps-name: the command is used to create an ERPS instance and specify the instance name.

By default, no configuration.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
```

7.3 ConfigureERPS Instance ID

【Command】

erps <*NAME*> set instanceID <*instance*>

no erps <*NAME*> set instanceID

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name

< instance > : MSTP instance number, the range is 0-16

【Description】

erps set instanceID: the command is used to configure the ERPS protection instance (configured by the spanning tree).

By default, no configuration.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set instanceID 1
```

7.4 Specify the Ring Instance Corresponding to the ERPS Instance

【Command】

```
erps <NAME> set ring <NAME>
no erps <NAME> set ring
```

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

< NAME > : ring instance name of ERPS

【Description】

erps set ring: this command is used to specify the ring instance corresponding to the ERPS instance (the ring instance is created and configured by the command in ring mode).

By default, no configuration.

【Instance】

```
Switch> enable
```

```
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set ring 1
```

7.5 Specify the Timer Instance Corresponding to the ERPS Instance

【Command】

erps <*NAME*> set timer <*NAME*>

no erps <*NAME*> set timer

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

< NAME > : timer instance name of ERPS.

【Description】

erps set ring: this command is used to specify the timer instance corresponding to the ERPS instance (the timer instance is created and configured by the command in ring mode).

By default, no configuration.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set timer 1
```

7.6 ERPS Instance Device Role

【Command】

erps <*NAME*> set role {rpl-owner|neighbor|interconnection|other}

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

【Description】

erps set role: this command is used to specify the role of the ERPS instance in the ring network.

By default, it is other.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set role rpl-owner
```

7.7 ERPS Instance Ring Role

【Command】

erps <*NAME*> set ring-role { major-ring| sub-ring}

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

【Description】

erps set ring-role: this command is used to specify the role of the ERPS instance in the ring network.

By default, it is a major-ring role.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set role-ring major-ring
```

7.8 Major Instance Name of ERPS Instance

【Command】

erps <*NAME*> set major-instance-name <*NAME*>

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS subinstance name.

< NAME >: ERPS major instance name.

【Description】

erps set majority-instance-name: this command is used to set the major instance of ERPS for the specified subinstance of ERPS, and is executed only if the specified instance of ERPS is a subring.

By default, no configuration.

【Instance】

```
Switch> enable
```

```
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set role-ring sub-ring
Switch(config-erps-instance)#erps 1 set major-instance-name 2
```

7.9 ERPS Instance Protocol Message Management VLAN

【Command】

erps <*NAME*> set raps-channel <*vlan*>

no erps <*NAME*> set raps-channel

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

< vlan > : VLAN of raps protocol message, the range is 1-4094.

【Description】

erps set raps-channel: this command is used to set the raps protocol message channel for the erps instance.

By default, it is 0 and invalid VLAN.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set raps-channel 10
```

7.10 ERPS Instance Virtual Channel

【Command】

erps <*NAME*> set virtual-channel {enable|disable}

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

【Description】

erps set ring-role: this command is used to set whether raps protocol massage are going through virtual channels (note: virtual channels are not currently supported). By default, it is default.

【Instance】

-

7.11 ERPS Instance Reverse Mode

【Command】

erps <*NAME*> set revertive {enable|disable}

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

【Description】

erps set revertive: command is used to configure the work mode of ERPS instance, enable is revertive mode and disable is irreversible mode.

By default, it is enable, that is reversible mode.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 set revertive disable
```

7.12 ERPS Instance Force-switch or Manual-switch

【Command】

erps <*NAME*> command { force-Switch| manual-Switch}

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

【Description】

erps command: this command is used to perform forced or manual switch commands of ERPS instance.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 command force-Switch
```

7.13 ERPS Instance Clear Command

【Command】

erps <*NAME*> command clear

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

【Description】

erps command clear: this command is used to configure the ERPS instance to perform the clear command.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 command clear
```

7.14 ERPS Instance Enablement

【Command】

erps <*NAME*> {start|stop}

【View】

ERPS instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

【Description】

erps start|stop: this command is used to start or stop an ERPS instance.

By default, the ERPS instance is in the stop state.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps instance config
Switch(config-erps-instance)#erps creat erps-name 1
Switch(config-erps-instance)#erps 1 start
```

7.15 Enter Ring Instance Configuration View

【Command】

erps ring config

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

erps ring config: this command is used to enter the ERPS ring configuration view.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps ring config
```

7.16 Create Ring Instance Name

【Command】

ring creat ring-name <*NAME*> ring-id <*ring-id*>

no ring creat ring-name <*NAME*>

【View】

ERPS ring instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS ring name.

< ring-id > : ERPS ring ID, the range is1-239.

【Description】

erps creat ring-name: this command is used to create the RING instance and specify the RING name and RING ID.

By default, no configuration.

RING ID will be the last byte of the MAC destination of the raps message.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps ring config
Switch(config-erps-ring)#ring creat ring-name 1 ring-id 1
```

7.17 Ring Instance Interface

【Command】

ring <*NAME*> set east-ifname <*if-name*> west-ifname <*if-name*>

【View】

ERPS ring instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

<if-name>: port name.

【Description】

ring set east-ifname: this command is used to configure the ring port for the specified ring instance.

By default, no configuration.

Notice:

1. ERPS ring ports can be normal physical ports or static aggregation groups.

2. ERPS ring port cannot be opened at the same time with other layer 2 protocols (MSTP, SWRING, etc., when ERPS protection is not 0, it can be opened at the same time with MSTP).

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps ring config
Switch(config-erps-instance)#ring creat ring-name 1
Switch(config-erps-instance)#ring 1 set east-ifname ge1 west-ifname ge2
```

7.18 Ring Instance Network Level

【Command】

ring <*NAME*> set ring-level <*level*>

【View】

ERPS ring instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name.

<level> : ring grade, the range is 1-7.

【Description】

erps set ring-level: this command is used to configure the RING level for the specified RING instance.

By default, the RING level is 1.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps ring config
Switch(config-erps-ring)#ring creat ring-name 1
Switch(config-erps-ring)#ring 1 set ring-level 2
```

7.19 Enter Timer Instance Configuration View

【Command】

erps timer config

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

erps timer config: this command is used to enter the ERPS timer configuration view.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps timer config
```

7.20 Create Timer Instance Name

【Command】

timer creat timer-name <*NAME*>

no timer creat timer-name <*NAME*>

【View】

ERPS timer instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS timer instance name.

【Description】

timer creat timer-name: this command is used to create a timer instance and specify the timer instance name.

By default, no configuration.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps timer config
Switch(config-erps-time)#timer creat timer-name 1
```

7.21 WTB Timer

【Command】

timer <*NAME*> set wtb <*interval*>

【View】

ERPS timer instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS timer instance name.

<interval>: wtb timer value, ranging from 1 to 12min.

【Description】

timer set wtb: this command is used to create the timing cycle of the TIMER instance WTB timer.

By default, it is 5min.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps timer config
Switch(config-erps- time)#timer 1 set wtb 1
```

7.22 WTR Timer

【Command】

timer <*NAME*> set wtr <*interval*>

【View】

ERPS timer instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS timer instance name.

<interval>: wtr timer value, ranging from 1 to 12min.

【Description】

timer set wtr: this command is used to create the timing cycle of the timer instance WTR timer.

By default, it is 5min.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps timer config
Switch(config-erps- time)#timer 1 set wtr 1
```

7.23 GuardTimer

【Command】

timer <*NAME*> set guard <*interval*>

【View】

ERPS timer instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS timer instance name.

<interval>: guard timer value, ranging from 10 to 2000ms.

【Description】

timer set guard: this command is used to create the timing cycle of TIMER instance guard timer.

By default, it is 500ms.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps timer config
Switch(config-erps- time)#timer 1 set guard 1000
```

7.24 HoldTimer

【Command】

timer <*NAME*> set hold <*interval*>

【View】

ERPS timer instance configuration view

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS timer instance name.

<interval> : hold timer value, the range is 0-10s.

【Description】

timer set hold: this command is used to create the timing cycle of TIMER instance hold timer.

By default, it is 0.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#erps timer config
Switch(config-erps- time)#timer 1 set hold 1
```

7.25 Display ERPS Instance Information

【Command】

show {erps <*NAME*>| erps-all}

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS instance name

【Description】

show erps: this command is used to display the ERPS instance information.

【Instance】

```
Switch#show erps 1

---------------ERPS INSTANCE INFORMATION START-----------------
ERPS  Name:1                          ERPS Version:1
ERPS-STATE:ERPS_PROTECTION            Device  Role:NEIGHBOR
InstanceID:0                          Channel Mode:NON-VRITUAL
ERPS  revert  mode:REVERTIVE
Major InstanceName:NULL
R-APS Vlan Channel:10
Data  Vlan Channel:NULL
```

```
WTR    Timer State:Stop
WTB    Timer State:Stop
Guard  Timer State:Stop
Hold   Timer State:Stop
Hello  Timer State:Running
Instance Run State:Running
-----------------RING INSTANCE INFORMATION START---------------
Ring Name:1
East Port:ge2    Port Role:OTHER-PORT           Port State:BLOCK
West Port:ge1    Port Role:RPL-NEIGHBOR-PORT    Port State:BLOCK
Ring   ID:1      Ring Level:1               Ring Role:Major Ring
----------------RING INSTANCE INFORMATION END-------------------
----------------TIMER INSTANCE INFORMATION START----------------
Timer        Name:1
WTR    Timer Value:1 min
WTB    Timer Value:5 min
Guard  Timer Value:10 ms
Hold   Timer value:0 ms
Hello  Timer value:5 s
---------------TIMER INSTANCE INFORMATION END-----------------
----------------ERPS INSTANCE INFORMATION END-----------------
```

7.26 Display Ring Instance Information

【Command】

show erps {ring <*NAME*>| ring-all}

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS ring instance name.

【Description】

show erps ring: this command is used to display the ERPS ring instance information.

【Instance】

```
Switch#show erps ring 1
--------------RING INSTANCE INFORMATION START---------------
Ring Name:1
East Port:ge2     Port Role:OTHER-PORT          Port State:BLOCK
West Port:ge1     Port Role:RPL-NEIGHBOR-PORT     Port State:BLOCK
Ring   ID:1      Ring Level:1               Ring  Role:Major Ring
---------------RING INSTANCE INFORMATION END-----------------
```

7.27 Display Timer Instance Information

【Command】

show erps {timer <*NAME*>| timer-all}

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

< NAME >: ERPS timer instance name.

【Description】

show erps timer: this command is used to display the instance information of the ERPS timer.

【Instance】

```
Switch#show erps timer 1
------------TIMER INSTANCE INFORMATION START------------
Timer        Name:1
WTR    Timer Value:1 min
WTB    Timer Value:5 min
Guard  Timer Value:10 ms
Hold   Timer value:0 ms
Hello  Timer value:5 s
------------TIMER INSTANCE INFORMATION END-------------
```

8 Remote Loop Detection Configuration

GSTP means the remote loop detection function. Switch connect with the client, if the client network has a loop, it will affect the entire network. The GSTP is designed to solve this problem. After the switch port enabled the remote loop detection function, it will periodically broadcast and send detection messages. When the switch port enabled the remote loop detection function, it will periodically broadcast the detection message. If the client network has a loop, the switch will receive detection message sent by itself. The switch will regard client network has loop network and set the ports that connect with client port to discarding or shutdown according to processing strategy.

8.1 Enable configuration

【Command】

```
loop-detect enable
no loop-detect enable
```

【View】

Global configuration mode

【Default Level】

2. Configuration level

【Parameter】

None

【Description】

loop-detect enable: enable loop detection function.

no loop-detect enable: disable loop-detect function.

【Instance】

```
Switch#configure terminal
Switch(config)#loop-detect enable
```

8.2 Port Loopback Detection

【Command】

```
loop-detect force up
loop-detect protect vlan <1-4094>
loop-detect resume time <300-600>
loop-detect tx-interval time <10-300>
```

【View】

Ethernet port configuration mode

【Default Level】

2. Configuration level

【Parameter】

<1-4094> : VLAN ID range 1-4094.

<300-600>: the recovery time of the port, ranging from 300 to 600 seconds.

<10-300> : probe packet detection interval, the range is 10-300 seconds.

【Description】

loop - Detect force up: Forces to open the port closed by the protocol (this command does not save to the disk).

Loop-detect protect vlan <1-4094> : specify protection VLAN and enable port check.

loop-detect resume time <300-600>: Recovery port time.

loop-detect tx-interval time <10-300>: The time interval between sending probe packets.

【Instance】

```
Switch>enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#loop-detect protect vlan 1
```

9 IGMP Configuration

9.1 IGMP Enablement

【Command】

ip igmp

no ip igmp

【View】

VLAN-IF Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

ip igmp: This command is used to enable IGMP on the interface.

no ip igmp: this command is used to disable IGMP on the interface.

By default, IGMP on the interface is disabled.

Configuration of other IGMP features on an interface takes effect only if IGMP is enabled on that interface.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp
```

9.2 IGMP Versions

【Command】

ip igmp version VERSION-NUMBER

no ip igmp version

【View】

VLAN-IF Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

VERSION-NUMBER:: represents the version number of IGMP, and the value range is 1-3.

【Description】

ip igmp version: this command is used to configure the version of IGMP on the interface.

no ip igmp version: this command is used to restore to IGMP default.

By default, the version of IGMP is IGMPv3.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp version 2
```

9.3 The Startup Times of IGMP Querier

【Command】

ip igmp startup-query-count <2-10>

no ip igmp startup-query-count

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

<2-10> : specifies the number of times an IGMP query is started, with a value range of 2-10.

【Description】

ip igmp startup-query-count: this command is used to configure the number of start queries for the IGMP querier on the interface.

no ip igmp startup-query-count: this command is used to restore to the default value.

By default, the number of starts of an IGMP querier is equal to the robustness of the IGMP querier.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp startup-query-count 5
```

9.4 Start Query Interval of IGMP Querier

【Command】

```
ip igmp startup-query-interval <1-18000>
no ip igmp startup-query-interval
```

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

<1-18000> : specifies the start query interval for the IGMP query, in the range 1-18000 in seconds.

【Description】

ip igmp startup-query-interval: this command is used to configure the start query interval for the IGMP query on the interface.

no ip igmp startup-query-interval: this command is used to restore to the default value. By default, the IGMP query starts at a quarter of the time it took to send the IGMP universal group query message. The time interval of sending IGMP universal group query message is 125 seconds, then the start query interval of IGMP querier is 125÷4=31 (seconds).

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp startup-query-interval 20
```

9.5 The Robustness Factor of the IGMP Query

【Command】

```
ip igmp robustness-variable <2-7>
no ip igmp robustness-variable
```

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

<2-7> : specifies the robustness factor of the IGMP query, with a value range of 2-7. This coefficient is used to specify the default value of the number of times an IGMP query message is sent by the IGMP query at startup, and the number of times an IGMP query message is sent by the IGMP query after the IGMP query receives the message leaving the group.

【Description】

ip igmp robustness - variable: this command is used to configure the robustness coefficient of the IGMP query on the interface.

no ip igmp robustness-variable: this command is used to restore to the default value.

By default, the IGMP query has a robustness factor of 2.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp robustness-variable 3
```

9.6 Time Interval of IGMP Universal Group Query Message

【Command】

ip igmp query-interval <1-1800>

no ip igmp query-interval

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

<1-1800> : specifies the time interval between sending IGMP universal group query messages, with a value range of 1-18000, in seconds.

【Description】

ip igmp query-interval: this command is used to configure the interval at which IGMP universal group query messages are sent on the interface.

no ip igmp query-interval: this command is used to restore the default.

By default, IGMP universal group query messages are sent at an interval of 125 seconds.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp query-interval 240
```

9.7 The Lifetime of Other IGMP Queriers

【Command】

ip igmp querier-timeout <60-300>

no ip igmp querier-timeout

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

<60-300> : specifies the duration of the IGMP other queries, in the range of 60-300 in seconds.

【Description】

ip igmp querier-timeout: this command is used to configure the lifetime of IGMP other queries on the interface.

no ip igmp querier-timeout: this command is used to restore to the default value.

By default, the existence time of other IGMP queriers = the time interval of sending IGMP universal group query message × the robustness coefficient of IGMP queriers + the maximum response time of IGMP universal group query ÷2.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp querier-timeout 180
```

9.8 The IGMP Universal Group Queries the Maximum Response Time of Message

【Command】

ip igmp query-max-response-time <1-240>

no ip igmp query-max-response-time

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

<1-240>: specifies the maximum response time of IGMP universal group query message, and the value range is 1-240, in seconds.

【Description】

ip igmp query-max-response-time: this command is used to configure the maximum response time for IGMP universal group queries on the interface.

No ip igmp query-max-response-time: this command is used to restore the default.

By default, the maximum response time of IGMP universal group query messages is 10 seconds.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp query-max-response-time 20
```

9.9 Number of IGMP Query Packets for a Specific Group

【Command】

ip igmp last-member-query-count <2-7>

no ip igmp last-member-query-count

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

<2-7> : specifies the number of query message to send IGMP specific groups, and the value range is 2-7.

【Description】

ip igmp last-member-query-count: this command is used to configure the number of sending query message of IGMP specific groups on the interface.

no ip igmp last-member-query-count: command is used to restore to the default value. By default, the number of sending IGMP specific group query message is 2.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp last-member-query-count 3
```

9.10 The Time Interval of IGMP Specific Group Querying Message

【Command】

```
ip igmp last-member-query-interval <1000-25500>
no ip igmp last-member-query-interval
```

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

<1000-25500> : specifies the time interval for sending IGMP specific group of query messages. The value range is 1000-25500, in milliseconds.

【Description】

ip igmp last-member-query-interval: the command is used to configure the interval at which the IGMP specific group query message is sent on the interface.

no ip igmp last-member-query-interval: the command is used to restore the default.

By default, IGMP specific group query message are sent at an interval of 1000 ms.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp last-member-query-interval 2000
```

9.11 IGMP Message with RA Option

【Command】

ip igmp ra-option

no ip igmp ra-option

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

ip igmp ra-option: this command is used to configure the interface to discard igmp message that do not carry the Router-Alert option.

no ip igmp ra-option: this command is used to restore the default value.

By default, devices do not check for the Router-Alert option, that is, they send all IGMP message they received to the upper protocol for processing, whether or not they carry the Router-Alert option.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp ra-option
```

9.12 Fast Aging ACL Group

【Command】

ip igmp immediate-leave group-list <ACL-NUMBER | ACL-NAME**>**

no ip igmp immediate-leave

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

acl-number: standard acl number, ranging from 1-99 or 1300-1999.

acl-name: extended acl name.

【Description】

ip igmp immediate-leave group-list: the command is used to configure the acl group address range of fast leave. The acl action must be permit.

no ip igmp immediate-leave: the command is used to restore to the default value.

By default, when the interface is working on version 2 and version 3, upon receiving the igmp leave message, a group-specific query message is sent to determine whether to age the multicast member table entry. Once this capability is configured, the multicast member table entry can be aged immediately if the group address specified by the acl is within the group address specified by the acl.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 1300 permit 225.1.1.0 0.0.0.255
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp immediate-leave group-list 1300
```

9.13 Illegal Multicast Group

【Command】

ip igmp access-group <ACL-NUMBER **|** ACL-NAME**>**

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

acl-number: standard acl number, the value range is 1-99.

acl-name: extended acl name.

【Description】

Ip igmp access-group: this command is used to configure an invalid multicast group range. The action of the acl must be deny, and if the action is permit, mismatched multicast groups are considered legitimate.

no ip igmp access-group: the command is used to remove illegal multicast group range restrictions.

By default, the range of multicast groups that an interface can learn is unrestricted.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 1300 deny 225.1.1.0 0.0.0.255
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp access-group 1300
```

9.14 Multicast Group Number Limit

【Command】

```
ip igmp limit VALUE [except <ACL-NUMBER | ACL-NAME > ]
no ip igmp limit
```

【View】

Global configuration mode

VLAN-IF interface configuration view

【Default Level】

2: Configuration level

【Parameter】

value: the maximum number of multicast groups allowed to be added by the global or interface, ranging from 1-1024.

acl-number: standard acl number, the value range is 1-99.

acl-name: extended acl name.

【Description】

ip igmp limit: this command is used to configure the maximum number of multicast groups that are allowed to be added to the global or interface.

no ip igmp limit: this command is used to restore to the default value. In the process of working, the device first determines whether it exceeds the global limit, then determines whether it exceeds the interface limit, or ignores the new multicast group learning.

An acl of type permit can be referenced by the except parameter, indicating that there are no restrictions on the number of multicast groups within the range specified by the acl.

By default, there is no limit to the number of multicast groups that can be added to a global or interface.

 Notice

When the configured limit value is less than the number of established multicast groups on the global or current interface, the system will not automatically delete the additional multicast groups.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#ip igmp limit 1000
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp limit 100
```

9.15 IGMP Message Source Address and Receive Interface Subnet Restrictions

【Command】

ip igmp offlink

no ip igmp offlink

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

ip igmp offlink: this command is used to remove the restriction that the source address of an igmp message must be in the same subnet as the receiving interface, except for querying message and leaving message.

no ip igmp offlink: this command is used to restore to the default value.

By default, the source address of an igmp message must be on the same subnet as the receiving interface. Once the restriction is removed, the source address of the message will be considered valid as long as it passes RPF check.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp offlink
```

9.16 Static Multicast Group

【Command】

ip igmp static-group <group-address> [source <source-address> | ssm-map]

no ip igmp static-group <group-address> [source <source-address> | ssm-map]

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

group-address: specify multicast group address with values ranging from 224.0.1.0 to 239.255.255.255.

source-address: specifies the address of the multicast source.

ssm-map: obtain the address of multicast source by ssm-mapping function

【Description】

ip igmp static- group: This command is used to configure the interface to statically join a multicast group or multicast source group.

no ip igmp static-group: this command is used to restore to the default value. By default, the interface does not statically join any multicast group or multicast source group.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp static 225.1.1.1 source 192.168.1.10
```

9.17 Global IGMP SSM Mapping Enablement

【Command】

ip igmp ssm-map enable

no ip igmp ssm-map enable

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

ip igmp ssm-map enable: this command is used to enable the IGMP SSM Mapping function globally.

no IP igmp ssm-map enable: this command is used to disable the global IGMP SSM Mapping function.

By default, the IGMP SSM Mapping function is disabled.

IGMPv1/IGMPv2 cannot specify the multicast source in the report message, so IGMP SSM Mapping technology is required for compatibility. This feature provides SSM services for the interface that receives vesion1 and version2 igmp report packets, with the source address specified by the ip igmp ssm-map static command.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#ip igmp ssm-map enable
```

9.18 IGMP SSM-Map Static Multicast

【Command】

ip igmp ssm-map static <ACL-NUMBER | ACL-NAME> <SOURCE-ADDRESS>

no ip igmp ssm-map static <ACL-NUMBER | ACL-NAME> <SOURCE-ADDRESS>

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

acl-number: standard acl number, ranging from 1 ~ 99 or 1300 ~ 1999.

acl-name: extended acl name.

source-address: the static mapping source address for SSM mapping.

【Description】

Ip igmp ssm-map static: this command is used to configure the IGMP SSM Mapping rule.

no ip igmp ssm-map: this command is used to delete the IGMP SSM Mapping rule.

IGMP SSM Mapping rules are not configured by default.

IGMPv1/IGMPv2 cannot specify the multicast source in the report message, so IGMP SSM Mapping technology is required for compatibility. This feature needs to work with ip igmp ssm-map enable.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 1300 deny 225.1.1.0 0.0.0.255
Switch(config)#ip igmp ssm-map enable
Switch(config)#ip igmp ssm-map static 1300 192.168.1.10
```

9.19 Display IGMP Multicast Information

【Command】

```
show ip igmp groups [<IFNAME> | <GROUP-ADDRESS> | detail ]
```

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

ifname: vlanif interface.

group-address: ipv4 multicast address.

detail: outputs the details of the multicast group.

【Description】

View the running condition of the specified parameter or the entire multicast group.

【Instance】

```
Switch#show ip igmp groups detail
IGMP Connected Group Membership, Total is 1
```

```
Interface:     vlanif1
Group:       255.1.1.1
Uptime:      01:09:31
Group mode:   Exclude (Expires: 00:03:56)
Last reporter:   192.168.1.11
Source list is empty
```

9.20 Displays IGMP Interface Information

【Command】

show ip igmp inteface <IFNAME**>**

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

Ifname: vlanif interface

【Description】

View the configuration and operation of the interface with the specified parameters or all igmp enabled.

【Instance】

```
Switch#show ip igmp interface vlanif1
Interface vlanif1 (Index 3)
 IGMP Enabled, Active, Querier, Configured for version 2
 L3 mcast is not enabled on this interface
 Internet address is 192.168.1.254
 IGMP interface has 1 group-record states
 IGMP activity: 54 joins, 0 leaves
 IGMP query interval is 125 seconds
 IGMP Startup query interval is 31 seconds
 IGMP Startup query count is 2
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
```

```
IGMP Last member query count is 2
L2 mcast is not enabled on this interface
IGMP Snooping is globally disabled
IGMP Snooping is not enabled on this interface
IGMP Snooping fast-leave is not enabled
IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
```

10 IGMP Snooping Configuration

10.1 IGMP SnoopingEnablement

【Command】

```
ip igmp snooping
no ip igmp snooping
```

【View】

Global configuration mode

VLAN-IF interface configuration view

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

ip igmp snooping: this command is used to enable IGMP snooping on global or VLAN interfaces.

no ip igmp snooping: this command is used to disable igmp snooping on the global or VLAN interface.

IGMP snooping is disabled by default on the global or VLAN interfaces.

Notice

Only when IGMP snooping is enabled on the global and VLAN interfaces can the configuration of the other IGMP snooping properties on that interface take effect.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp snooping
```

10.2 IGMP Snooping Querier Enablement

【Command】

ip igmp snooping querier

no ip igmp snooping querier

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

ip igmp snooping querier: this command is used to enable IGMP Snooping querier.

no ip igmp snooping querier: this command is used to disable IGMP Snooping querier.

By default, the IGMP Snooping querier is disabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp snooping querier
```

10.3 IGMP Snooping Port Fast-leave Enablement

【Command】

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

ip igmp-snooping fast-leave: this command is used to enable the fast leave function on all ports of the VLAN interface. Port fast leave means that when the switch receives the IGMP leaving a multicast group message sent by the host from a port, the port is directly deleted from the list of outgoing ports of the corresponding forwarding item.

no ip igmp-snooping fast-leave: this command is used to disable the fast leave function on all ports of the VLAN interface.

By default, the fast leave function of the port is disabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp snooping fast-leave
```

10.4 IGMP SnoopingPort Suppression Enablement

【Command】

ip igmp snooping report-suppresstion

no ip igmp snooping report-suppresstion

【View】

VLAN-IF Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

ip igmp snooping report-suppresstion: this command is used to enable port reporting suppression on all ports of the VLAN interface. When the port is in IGMPv1 or IGMPv2, when receiving the leave message, if the port report suppression function is enabled, the report message will not be sent.

no ip igmp-snooping report-suppresstion command: this command is used to disable port reporting suppression on all ports of the VLAN interface.

By default, port report suppression is disabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip igmp snooping report-suppresstion
```

10.5 Display the IGMP Snooping Multicast Group Routing Interface

【Command】

show ip igmp snooping mrouter inteface <IFNAME>

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

Ifname: vlanif interface

【Description】

View the multicast group routing port of the specified interface

【Instance】

```
Switch#show ip igmp snooping mrouter interface vlanif1
VLAN     interface
1        ge2
```

10.6 Display IGMP SnoopingMulticast Statistics

【Command】

show ip igmp snooping statistics inteface <IFNAME>

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

Ifname: vlanif interface

【Description】

View the multicast group statistics of the specified interface

【Instance】

-

11 GMRP and MMRP Configuration

As a carrier of an Attribute Registration Protocol, GARP (Generic Attribute Registration Protocol) can be used to propagate attributes. Application entities that follow the GARP protocol are called GARP applications,

GMRP(GARP Multicast Registration Protocol) is one of the applications of the generic property Registration Protocol (GARP) to provide a limited Multicast diffusion capability similar to IGMP probe technology.

As the carrier of an attribute registration protocol, MRP (Multiple Register Protocol) can be used to propagate attribute messages. The application entity following MRP Protocol is called MRP application. MVRP (Multiple VLAN Register Protocol) is one of the applications of MRP. MRP, MVRP and MMRP are the upgraded versions of GARP (Generic Attribute Registration Protocol), GVRP (GARP VLAN Registration Protocol) and GMRP(GARP Multicast Registration Protocol) respectively, which improve the efficiency of Attribute declaration and are used to replace GARP, GVRP, GMRP protocol. MVRP is used to publish and learn VLAN configuration information between devices, so that devices can automatically synchronize VLAN configuration and reduce the configuration work of network administrators. After the network topology changes, MVRP reissues and learns the VLAN according to the new topology, so as to update the network topology synchronously in real time.

11.1 Global GMRP or MMRP Enablement

【Command】

```
(gmrp | mmrp) (enable | disable)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

(gmrp | mmrp) enable: this command is used to enable the global GMRP (MMRP) function.

(gmrp | mmrp) disable: this command is used to disable the global GMRP（MMRP） function.

By default, the global GMRP（MMRP） is disabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#gmrp enable
```

11.2 Port GMRP or MMRP Enablement

【Command】

```
(gmrp | mmrp) (enable | disable)
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

port (gmrp | mmrp) enable: this command is used to enable the GMRP (MMRP) function of the port.

port (gmrp | mmrp) disable: this command is used to disable the GMRP（MMRP） function of the port.

By default, the GMRP（MMRP）function of the port is disabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#gmrp enable
Switch(config)#interface ge5
Switch(config-ge5)#gmrp enable
```

11.3 GMRP or MMRP Registration Mode

【Command】

(gmrp | mmrp) registration (fixed| forbidden | normal | restricted)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

fixed: Fixed mode.

forbidden: Forbidden mode.

normal: Normal mode, allowing registering and deregistering multicast dynamically.

restricted: Restricted mode.

【Description】

(gmrp | mmrp) registration: this command is used for GMRP port registration mode.

By default, the GMRP port registration mode is normal.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#gmrp enable
Switch(config)#interface ge5
Switch(config-ge5)#gmrp registration normal
```

11.4 GMRP or MMRP Timer

【Command】

(gmrp | mmrp) timer (join| leave| leaveall) <TIMER_VALUE>

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

leaveall | join | leave: represent leave All, join and leave three timers respectively. After GARP is started on each port and LeaveAll timer is started at the same time, the port will send LeaveAll messages to the outer loop to cause the other ports to re-register all their property information. GARP port can send out each Join packet twice to ensure the reliable transmission of message, and the time interval between the two times is controlled by Join timer. The GARP port that receives the Leave packet enable the Leave timer, and if the Join packet is not received before the timer timeout, the corresponding attribute information will be logged out.

<TIMER_VALUE> : timer value, leave All defaults to 1000; The default value for join is 20; The default value for leave is 60. Unit: centiseconds.

【Description】

(gmrp | mmrp) timer: this command is used to configure leave All, join, and leave timers of the GARP ports.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#gmrp enable
Switch(config)#interface ge5
Switch(config-ge5)#gmrp timer leave 100
```

11.5 Display GMRP or MMRP Configuration Information

【Command】

show (gmrp | mmrp) configuration

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show gmrp | mmrp configuration: this command is used to display GMP| MMRP configuration information.

【Instance】

***Switch#show gmrp configuration**

11.6 Display GMRP or MMRP State Machine Information

【Command】

show (gmrp | mmrp) machine

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show gmrp | mmrp machine command: this command is used to display GMRP| MMRP state machine information.

【Instance】

```
Switch> enable
Switch#show gmrp machine
```

11.7 Display GMRP or MMRP Message Statistics

【Command】

show (gmrp | mmrp) statistics vlanid [<VLANID>]

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

vlanid: VLAN ID.

【Description】

show gmrp | mmrp statistics: this command is used to display GMRP| MMRP message statistics.

【Instance】

```
Switch> enable
Switch#show gmrp statistics vlanid 3
```

11.8 Display GMRP or MMRP Timer Information

【Command】

show (gmrp | mmrp) timer <IFNAME>

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

Ifname: port name.

【Description】

show gmrp | mmrp timer: this command is used to display the GMRP| MMRP port timer information.

【Instance】

```
Switch> enable
Switch#show gmrp timer ge2
```

12 GVRP and MVRP Configuration

As a carrier of an Attribute Registration Protocol, GARP (Generic Attribute Registration Protocol) can be used to propagate attributes. Application entities that follow the GARP protocol are called GARP applications,GVRP (GARP VLAN Registration Protocol) is one of the applications of the common property Registration Protocol (GARP) for VLAN properties login and logout.

As the carrier of an attribute registration protocol, MRP (Multiple Register Protocol) can be used to propagate attribute messages. The application entity following MRP Protocol is called MRP application. MVRP (Multiple VLAN Register Protocol) is one of the applications of MRP. MRP, MVRP and MMRP are the upgraded versions of GARP (Generic Attribute Registration Protocol), GVRP (GARP VLAN Registration Protocol) and GMRP(GARP Multicast Registration Protocol) respectively, which improve the efficiency of Attribute declaration and are used to replace GARP, GVRP, GMRP protocol. MVRP is used to publish and learn VLAN configuration information between devices, so that devices can automatically synchronize VLAN configuration and reduce the configuration work of network administrators. After the network topology changes, MVRP reissues and learns the VLAN according to the new topology, so as to update the network topology synchronously in real time.

12.1 Global GVRP or MVRP Enablement

【Command】

```
(gvrp | mvrp) (enable | disable)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

(gvrp | mvrp) enable: this command is used to enable the global GVRP (MVRP) function.

(gvrp | mvrp) disable: this command is used to disable the global GVRP (MVRP) function.

By default, the global GVRP (MVRP) function is disabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#gvrp enable
```

12.2 GVRP or MVRP Dynamic VLAN Enablement

【Command】

(gvrp | mvrp) dynamic-vlan-creation (enable | disable)

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

(gvrp | mvrp) dynamic-vlan-creation enable: this command is used to enable the dynamic creation of VLAN functions.

(gvrp | mvrp) dynamic-vlan-creation disable: this command is used to disable the dynamic creation of VLAN functions.

By default, the dynamic creation VLAN feature is disabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#gvrp enable
Switch(config)#gvrp dynamic-vlan-creation enable
```

12.3 Port GVRP or MVRP Enablement

【Command】

(gvrp | mvrp) (enable | disable)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

port (gvrp | mvrp) enable: this command is used to enable port GVRP (MVRP) function.

port (gvrp | mvrp) disable: this command is used to disable the GVRP（MVRP）function.

By default, the GVRP（MVRP）function of the port is disabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#gvrp enable
Switch(config)#gvrp dynamic-vlan-creation enable
Switch(config)#interface ge5
Switch(config-ge5)#gvrp enable
```

12.4 GVRP or MVRP Registration Mode

【Command】

(gvrp | mvrp) registration (fixed| forbidden | normal)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

fixed: Fixed mode, no dynamic VLAN registration on the port, only static VLAN declaration messages are sent.

forbidden: Forbidden mode, does not allow dynamic VLAN to register on the port, simultaneously deletes all VLANs except VLAN 1 on the port, only sends VLAN 1 declaration message.

normal: normal mode, which allows dynamic VLANs to be registered on the port and simultaneously sends both static and dynamic VLAN declaration messages.

【Description】

(gvrp | mvrp) registration: this command is used for the GVRP port registration mode. By default, the GVRP port registration mode is normal.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#gvrp enable
Switch(config)#interface ge5
Switch(config-ge5)#gvrp registration normal
```

12.5 GVRP or MVRP Timer

【Command】

(gvrp | mvrp) timer (join| leave| leaveall) <TIMER_VALUE>

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

leaveall | join | leave: represent leave All, join and leave three timers respectively. After GARP is started on each port and LeaveAll timer is started at the same time, the port will send LeaveAll messages to the outer loop to cause the other ports to re-register all their property information. GARP port can send out each Join packet twice to ensure the reliable transmission of message, and the time interval between the two times is controlled by Join timer. The GARP port that receives the Leave packet enable the Leave timer, and if the Join packet is not received before the timer timeout, the corresponding attribute information will be logged out.

<TIMER_VALUE> : timer value, leave All defaults to 1000; The default value for join is 20; The default value for leave is 60. Unit: centiseconds.

【Description】

(gvrp | mvrp) timer: this command is used to configure leave All, join, and leave timers of the GARP ports.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#gvrp enable
Switch(config)#interface ge5
Switch(config-ge5)#gvrp timer join 10
```

12.6 Display Dynamic VLAN Information

【Command】

show vlan dynamic

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show vlan dynamic: this command is used to display dynamic vlan information.

【Instance】

```
Switch> enable
Switch#show vlan dynamic
```

12.7 Display GVRP or MVRP Configuration Information

【Command】

```
show (gvrp | mvrp) configuration
```

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show gvrp | mvrp configuration: this command is used to display GVRP| MVRP configuration information.

【Instance】

```
Switch> enable
Switch#show gvrp configuration
```

12.8 Display GVRP or MVRP State Machine Information

【Command】

show (gvrp | mvrp) machine

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show gvrp | mvrp machine: this command is used to display GVRP| MVRP state machine information.

【Instance】

```
Switch> enable
Switch#show mvrp machine
```

12.9 Display GVRP or MVRP Message Statistics

【Command】

show (gvrp | mvrp) statistics [<IFNAME>]

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

Ifname: port name.

【Description】

show gvrp | mvrp statistics: this command is used to display GVRP| MVRP message statistics.

【Instance】

```
Switch> enable
Switch#show mvrp statistics
```

12.10Display GVRP or MVRP Timer Information

【Command】

show (gvrp | mvrp) timer <IFNAME>

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

Ifname: port name.

【Description】

show gvrp | mvrp timer: this command is used to display timer information of GVRP| MVRP port .

【Instance】

```
Switch> enable
Switch#show mvrp time ge1
```

13 DHCP Configuration

13.1 Global DHCP Service Enablement

【Command】

ip dhcp service

no ip dhcp service

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

No.

【Description】

ip dhcp service: command is used to globally enable the dhcp server service.

【Instance】

```
#Configure to enabled DHCP server service globally
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
```

13.2 Interface DHCP Relay Address

【Command】

ip dhcp relay-to <*A.B.C.D*>

no ip dhcp relay-to [<*A.B.C.D*>]

【View】

Layer 3 Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D: dhcp server IP address.

【Description】

This command is in the Interface view and only configure the corresponding Interface relay and dhcp server IP addresses.

ip dhcp relay-to <A.B.C.D>: the command is used to set the dhcp server ip address required by the relay. This command can be executed repeatedly to configure multiple server IP addresses, which up to 9 relay servers can be configured.

no ip dhcp relay-to [<A.B.C.D>]: used to delete a relay server ip address, the function is opposite to ip dhcp relay-to <A.B.C.D>; With no parameter, the command deletes all relay server ip addresses of the corresponding interface.

【Instance】

```
Configure the dhcp relay server IP address for vlanif 1,the
parameter IP address is 192.168.1.1
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip dhcp relay enable
Switch(config-vlanif1)#ip dhcp relay-to 192.168.1.1

# Remove the DHCP relay server address with IP of 192.168.1.1 under
vlanif 1
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
```

```
Switch(config-vlanif1)#no ip dhcp relay-to 192.168.1.1

# Remove all the dhcp relay server address under vlanif 1
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#no ip dhcp relay-to
```

13.3 DHCP Option82 Enablement

【Command】

ip dhcp option

no ip dhcp option

【View】

Layer 3 Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

None.

【Description】

Ip dhcp option: enable the option 82 function of dhcp relay, and enable the relay message sent by the relay process to carry option 82.

no ip dhcp option: disable option 82 function of dhcp relay.

【Instance】

```
For vlanif1 interface, enable option 82 function of dhcp relay
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip dhcp relay enable
Switch(config-vlanif1)#ip dhcp option
For vlanif1 interface, enable option 82 function of dhcp relay
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#no ip dhcp option
```

13.4 Treatment Strategy of DHCP Option82

【Command】

ip dhcp relay-information policy （append | discard | replace | untouched ）

no ip dhcp relay-information policy

【View】

Layer 3 Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

append: configure the option check policy as Append.

discard: configure the option check policy as Discard.

replace: configure the option check policy as Replace.

untouched: configure the option check policy as Untouched.

【Description】

ip dhcp relay-information policy <append | discard | replace | untouched >: set an option processing policy of dhcp relay, the relay process will process the received dhcp message with option 82 according to the policy.

no ip dhcp relay-information policy: disable the option processing strategy of dhcp relay, strategy will restore to the default strategy, namely only forward received dhcp message with the option 82 (Untouched).

【Instance】

```
# configure option 82 with the policy replace for vlanif1 port.
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip dhcp relay enable
Switch(config-vlanif1)#ip dhcp option
Switch(config-vlanif1)#ip dhcp relay-to 192.168.1.1
Switch(config-vlanif1)#ip dhcp relay-information policy replace

#Disable option 82 policy on port vlanif1.
Switch> enable
```

```
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#no ip dhcp relay-information policy
```

13.5 Relay Identity of DHCP Option82

【Command】

ip dhcp relay-information circuitid (basic | string OPTION**)**

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

Basic: configure sub option circuited is the base (default) configuration.

String: configure sub option circuited as the string given by option.

【Description】

ip dhcp relay-information circuitid (basic | string OPTION): Set the value of option82 suboption circuitid of DHCP relay.

【Instance】

```
#Configure the value of suboption circuited of option 82 is the
string "vlan2:ge10" for vlanif1 port.
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip dhcp relay enable
Switch(config-vlanif1)#ip dhcp option
Switch(config-vlanif1)#ip dhcp relay-information circuitid string
vlan2:ge10
```

13.6 Remote Identity of DHCP Option82

【Command】

ip dhcp relay-information remoteid (basic | string OPTION)

【View】

Layer 3 Interface Configuration View

【Default Level】

2: Configuration level

【Parameter】

Basic: configure sub option remoteid is the base (default) configuration.

String: configure sub option remoteid as the string given by option.

【Description】

ip dhcp relay-information remoteid (basic | string OPTION): Set the value of option82 suboption remoteid of DHCP relay.

【Instance】

```
Configure the value of sub option circuited of option 82 is the
string "00:11:22:33:44:55” for vlanif1 port.
Switch> enable
Switch#configure terminal
Switch(config)#interface vlanif1
Switch(config-vlanif1)#ip dhcp relay enable
Switch(config-vlanif1)#ip dhcp option
Switch(config-vlanif1)#ip dhcp relay-information remoteid string
00:11:22:33:44:55
```

13.7 Create DHCP Address Pool

【Command】

ip dhcp pool <WORD>

no ip dhcp pool <WORD>

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

WORD: the name of dhcp address pool

【Description】

ip dhcp pool: the command is used to create the dhcp address pool.

no ip dhcp pool: the command is used to delete the dhcp address pool.

【Instance】

```
#Create a dhcp address pool named "test" :
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#

#Delete a dhcp address pool named "test" :
Switch> enable
Switch#configure terminal
Switch(config)#no ip dhcp pool test
```

13.8 DHCP Address Pool Subnet Segment

【Command】

network (<A.B.C.D A.B.C.D>/<A.B.C.D/M>)

no network

【View】

DHCP Configuration View

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D: IP address & mask, used to represent subnet segments.

A.B.C.D/M: IP address and mask,used to represent subnet segments.

【Description】

Network:: configure the subnet segment of DHCP pool , among which the parameters give the specific subnet segment value.

no network: deletes the subnet segment configuration of a specified DHCP pool.

【Instance】

```
#Configure network for address pool "test”
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.1.1 255.255.255.0
Switch(dhcp-config)#network 192.168.1.1/24

#Delete network configuration of address pool "test”
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no network
```

13.9 Default Route of DHCP Address Pool

【Command】

default-router A.B.C.D

no default-router

【View】

dhcp View

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D: The default routing address used by dhcp.

【Description】

default-router: configure the default routing IP address of DHCP pool.

no default-router: delete the default routing configuration of DHCP pool.

【Instance】

```
#Configure the default route to 192.168.1.1 of dhcp pool test
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
```

```
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.1.1 255.255.255.0
Switch(dhcp-config)#default-router 192.168.1.1

#delete the default routing configuration of dhcp pool test
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no default-router 192.168.1.1
```

13.10 DHCP Address Pool

【Command】

```
range  <A.B.C.D A.B.C.D>
no range (<A.B.C.D A.B.C.D>|)
```

【View】

dhcp View

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D A.B.C.D: The lowest and highest addresses of dhcp pool.

【Description】

range: configure the address range of DHCP pool, that is, the addresses that belong to the range can be allocated effectively by DHCP.

no range: delete the address range of DHCP pool. If no range parameters are given, delete all range configurations.

【Instance】

```
Configuration the address range of dhcp pool test to: 192.168.1.10
192.168.1.20
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.1.1 255.255.255.0
Switch(dhcp-config)#range  192.168.1.10 192.168.1.20
```

```
Delete the address range of dhcp pool test: 192.168.1.10
192.168.1.20
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no range 192.168.1.10 192.168.1.20

Delete all the address range of dhcp pool test:
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no range
```

13.11 The Lease Time of DHCP Address Pool

【Command】

lease-time <0-30> <0-24> <0-60>

no lease-time

【View】

dhcp View

【Default Level】

2: Configuration level

【Parameter】

<0-30> : days.

<0-24> : hours.

<0-60> : minutes.

【Description】

lease-time: configure the address lease duration of dhcp pool. When the IP address obtained by the dhcp client is about to reach the lease duration, it is necessary to renew the lease. Otherwise, the IP address will be invalid, and the dhcp client needs to re-request the IP address.

no lease-time: delete the address lease duration configuration of dhcp pool and restore the lease duration to the default value.

【Instance】

```
#set the lease-time of dhcp pool test to 30 minutes.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.1.1 255.255.255.0
Switch(dhcp-config)#lease-time 0 0 30

# set the lease-time of dhcp pool test.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no lease-time
```

13.12 The Threshold of DHCP Address Pool

【Command】

threshold <1-254>

no threshold

【View】

dhcp View

【Default Level】

2: Configuration level

【Parameter】

<1-254> : threshold value.

【Description】

threshold: threshold value to configure dhcp pool.

no threshold: Delete the threshold value of DHCP pool (that is, restore to the default value).

【Instance】

```
# set the threshold of dhcp pool test to 8.
Switch> enable
```

```
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#network 192.168.1.1 255.255.255.0
Switch(dhcp-config)#threshold 8

# set the threshold of dhcp pool test.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no threshold
```

13.13 MAC Binding Configuration

【Command】

static A.B.C.D MAC

no static A.B.C.D

【View】

dhcp View

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D: IP address

MAC: MAC address

【Description】

static A.B.C.D MAC: Configure static ip address binding for MAC addresses.

no port-bind PORT: deletes the static ip address binding of mac address.

【Instance】

```
# set dhcp pool test; ; configure the Ip address of d536.cf3a.de34
to 192.168.1.56.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
```

```
Switch(dhcp-config)# network 192.168.1.1 255.255.255.0
Switch(dhcp-config)# static 192.168.1.56 d536.cf3a.de34

#delete the ip address binding of 92.168.1.56 in dhcp pool test.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no static 192.168.1.56
```

13.14Port Binding Configuration

【Command】

port-bind PORT A.B.C.D

no port-bind PORT

【View】

dhcp View

【Default Level】

2: Configuration level

【Parameter】

Port: layer 3 port

A.B.C.D: IP address

【Description】

port-bind PORT A.B.C.D: Configure the port binding of ip addresses, that is, dhcp requests received on a given port are assigned with fixed ip addresses.

no port-bind PORT: deletes the ip address of the port binding.

【Instance】

```
#set dhcp pool test; Configure the ip address binding of vlanif1
to 192.168.1.56.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)# network 192.168.1.1 255.255.255.0
Switch(dhcp-config)# port-bind vlanif1 192.168.1.56
```

```
#delete ip address binding of vlanif1 in dhcp pool test.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp pool test
Switch(dhcp-config)#no port-bind vlanif1
```

13.15DNS Server Address

【Command】

ip dhcp dns-server <A.B.C.D> [<A.B.C.D>] [<A.B.C.D>]

no ip dhcp dns-server

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

< A.B.C.D>: dns server ip address.

【Description】

ip dhcp dns-server: configure dns servers for all dhcp pools, up to three different dns servers can be configured (this configuration is global).

no ip dhcp dns-server: delete all dns server configurations.

【Instance】

```
# set the DNS -serve of DHCP pool to 114.114.114.114 8.8.8.8.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp dns-server 114.114.114.114 8.8.8.8

Remove all dns-serve configurations.
Switch> enable
Switch#configure terminal
Switch(config)#no ip dhcp dns-server
```

13.16 Log Server Address

【Command】

ip dhcp log-server <A.B.C.D> [<A.B.C.D>] [<A.B.C.D>]

no ip dhcp log-server

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

< A.B.C.D>: log server ip address.

【Description】

ip dhcp log-server: configure log servers for all dhcp pools, up to three different log servers can be configured (this configuration is global).

no ip dhcp log-server: delete all log server configurations.

【Instance】

```
# set the log-server of dhcp pool to 192.168.1.1 192.168.1.2
192.168.1.3.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp dns-server 192.168.1.1 192.168.1.2
192.168.1.3

#Remove all log-server configurations.
Switch> enable
Switch#configure terminal
Switch(config)#no ip dhcp log-server
```

13.17 WINS Server Address

【Command】

ip dhcp wins-server <A.B.C.D> [<A.B.C.D>] [<A.B.C.D>]

no ip dhcp wins-server

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

< A.B.C.D>: wins server ip address.

【Description】

ip dhcp wins-server: configure wins servers for all dhcp pools, up to three different wins servers can be configured (this configuration is global).

no ip dhcp win-server: delete all winserver configurations.

【Instance】

```
# configure the wins-server of dhcp pool to be 192.168.1.1
192.168.1.2 192.168.1.3.
Switch> enable
Switch#configure terminal
Switch(config)#ip dhcp service
Switch(config)#ip dhcp wins-server 192.168.1.1 192.168.1.2
192.168.1.3

#Delete all wins-server configurations.
Switch> enable
Switch#configure terminal
Switch(config)#no ip dhcp wins-server
```

13.18Display DHCP Information

【Command】

```
show ip dhcp global
show ip dhcp lease ((interface [IFNAME]) | (summary [IFNAME]))
show ip dhcp pool [WORD]
show ip dhcp relay [IFNAME]
show ip dhcp statistics [IFNAME]
show ip dhcp status
```

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

[IFNAME]: interface name.

[WORD]: address pool identification.

【Description】

show ip dhcp global: view DHCP global information.

show ip dhcp lease: view DHCP lease information.

show ip dhcp pool: view DHCP address pool information.

show ip dhcp relay: view DHCP relay information.

show ip dhcp statistics: view DHCP statistics information.

show ip dhcp status: view DHCP status information.

【Instance】

```
Switch#show ip dhcp status
Interface       IP Address      DHCP Status
-----------------------------------------------
vlanif1         192.168.1.254   DHCP Relay
-----------------------------------------------
```

14 SNMP Configuration

14.1 SNMP Enable

【Command】

snmp-server enable traps

no snmp-server enable traps

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

snmp-server enable traps: command is used to enable SNMP server.

no snmp-server enable: command is used to disable SNMP server.

By default, SNMP function is enabled.

【Instance】

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

14.2 SNMP View

【Command】

snmp-server view VIEWNAME OID (included | excluded)

no snmp-server view VIEWNAME OID

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

VIEWNAME: the view name, with a value range of 1-32 bytes.

OID: OID MIB subtree of MIB object subtree, variable OID only allows digital input (such as 1.3.6.1).

Included: means that this MIB view includes the MIB subtree.

excluded: means that this MIB view excludes the MIB subtree.

【Description】

snmp-server view: command is used to create or update information about the MIB view to restrict the MIB objects that can be accessed by the NMS.

no snmp-server view: the command is used to cancel the current configurations.

The MIB is a collection of managed objects, and the MIB view is a subset of the MIB, and the user can bind the community name/user name to the MIB view to restrict the MIB objects that can be accessed by the NMS. The user can configure the MIB object to excluded or included within the view. Excluded means that the current view does not include all the modes of the MIB subtree; Included means that the current view includes all nodes of the MIB subtree.

By default, the view name is system. The OID included is 1.3.6.1.

SNMP community name or group name configuration needs to determine the MIB view permissions of the community name or group, related configuration can refer to the command snmp-server community, snmp-server group.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#snmp-server view viewname 1.3.6.1.5 included
```

```
Switch(config)#no snmp-server view viewname 1.3.6.1.5
```

14.3 SNMP Community Name

【Command】

```
snmp-server community NAME {view VIEWNAME| } (ro | rw)
no snmp-server community {COMMUNITYNAME | }
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

NAME: the team name, with a value range of 1-32 bytes.

View: MIB view name, this parameter is optional, if not entered, by default it is the default view.

ro: read only means read-only access to MIB objects. Communities with read-only access can only view device information.

rw: read and write indicates read and write access to MIB objects, and communities with read and write permissions can configure devices.

【Description】

snmp-server community: command is used to set the community name, SNMP v1/v2c version uses the group name to restrict access rights. This command can be used to configure the group name, read or write view rights and access control policies. **no snmp-server community**: command is used to cancel group access name settings.

Normally, "public" is used as the name of the read permission group. For security reasons, it is recommended that network administrators configure other community names.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#snmp-server community communityname view viewname
rw
```

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

14.4 SNMP Group

【Command】

```
snmp-server group NAME v3 (auth | noauth | priv ) { notify | read
| write } VIEWNAME
no snmp-server group NAME v3 (auth | noauth | priv )
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

NAME: the group name, with a value range of 1-32 bytes.

v3: SNMP v3 version.

Auth: indicates that the message is authenticated but not encrypted.

noauth: indicates that the message is neither authenticated nor encrypted.

Priv: indicates that the message is authenticated and encrypted.

VIEWNAME: view name, ranging from 1 to 32 bytes. By default, the Trap message view is not configured, meaning that the Agent does not send Traps to the NMS.

Read: specifies the read view of the group.

write: specifies the write and read view of the group.

VIEWNAME: view name

【Description】

snmp-server group: command is used to configure a new SNMP group and set the secure mode and corresponding SNMP view of the SNMP group.

no snmp-server group: command is used to delete a specified SNMP group. For SNMP v3, the group name and the security mode (authentication or not, encryption or not) together determine a group, with the same group name but different security mode are two different groups.

This system defaults to snmp v2, so there is no default configuration for group. If the view name for read is not specified in the command, it defaults to the default view.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#snmp-server group groupname v3 priv read viewname
write viewname
Switch(config)#no snmp-server group groupname v3 priv
```

14.5 SNMP User

【Command】

```
snmp-server user USERNAME GROUPNAME
snmp-server user USERNAME GROUPNAME v3
snmp-server user USERNAME GROUPNAME v3 auth md5 MD5
snmp-server user USERNAME GROUPNAME v3 auth md5 MD5 priv ( aes |
des) pasword
no snmp-server user USERNAME GROUPNAME v3
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

USERNAME: user name, ranging from 1-32 bytes.

GROUPNAME: group name

v3: specifies that it is SNMP v3 version user, and defaults to v1 version user.

Auth: indicates that security mode requires authentication. If do not enter this parameter, the default is no authentication, no encryption mode.

md5: specifies the authentication protocol as the HMAC MD5 algorithm.

MD5: authentication password, string, value range of plaintext is 1 ~ 64 characters. If MD5 algorithm is adopted in ciphertext form, the authentication key is 32-bit hexadecimal number. If SHA algorithm is used, the authentication key is a 40-bit hexadecimal number.

priv: indicates that security mode requires authentication.

aes: the encryption algorithm is specified as AES (Advanced Encryption Standard), which has higher security than DES.

des: the encryption algorithm is specified as DES (Data Encryption Standard).

password: encrypted password, string, value range of plaintext is 1 ~ 64 characters. If MD5 algorithm is adopted in ciphertext form, the authentication key is 32-bit hexadecimal number. If SHA algorithm is used, the authentication key is a 40-bit hexadecimal number.

【Description】

snmp-server user: the command is used to add a new user to an SNMP group.

no snmp-server user: command is used to delete a user of an SNMP group.

This command applies to SNMP v3 version. If the Agent interact with the message of NMS using SNMP v3 version, then SNMP v3 users need to be created. For the configured user to take effect, a group must be created first. Authentication and encryption are configured when the group is created, and the specific algorithm and password for authentication and encryption are configured when the user is created.


Notice

This command is used several times to configure the same user (that is, the user name is the same, no other parameters are required), and the configuration results are subject to the last configuration.

【Instance】

```
Switch> en
Switch#configure terminal
Switch(config)#snmp-server user admin groupname v3
Switch(config)#no snmp-server user username groupname v3
```

14.6 SNMP Trap Destination

【Command】

```
snmp-server host IP traps (version ( 1 | 2c )) NAME
no snmp-server host IP traps NAME
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

traps: specify the host as Trap host.

IP: the IPV4 address of a host that accepts Traps.

1: represents SNMP v1 version.

2c: represents SNMP v2c version.

NAME: when there is a parameter version, NAME represents SNMPv1/v2c community. When there is no version parameter, NAME represents SNMPv3 user name.

【Description】

snmp-server host: command is used to set the destination host to receive SNMP Trap messages.

no snmp-server host: command is used to cancel the current configurations.

Depending on network management needs, users can configure multiple destination hosts to receive Trap messages through this command.

If a device is needed to send Trap messages, the snmp -server host command should be used in conjunction with the snmp -server enable trap command (the default is to send all traps).

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#snmp-server host 192.168.5.123 traps version 2c
communityname
Switch(config)#no snmp-server host 192.168.5.123 traps name
```

15 LLDP Configuration

15.1 LLDP Enablement

【Command】

lldp enable

no lldp enable

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

lldp enable: command is used to enable the LLDP function.

no lldp enable: the command is used to turn off lldp function.

By default, global LLDP function is disabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#lldp enable
```

15.2 LLDP Port Operating Mode

【Command】

lldp admin-status (*tx-enable* | *rx-enable* | *txrx-enable* | *disable*)

no lldp admin-status disable

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

tx-enable: working mode is Tx, only sending and not receiving LLDP message.

rx-enable: work mode is Rx, it only receives LLDP message and not transmit it.

txrx-enable: work mode is TxRx, it transmits LLDP message as well as receive it.

disable: the working mode is Disable, neither receiving nor sending LLDP message.

【Description】

lldp admin-status: command is used to configure the lldp working mode of the port.

no lldp admin-status disable: command is used to restore the default working mode of the port.

By default, the working mode of LLDP works in TxRx when global LLDP is enabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#lldp admin-status tx-enable
```

15.3 Time Interval of Sending LLDP Message

【Command】

lldp timer <INTERVAL>

no lldp timer

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

interval: the time interval between ports to send LLDP message, ranging from 5-300 in seconds.

【Description】

lldp timer: command is used to set the time interval for sending LLDP message.

no lldp timer: command is used to restore the default packet time interval for LLDP.

By default, the sending interval between LLDP message is 30 seconds

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#lldp timer 50
```

15.4 LLDP Interface Management Address

【Command】

lldp management-address A.B.C.D

no lldp management-address

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D: administrative address published in LLDP message.

【Description】

lldp management-address: command is used to configure the management address published in the LLDP message.

no lldp management-address: command is used to restore the default management address published in the LLDP message.

The management address released by the port in the LLDP message defaults to the main IP address of the smallest VLAN o in the VLAN where the port resides. If the VLAN is not configured with a main IP address, it will be 0.0.0.0.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#lldp management-address 2.2.2.2
```

15.5 Encapsulation Format of LLDP Message

【Command】

lldp frame-format (snap | ethernet2)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

snap: encapsulation format of LLDP message is snap.

ethernet2: the encapsulation format of LLDP message is ethernet2

【Description】

lldp frame-format: command is used to configure the encapsulation format of LLDP message.

By default, the encapsulation format of LLDP message is ethernet2.

【Instance】

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#interface ge8
Switch(config-ge8)#lldp frame-format snap
```

15.6 Display LLDP neighbor information

【Command】

show lldp neighbor-information (*brief* |)

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

Brief:displays a summary of the neighbor device, or neighbor information of all ports without this parameter.

【Description】

show lldp neighbor-information: command is used to display information about the neighbor device.

【Instance】

```
Switch> enable
Switch#show lldp neighbor-information
LLDP neighbor information of port ge2
----------------------------------------
Neighbor index                      : 1
Update time                         : 1hours 57minutes 40seconds
Ageing time                         : 114seconds
Chassis ID type                     : MAC Address
Chassis ID                          : 0022.6f55.5556
Port ID type                        : Interface Name
Port ID                          : ge10
Time to live                        : 120 seconds
Port description                    : ge10
System name                       : SW5
System capabilities supported           : Bridge/Switch,Router
System capabilities enabled             : Bridge/Switch,Router
Management address subtype          : IPv4
```

```
Management address                : 192.168.1.254
Interface number subtype            : System Port Number
Interface number                    : 5010
Object ID                           : Standard LLDP MIB
MAC/PHY Configuration/Status        :
   Auto-Negotiation supported       : Yes
   Auto-Negotiation enabled         : Yes
   Operational MAU type             : 1000BASE-T full duplex mode
Link Aggregation                    :
   Link aggregation supported       : Yes
   Link aggregation enabled         : No
   Aggregated port ID               : 0
Maximum Frame Size                  : 1518
Port VLAN ID                        : 1
----------------------------------------

LLDP Neighbors Number               : 1

Switch#show lldp neighbor-information brief
Local  Intf       Neighbor  System  Name       Neighbor  Port  ID
Ageing-time(s)
ge2           SW5                ge10           91

LLDP Neighbors Number             : 1
```

15.7 Display LLDP Statistics Information

【Command】

show lldp statistics (interface IFNAME **|)**

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

interface IFNAME: displays statistics information of the specified port.

【Description】

show lldp statistics: command is used to display statistics for all ports, or for the specified port.

【Instance】

```
Switch> enable
Switch#show lldp statistics
Global LLDP traffic statistics:
       Total frames out: 268
       Total ages out: 0
       Total frames discarded: 0
       Total frames received in error: 0
       Total frames received in: 260
       Total frames TLVs discarded: 0
       Total frames TLVs unrecognized: 0

Switch#show lldp statistics ge2
Interface ge2 LLDP traffic statistics:
       Total frames out: 269
       Total ages out: 0
       Total frames discarded: 0
       Total frames received in error: 0
       Total frames received in: 260
       Total frames TLVs discarded: 0
       Total frames TLVs unrecognized: 0
```

15.8 Display LLDP Local Information

【Command】

show lldp local-information (interface IFNAME **|)**

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

Interface IFNAME: displays local information of the specified port.

【Description】

show lldp local-information: command is used to display all LLDP local information, or LLDP local information of the specified port.

【Instance】

```
Switch> enable
Switch#show lldp local-information
*Switch#show lldp local-information
LLDP local-information of port ge2:
       Chassis ID subtype : MAC address
       Chassis ID        : 0022.6f01.cca3
       Port ID subtype   : Interface name
       Port ID          : ge2
       Port description  : ge2

       Management address type         : IPv4
       Management address             : 192.168.1.254
       Management address interface type : ifIndex
       Management address interface ID   : 5002
       Management address OID          : 0

       Port VLAN ID(PVID) : 1

       Port and protocol VLAN ID(PPVID) : 0
       Port and protocol VLAN supported : not supported
       Port and protocol VLAN enabled   : no enabled

       VLAN name of VLAN 1 : default

       Link aggregation supported : supported
       Link aggregation enabled   : not enabled
       Aggregated port ID        : 0

       Auto-negotiation supported     : supported
       Auto-negotiation enabled       : enabled
       PMD auto-negotiation advertised :
          10BASE-T half duplex mode
          10BASE-T full duplex mode
          100BASE-TX half duplex mode
          100BASE-TX full duplex mode
          1000BASE-T half duplex mode
```

```
        1000BASE-T full duplex mode
    Operational MAU type          : speed(1000)/duplex(full)
```

15.9 Display LLDP Status Information

【Command】

show lldp status (interface IFNAME **|)**

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

Interface IFNAME: displays state information of the specified port.

【Description】

show lldp status: command is used to display global LLDP status information, or LLDP status information on the specified port.

【Instance】

```
Switch> enable
Switch#show lldp status
LLDP running-information
       System running status          : Running
       System description             : Switch
       Transmit interval              : 30 s
       Hold multiplier                : 4
       Reinit delay                   : 2 s
       Transmit delay                 : 2 s
       Notification enable            : Enable
       Notification Interval          : 5 s

Switch#show lldp status interface ge2
Interface[ge2] lldp status
       Port status of LLDP            :  Enable
       Admin status                   :  Rx_Tx
       Trap flag                      :  No
       Number of neighbors            :  1
```

```
Number of sent optional TLV    :  9
```

16 QOS Configuration

16.1 Configure Global QOS Enable/Disable

【Command】

```
mls  qos enable
no mls qos
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

On is enable, disable is no

【Description】

Used to configure global QoS switch. During all QoS configuration, the MLS QoS switch must be enabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos enable
Switch(config)#no mls qos
```

16.2 Configure the queue bitmap

【Command】

mls qos cos-map <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>
no mls qos cos-map
show mls qos cos-map

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

Parameter 1: select a queue for COS 0 message;
Parameter 2: select a queue for COS 1 message;
Parameter 3: select a queue for COS 2 message;
Parameter 4: select a queue for COS 3 message;
Parameter 5: select a queue for COS 4 message;
Parameter 6: select a queue for COS 5 message;
Parameter 7: select a queue for COS 6 message;
Parameter 8: select a queue for COS 7 message;

【Description】

Configure the queue value for each COS. No is to deleted and show is to view configuration.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos enable
Switch(config)#mls qos cos-map 1 2 3 4 5 6 7 0
Switch(config)#show mls qos cos-map
Switch(config)#no mls qos cos-map
```

16.3 Configure Queue Mode

【Command】

mls qos scheduler (sp|wrr <1-10> <1-10> <1-10> <1-10> <1-10> <1-10> <1-10> <1-10> <1-10>)

no mls qos scheduler

show mls qos scheduler

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

sp: represents strict priority; WRR means to configure each queue with a weight according to weight priority <1-10>.

no: means delete. The default mode is simple polling mode.

Show: to view the configuration.

【Description】

SP: Strict Priority, the SP schedule sends packets in the higher-priority queue in Strict Priority order from highest to lowest, and then sends packets in the lower-priority queue when the higher-priority queue is empty. Queue 7 has the highest priority and queue 0 has the lowest priority.

Weighted dispatching WRR based on messages can be configured to move to the next queue as many messages are scheduled out of each queue.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos enable
Switch(config)#mls qos sschedule sp //configured to SP mode
Switch(config)#show mls qos sschedule
Switch(config)#mls qos sschedule wrr 1 2 3 4 5 6 7 0 // the configuration effect is: each queue takes away the message with the corresponding weight ratio
Switch(config)#no mls qos schedule // restore default configuration SRR
```

16.4 Configure the DSCP-COS Bitmap

【Command】

```
mls qos map dscp-cos NAME (<0-63>|<0-63> <0-63>|<0-63> <0-63>
<0-63>|<0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>
<0-63>|<0-63> <0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63>
<0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>
<0-63> <0-63> <0-63> <0-63>) to <0-7>
no mls qos map dscp-cos (NAME|all)
show mls qos dscp-cos (NAME|all)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

NAME: create a name for the dscp-cos map.

<0-63> to <0-7>: transfer each DSCP value to the corresponding COS queue.

no: means to delete.

Show: means to view the configuration.

【Description】

The default dscp-cos map is 0-7 to cos 0 8-15 to cos 1 16-23 to cos 2 24-31 to cos 3 32-39 to cos 4 40-47 to cos 5 48-55 to cos 6 56-63 to cos 7.

The configuration is only issued when it is referenced. No means to delete NAME, specifying which one to delete.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos enable
Switch(config)# mls qos dscp-cos dscp1 10 46 56 6// means that the
message DSCP value is 10 46 56 and so on will be transfered to queue
6
Switch(config)#show  mls qos dscp-cos dscp1
Switch(config)#no mls qos map dscp-cos dscp1// specify to delete
dscp1
```

16.5 Configure DSCP -DSCP Bitmap

【Command】

```
mls qos map dscp-mutation NAME (<0-63>|<0-63> <0-63>|<0-63> <0-63>
<0-63>|<0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>
<0-63>|<0-63> <0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63>
<0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>
<0-63> <0-63> <0-63> <0-63>) to <0-63>
no mls qos map dscp-mutation （NAME |all）
show mls qos map dscp-mutation(NAME|all)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

By default, it is dscp-mutation map 0-63 to dscp 0-63

No means to delete, name is to specify which MAP to delete, all means to delete all.

Show means to view, NAME means to specify which MAP to view, all means to view all.

【Description】

When different DSCP values received, some changes can be made to the DSCP and then transfer to different queues.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos map dscp-mutation dscp2  2 61
Switch(config)#show mls qos map dscp-mutation dscp2
Switch(config)#no mls qos map dscp-mutation dscp2
```

16.6 Create a CLASS-MAP

【Command】

```
class-map NAME
```

```
no class-map NAME
show class-map(NAME|)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

no: means to delete.

Show: means to view the specified class-map or all class-maps including the information configured therein.

【Description】

Class map: Class map is a definition of a Class map that groups different types of data flows.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#class-map ac
Switch(config)#show class-map
Switch(config)#no class-map ac
```

16.7 Create a POLICY-MAP

【Command】

```
policy-map NAME
no policy-map NAME
show policy-map (NAME|)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

no: means to delete.

show: means to view the information specified or all included in it.

【Description】

policy map: It is a definition of a policy map that matches a class map to determine the bandwidth and/or priority of a class of data flows.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#policy-map ad
Switch(config)#show policy-map (ad)
Switch(config)#no policy-map ad
```

16.8 Configure the CLASS-MAP Property

【Command】

```
match ip-dscp (<0-63>|<0-63> <0-63>|<0-63> <0-63> <0-63>|<0-63>
<0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63> <0-63>|<0-63>
<0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>
<0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63> <0-63> <0-63>
<0-63> <0-63>)
no match ip-dscp

match ip-precedence (<0-7>|<0-7> <0-7>|<0-7> <0-7> <0-7>|<0-7>
<0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7>
<0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>|<0-7>
<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>)
no match ip-precedence <0-7>

match layer4 (source-port|destination-port) <1-65535>
no match layer4 (source-port|destination-port) <1-65535>

match vlan <1-4094>
match vlan-range <1-4094> to <1-4094>
no match vlan
```

【View】

CLASS-MAP Configuration View

【Default Level】

2: Configuration level

【Parameter】

The ip-dscp ip-precedence command is used to configure fields layer4 of dscp precedence, matching L4 port protocol number, vlan <1-4094> message forwarded to the new vlan.

【Description】

None

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#class-map ac
*Switch(config-cmap)#match layer4 destination-port 80
*Switch(config-cmap)#do show class-map
   CLASS-MAP-NAME: ac
     Match Destination Port: 80
 *Switch(config-cmap)#no match layer4 destination-port 80
```

16.9 Configure the POLICY-MAP property

【Command】

class NAME

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

Enter config-pmap-c mode.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos enable
*Switch(config)#policy-map ac
*Switch(config-pmap)#class aa
*Switch(config-pmap-c)#
```

16.10Configure the POLICY-MAP-C Property

【Command】

```
set cos （<0-7>|cos-inner）
no set cos

set ip-dscp <0-63>
no set ip-dscp

set ip-predence <0-7>
no  set ip-predence

police <64-1000000> <0-64000> exceed-action drop
no police <64-1000000> <0-64000> exceed-action drop
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

COS sets the priority, cos-inner copies the vlanID of the ingress to the priority, and no means restore to the default value.

The ip-dscp ip-predence command is to set the priority.

police <64-1000000> <0-64000> exceed-action drop performs the discard action when the rate within this range and the rate should be a multiple of 64.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#mls qos enable
*Switch(config)#policy-map ad
*Switch(config-pmap)#class ac
*Switch(config-pmap-c)#police 2000 2000 exceed-action drop
*Switch(config-pmap-c)#do show policy-map
  POLICY-MAP-NAME: ad
    State: detached
    CLASS-MAP-NAME: ac
      Police: average rate (2000 kbps)
              burst size (2000 bytes)
              exceed-action (drop)
              excess burst size (2000 bytes)
              flow control mode (none)
```

16.11Configure QOS Interface Mode

【Command】

```
service-policy input NAME
no service-policy input NAME

mls qos trust dscp
no mls qos trust dscp

mls qos cos <0-7>
no mls qos cos

mls qos dscp-cos NAME
no mls qos dscp-cos NAME

mls qos dscp-mutation NAME
no mls qos dscp-mutation NAME

wrr-queue bandwidth <1-65535> <1-65535> <1-65535> <1-65535>
<1-65535> <1-65535> <1-65535> <1-65535>
no  wrr-queue bandwidth <0-7>
```

【View】

Ethernet port configuration view

【Default Level】

2: Configuration level

【Parameter】

Name

【Description】

service-policy input NAME: means to install the contents of the policy-map into the specified interface.

No means cancel the installation.

mls qos trust dscp: means that messages received at the specified port are queued according to the value of DSCP, and the default mode is COS. No means restore to default value.

mls qos dscp-cose NAME: installs the named dscp-mutation map to the specified port. No means to delete.

mls qos dscp-mutation NAME: installs the named dscp-mutation map to the specified port. No means to delete.

mls qos cos <0-7>: configure the default priority of the specified port. No means to restore the default value, which is 07 to 07

wrr-queue bandwidth <1-65535> <1-65535> <1-65535> <1-65535> <1-65535> <1-65535> <1-65535> <1-65535>: limit the speed of one or more queues on a specified port, enter a multiple of 64. No means contact speed limit.

【Instance】

```
Switch> enable
Switch#configure terminal
*Switch(config)#interface ge1
*Switch(config-ge1)#service-policy input ad
*Switch(config-ge1)#do show policy-map
  POLICY-MAP-NAME: ad
    State: attached
    CLASS-MAP-NAME: ac
      Police: average rate (2000 kbps)
             burst size (2000 bytes)
             exceed-action (drop)
             excess burst size (2000 bytes)
```

```
            flow control mode (none)

*Switch(config-ge1)#do show mls qos interface ge1
  INPUT-POLICY-MAP-NAME: ad
    CLASS-MAP-NAME: ac
      Police: average rate (2000 kbps)
            burst size (2000 bytes)
            exceed-action (drop)
            excess burst size (2000 bytes)
            flow control mode (none)
  Trust Mode: Ports default priority
  Port Default Prioiry: 0
  VLAN Priority Overide: Not Configured
  Egress Traffic Shaping: Not Configured
View all information on configuring MLS qos within a port.
```

17 ACL Configuration

17.1 Configure IPv4 Extended ACL based on IP addresses

【Command】

```
access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D
access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D
access-list (<1-99>|<1300-1999>) (deny|permit) host A.B.C.D
access-list (<1-99>|<1300-1999>) (deny|permit) any
no access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D
no access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D
no access-list (<1-99>|<1300-1999>) (deny|permit) host A.B.C.D
no access-list (<1-99>|<1300-1999>) (deny|permit) any
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

(<1-99>|<1300-1999>) : represents the scope of the standard ACL.

(deny|permit) : ACL action, deny, permit.

A.B.C.D A.B.C.D: represents the source IP address and mask. The mask adopts the anti-code mechanism, such as 192.168.1.1 0.0.0.0 means only match 192.168.1.1 source IP message.

host A.B.C.D: indicates that the source IP address is A.B.C.D 0.0.0.0.

any: indicates that the source IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

【Description】

Access-list: command is used to create a standard filter rule group. A group can support up to 32 rules. No is to delete a rule group. When the message matches the corresponding rule, the action will be executed. For example, the configuration rule is as follows: access-list 1 deny 192.168.1.1 0.0.0.0.When the message from 192.168.1.1 is received, the action performed is discarded. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 1 deny 192.168.1.1 0.0.0.0
```

17.2 Configure IPv4 Extended ACL based on IP addresses

【Command】

```
access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D A.B.C.D A.B.C.D A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D A.B.C.D any
access-list (<100-199>|<2000-2699>) (deny|permit) ip any A.B.C.D A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip any any
access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D A.B.C.D host A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip host A.B.C.D A.B.C.D A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip host A.B.C.D host A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip any host A.B.C.D
access-list (<100-199>|<2000-2699>) (deny|permit) ip host A.B.C.D any
```

```
no access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D
A.B.C.D A.B.C.D A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D
A.B.C.D any
no access-list (<100-199>|<2000-2699>) (deny|permit) ip any
A.B.C.D A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip any any
no access-list (<100-199>|<2000-2699>) (deny|permit) ip A.B.C.D
A.B.C.D host A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip host
A.B.C.D A.B.C.D A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip host
A.B.C.D host A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip any host
A.B.C.D
no access-list (<100-199>|<2000-2699>) (deny|permit) ip host
A.B.C.D any
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

(<100-199>|<2000-2699>) : indicates the scope of the extended ACL.

(deny|permit) : ACL action, deny, permit.

A.B.C.D A.B.C.D: represents the source/destination IP address and mask. The mask adopts the anti-code mechanism. For example: 192.168.1.1 0.0.0.0 represents messages that only matches 192.168.1.1 source/destination IP.

host A.B.C.D: represents the source/destination IP address.

any: indicates that the source /destination IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

No means to delete the corresponding rule.

【Description】

Access-list: command is used to create a standard filter rule group. A group can support up to 32 rules. No is to delete a rule group. When the message matches the corresponding rule, the action will be executed. For example, the configuration rule is as follows: access-list 101 deny 192.168.1.1 0.0.0.0 192.168.2.1 0.0.0.0 When the

message from 192.168.1.1 to 192.168.2.1 is received, the action performed is discarded. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 101 deny 192.168.1.1 0.0.0.0
192.168.2.1 0.0.0.0
```

17.3 Configure Other IPv4 Protocol Extended ACL based on IP Addresses

【Command】

```
access-list (<100-199>|<2000-2699>) (deny|permit)
(<0-255>|ahp|eigrp|esp|gre|ipinip|ospf|pcp|pim ) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) ((A.B.C.D A.B.C.D)|(any)|(host
A.B.C.D))
no access-list (<100-199>|<2000-2699>) (deny|permit)
(<0-255>|ahp|eigrp|esp|gre|ipinip|ospf|pcp|pim ) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) ((A.B.C.D A.B.C.D)|(any)|(host
A.B.C.D))
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

(<100-199>|<2000-2699>) : indicates the scope of the extended ACL.

(deny|permit) : ACL action, deny, permit.

(<0-255>|Ahp|eigrp|esp|gre|ipinip|ospf|pcp|pim) : configure IP protocol type:

- <0-255>: An IP protocol number
- Ahp: Authentication Header Protocol
- Eigrp: EIGRP routing protocol
- Esp: Encapsulation Security Payload
- Gre: General Routing Encapsulation
- Ipinip: iP in IP tunneling

- Ospf: OSPF routing protocol
- Pcp: Payload Compression Protocol
- Pim: Protocol Independent Multicast

((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) : configure the source IP address.

((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) : configure the destination IP address.

No means to delete.

【Description】

Since the message has a corresponding protocol port number, it can be configured to filter based on the protocol port number. For example, the configuration rules are as follows: access-list 101 deny ahp 192.168.1.1 0.0.0.0 192.168.2.1 0.0.0.0.When the ahp message from 192.168.1.1 to 192.168.2.1 is received, the action performed is discarded. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 101 deny ahp 192.168.1.1 0.0.0.0
192.168.2.1 0.0.0.0
```

17.4 Configure IPV4 ICMP Extend ACL Based on IP Addresses

【Command】

```
access-list (<100-199> | <2000-2699>) (deny | permit) (icmp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) ((A.B.C.D A.B.C.D)
|           (any)           |           (host           A.B.C.D))
(<0-255>|echo|echo-reply|redirect|ttl-exceeded|unreachable|)
no access-list (<100-199> | <2000-2699>) (deny | permit) (icmp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) ((A.B.C.D A.B.C.D)
|           (any)           |           (host           A.B.C.D))
(<0-255>|echo|echo-reply|redirect|ttl-exceeded|unreachable|)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

(<100-199>|<2000-2699>) : indicates the scope of the extended ACL.

(deny|permit) : ACL action, deny, permit.

Icmp: filter Icmp protocol message.

A.B.C.D A.B.C.D: represents the source/destination IP address and mask, and the mask adopts the anti-code mechanism. For example, 192.168.1.1 0.0.0.0 means that only matches the message with 192.168.1.1 source/destination IP.

host A.B.C.D: represents the source/destination IP address.

any: indicates that the source /destination IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

(<0-255>|echo|echo-reply|redirect|ttl-exceeded|unreachable|) : corresponding to icmp message type, echo (ping), echo reply, All redirects, TTL exceeded, All unreachables.

no: means to delete.

【Description】

Configure extended ACL icmp protocol based on IPV4. For example, the configuration rule is as follows: access-list 103 deny icmp 192.168.1.1 0.0.0.0 192.168.2.1 0.0.0.0 echo. Therefore, when receiving echo message from icmp 192.168.1.1 to icmp 192.168.2.1, the action executed is discarded. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

【Instance】

```
Switch> en
Switch#configure terminal
Switch(config)#access-list 103 deny icmp 192.168.1.1 0.0.0.0
192.168.2.1 0.0.0.0 echo
```

17.5 Configure IPV4 ICMP Extend ACL Based on IP Addresses

【Command】

```
access-list (<100-199>|<2000-2699>) (deny|permit) (igmp) ((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) ((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) (<0-255>|query|reportv1|reportv2|leave|reportv3|)
no access-list (<100-199>|<2000-2699>) (deny|permit) (igmp) ((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) ((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) (<0-255>|query|reportv1|reportv2|leave|reportv3|)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

(<100-199>|<2000-2699>) : indicates the scope of the extended ACL.

(deny|permit) : ACL action, deny, permit.

Igmp: filter Igmp protocol message.

A.B.C.D A.B.C.D: represents the source/destination IP address and mask, and the mask adopts the anti-code mechanism. For example, 192.168.1.1 0.0.0.0 means that only matches the message with 192.168.1.1 source/destination IP.

host A.B.C.D: represents the source/destination IP address.

any: indicates that the source /destination IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

(<0255>|query|reportv1|reportv2|leave|reportv3|): corresponding to different igmp message types, IGMP Membership Query, IGMPv1 Membership Report, IGMPv2 Membership Report, IGMPv2 Leave Group, IGMPv3 Membership Report.

no: means to delete.

【Description】

Configure extended ACL igmp protocol based on IPV4, destination address should be configured as multicast address, otherwise the corresponding rule cannot be matched.

For example, the configuration rule is as follows: access-list 103 deny igmp 192.168.1.1 0.0.0.0 224.1.2.3 0.0.0.0 leave. Therefore, when the leave message from 192.168.1.1 to igmp of group 224.1.2.3 is received, the action executed is discarded. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

【Instance】

```
Switch> en
Switch#configure terminal
Switch(config)#access-list 103 deny igmp 192.168.1.1 0.0.0.0
224.1.2.3 0.0.0.0 leave
```

17.6 Configure IPv4 TCP Extended ACL Based on IP Addresses

【Command】

```
access-list (<100-199> | <2000-2699>) (deny | permit) (tcp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) | ) ((A.B.C.D
A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) | )
(fin|syn|rst|psh|ack|urg| )

access-list (<100-199> | <2000-2699>) (deny | permit) (tcp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))) ((A.B.C.D
A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) | )
(fin|syn|rst|psh|ack|urg| )

access-list (<100-199> | <2000-2699>) (deny | permit) (tcp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) | ) ((A.B.C.D
A.B.C.D) | (any) | (host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)))
(fin|syn|rst|psh|ack|urg| )
```

```
access-list (<100-199> | <2000-2699>) (deny | permit) (tcp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))) ((A.B.C.D
A.B.C.D) | (any) | (host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)))
(fin|syn|rst|psh|ack|urg| )

no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp)
((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) (((eq|lt|gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))|) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) (((eq|lt|gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))|)
(fin|syn|rst|psh|ack|urg|)

no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp)
((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) (ftp|ftp-data
|pop3|smtp|telnet|www|<1-65535>))) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) (((eq|lt|gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))|)
(fin|syn|rst|psh|ack|urg|)

no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp)
((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) (((eq|lt|gt)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))|) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)))
(fin|syn|rst|psh|ack|urg|)

no access-list (<100-199>|<2000-2699>) (deny|permit) (tcp)
((A.B.C.D A.B.C.D)|(any)|(host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>)) (ftp|ftp-data
|pop3|smtp|telnet|www|<1-65535>))) ((A.B.C.D
A.B.C.D)|(any)|(host A.B.C.D)) (((range)
(ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))(ftp|ftp-data|po
p3|smtp|telnet|www|<1-65535>))) (fin|syn|rst|psh|ack|urg|)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

(<100-199>|<2000-2699>): indicates the scope of the extended ACL.

(deny|permit): ACL action, deny, permit.

Tcp: filter tcp protocol message.

A.B.C.D A.B.C.D: represents the source/destination IP address and mask, and the mask adopts the anti-code mechanism. For example, 192.168.1.1 0.0.0.0 means that only matches the message with 192.168.1.1 source/destination IP.

host A.B.C.D: represents the source/destination IP address.

any: indicates that the source /destination IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

(eq|lt|gt):

- Match only packets on a given port number
- Match only packets with a lower port number
- Match only packets with a greater port number。

((ftp|ftp-data|pop3|smtp|telnet|www|<1-65535>))|): corresponding to different TCP message types:

- File Transfer Protocol (21)，
- FTP data connections (20)，
- Post Office Protocol v3 (110)，
- Simple Mail Transport Protocol (25)，
- Telnet (23)，
- World Wide Web (HTTP, 80)，
- Port number(1-65535)。
- (fin|syn|rst|psh|ack|urg|):
- Match on the FIN bit，
- Match on the Syn bit，
- Match on the Rst bit，
- Match on the Psh bit，
- Match on the Ack bit，
- Match on the Urg bit.

no: means to delete.

【Description】

Configure extended ACL igmp protocol based on IPV4, destination address should be configured as multicast address, otherwise the corresponding rule cannot be matched. For example, the configuration rule is as follows: access-list 101 deny tcp host

192.168.1.1 eq ftp host 192.168.2.1 eq pop3 fin, then when receiving the tcp message from 192.168.1.1 to 192.168.2.1, the action executed is discard. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 101 deny tcp host 192.168.1.1 eq ftp
host 192.168.2.1 eq pop3 fin
Switch(config)#access-list 102 deny tcp host 192.168.1.1 range ftp
ftp host 192.168.2.1 range  pop3 pop3 fin
```

17.7 Configure IP Address-based IPv4 UDP Extend ACL

【Command】

```
access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | ) ((A.B.C.D A.B.C.D) | (any)
|     (host     A.B.C.D))     (((eq     |     lt     |     gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | )

 access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D  A.B.C.D)  |  (any)  |  (host  A.B.C.D))  (((range)
(<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp)) ((A.B.C.D A.B.C.D) | (any)
|     (host     A.B.C.D))     (((eq     |     lt     |     gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | )

access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | ) ((A.B.C.D A.B.C.D)|(any)
| (host A.B.C.D)) (((range) (<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp))

access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D  A.B.C.D)  |  (any)  |  (host  A.B.C.D))  (((range)
(<1-65535>|rip|snmp|snmp-trap|tftp)
```

```
(<1-65535>|rip|snmp|snmp-trap|tftp)) ((A.B.C.D A.B.C.D) | (any)
| (host A.B.C.D)) (((range) (<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp))

no access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D)) (((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | ) ((A.B.C.D A.B.C.D) | (any)
|     (host     A.B.C.D))     (((eq     |     lt     |     gt)
(<1-65535>|rip|snmp|snmp-trap|tftp))| )

no access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D  A.B.C.D)  |  (any)  |  (host  A.B.C.D))    (((range)
(<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp))  ((A.B.C.D A.B.C.D) | (any)
|     (host     A.B.C.D))     (((eq     |     lt     |     gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | )

no access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D A.B.C.D) | (any) | (host A.B.C.D))  (((eq | lt | gt)
(<1-65535>|rip|snmp|snmp-trap|tftp)) | ) ((A.B.C.D A.B.C.D) | (any)
| (host A.B.C.D)) (((range) (<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp))

 no access-list (<100-199> | <2000-2699>) (deny | permit) (udp)
((A.B.C.D  A.B.C.D)  |  (any)  |  (hostA.B.C.D))  (  ((range)
(<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp)) ((A.B.C.D A.B.C.D) | (any)
| (host A.B.C.D)) (((range) (<1-65535>|rip|snmp|snmp-trap|tftp)
(<1-65535>|rip|snmp|snmp-trap|tftp))
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

(<100-199>|<2000-2699>) : indicates the scope of the extended ACL.

(deny|permit) : ACL action, deny, permit.

udp: filter udp protocol message.

A.B.C.D A.B.C.D: represents the source/destination IP address and mask, and the mask adopts the anti-code mechanism. For example, 192.168.1.1 0.0.0.0 means that only matches the message with 192.168.1.1 source/destination IP.

host A.B.C.D: represents the source/destination IP address.

any: indicates that the source /destination IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

((eq|lt|gt):

- Match only packets on a given port number，
- Match only packets with a lower port number，
- Match only packets with a greater port number。

(<1-65535>|rip|snmp|snmp-trap|tftp): corresponding to different tcp message types:

- Port number(1-65535) (21)，
- Routing Information Protocol (router, in.routed, 520)，
- Simple Network Management Protocol (161)，
- SNMP Traps (162)，
- Trivial File Transfer Protocol (69).W

【Description】

Configure extended ACL igmp protocol based on IPV4, destination address should be configured as multicast address, otherwise the corresponding rule cannot be matched. For example, the configuration rule is as follows: access-list 101 deny udp host 192.168.1.1 eq tftp host 192.168.2.1 eq tftp, then when receiving the tcp tftp message from 192.168.1.1 to 192.168.2.1, the action executed is discarded. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list 101 deny tcp host 192.168.1.1 eq tftp host 192.168.2.1 eq tftp
Switch(config)#access-list 102 deny tcp host 192.168.1.1 range tftp tftp host 192.168.2.1 range 10 30
```

17.8 Configure Character Type ACL Based on IPv4 Addresses

【Command】

```
access-list swos WORD (deny|permit)
(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>)
(A.B.C.D/M|A.B.C.D A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|any)
((label(1-65535)|precedence<0-7>) | tos (0-255) | range <0-255>
<0-255> | pkt-size ((lt|gt)<0-65535> | range <0-65535> <0-65535>)
| fragments | log | interface (in|out) IFNAME)

access-list swos WORD (deny|permit) (icmp)(A.B.C.D/M|A.B.C.D
A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|any) ((icmp-type
ICMP-TYPE|label(1-65535)|precedence<0-7>)|tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

access-list swos WORD (deny|permit)(udp)(A.B.C.D/M|A.B.C.D
A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>)
 (A.B.C.D/M|A.B.C.D A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>)((label(1-65535)|precedence<0-7>)|tos (0-255)
|range <0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

access-list swos WORD (deny|permit)(tcp)(A.B.C.D/M|A.B.C.D
A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>)
 (A.B.C.D/M|A.B.C.D A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>)((label(1-65535)|precedence<0-7>)|tos (0-255)
|range <0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

no access-list swos WORD (deny|permit)(udp)(A.B.C.D/M|A.B.C.D
A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>)
 (A.B.C.D/M|A.B.C.D A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>)((label(1-65535)|precedence<0-7>)|tos (0-255)
|range <0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

no access-list swos WORD (deny|permit) (icmp)(A.B.C.D/M|A.B.C.D
A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|any) ((icmp-type
```

```
ICMP-TYPE|label(1-65535)|precedence<0-7>)|tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

no access-list swos WORD (deny|permit)( tcp)(A.B.C.D/M|A.B.C.D
A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range <0-65535> <0-65535>)
 (A.B.C.D/M|A.B.C.D A.B.C.D|any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>)((label(1-65535)|precedence<0-7>)|tos (0-255)
|range <0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

no access-list swos WORD (deny|permit)
(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>)
(A.B.C.D/M|A.B.C.D A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|any)
((label(1-65535)|precedence<0-7>)|tos (0-255) |range <0-255>
<0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

Swos WORD: configure a character ACL.

(deny|permit) : ACL action, deny, permit.

(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>):

A.B.C.D A.B.C.D: represents the source IP address and mask. The mask adopts the anti-code mechanism, such as 192.168.1.1 0.0.0.0 means only match 192.168.1.1 source IP message.

host A.B.C.D: indicates that the source IP address is A.B.C.D 0.0.0.0.

any: indicates that the source IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

Label: configure priority.

Precedence: configure priority.

Tos: configure priority.

Pkt-size: configure message length

Interface[IFNAME] : install port number.

【Description】

The access-list command is used to create a standard filter rule group. A group can support up to 32 rules. No is to delete a rule group. When the message matches the corresponding rule, the action will be executed. For example, the configuration rule is as follows: access-list swos AA deny ip 192.168.1.1 0.0.0.0 192.168.2.1 0.0.0.0.When the message from 192.168.1.1 is received and sent to 192.168.2.1, the action performed is discard. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#access-list swos AA deny ip 192.168.1.1 0.0.0.0
192.168.2.1 0.0.0.0
```

17.9 Configure Character Type ACL Based on IPV6 Address

【Command】

```
ipv6 access-list swos WORD (deny|permit)
(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>)
( X:X::X:X/M|X:X::X:X |any) (X:X::X:X/M|X:X::X:X |any)
((label(1-65535)|precedence<0-7>) | tos (0-255) |range <0-255>
<0-255> | pkt-size ((lt|gt) <0-65535> | range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

ipv6 access-list swos WORD (deny|permit) (icmp)
(X:X::X:X/M|X:X::X:X |any) (X:X::X:X/M|X:X::X:X |any) ((icmp-type
ICMP-TYPE|label(1-65535)|precedence<0-7>)|tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

ipv6 access-list swos WORD (deny|permit) (udp)
(X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>)(X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne)
<0-65535> | range <0-65535> <0-65535>)
((label(1-65535)|precedence<0-7>) | tos (0-255) |range <0-255>
```

```
<0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

ipv6 access-list swos WORD (deny|permit) (tcp)
(X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne) <0-65535> | range
<0-65535> <0-65535>)(X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne)
<0-65535> | range <0-65535>
<0-65535>)((label(1-65535)|precedence<0-7>) | tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

no ipv6 access-list swos WORD
(deny|permit)(udp)(X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne)
<0-65535> | range <0-65535> <0-65535>)(X:X::X:X/M|X:X::X:X |any)
((eq|lt|gt|ne) <0-65535> | range <0-65535>
<0-65535>)((label(1-65535)|precedence<0-7>)|tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

no ipv6 access-list swos WORD (deny|permit)
(icmp)(X:X::X:X/M|X:X::X:X |any) (X:X::X:X/M|X:X::X:X |any)
((icmp-type ICMP-TYPE|label(1-65535)|precedence<0-7>)|tos (0-255)
|range <0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

no ipv6 access-list swos WORD
(deny|permit)( tcp)(X:X::X:X/M|X:X::X:X |any) ((eq|lt|gt|ne)
<0-65535> | range <0-65535> <0-65535>)(X:X::X:X/M|X:X::X:X |any)
((eq|lt|gt|ne) <0-65535> | range <0-65535>
<0-65535>)((label(1-65535)|precedence<0-7>)|tos (0-255) |range
<0-255> <0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)

no ipv6 access-list swos WORD (deny|permit)
(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>)( X:X::X:X/M
|X:X::X:X |any) (X:X::X:X/M|X:X::X:X |any)
((label(1-65535)|precedence<0-7>)|tos (0-255) |range <0-255>
<0-255>|pkt-size ((lt|gt)<0-65535>|range <0-65535>
<0-65535>)|fragments|log|interface (in|out) IFNAME)
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

Swos WORD: configure a character ACL.

(deny|permit) : ACL action, deny, permit.

(ip|gre|igmp|pim|rsvp|ospf|vrrp|ipcom|any|<0-255>):

X:X::X:X/M|X:X::X:X |any: indicates the source IP address and mask, and the mask adopts the anti-code mechanism, for example: fe80::01:: indicates the message that only matches fe80::01 source IP.

any: indicates that the source IP address is 0.0.0.0 255.255.255.255, which means all IP addresses.

Label: configure priority.

Precedence: configure priority.

Tos: configure priority.

Pkt-size: configure message length

Interface[IFNAME] : install port number.

【Description】

The access-list command is used to create a standard filter rule group. A group can support up to 32 rules. No is to delete a rule group. When the message matches the corresponding rule, the action will be executed. For example, the configuration rule is as follows: Ipv6 access-list swos qwer deny any fe80::01 :: fe80::02 :: then when receiving the message from fe80::01 ::, to fe80::02 ::, the action executed is discard. These rules only take effect when activated on a port using the ip-access-group command. And has the "first activation first effect" feature.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#ipv6 access-list swos qwer deny any fe80::01 ::
fe80::02 ::
```

17.10View All Configured ACL

【Command】

```
Show access-list
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

None

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#show access-list
```

17.11Activate ACL

【Command】

```
ip-access-group (<1-199>|<1300-2699>) in
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

(<1-199>|<1300-2699>) in: ACL rule group ID, in represents the ingress direction.

【Description】

ACLS configured with time-range also need to be activated, meeting the rule of first activation first effect.

A port can only activate one IP address ACL and one MAC address ACL.

【Instance】

```
Switch> enable
```

```
Switch#configure terminal
Switch(config)#interface ge8
Switch(config-ge8)#ip-access-group 1 in
```

17.12Configure ACL Based on MAC Address

【Command】

```
mac access-list <2000-2699> (deny|permit) MAC MASK MAC MASK
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) MAC MASK MAC MASK
(<1-65535>|NUM|)

mac access-list <2000-2699> (deny|permit) MAC MASK host MAC
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) MAC MASK host MAC
(<1-65535>|NUM|)

mac access-list <2000-2699> (deny|permit) MAC MASK any
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) MAC MASK any
(<1-65535>|NUM|)

mac access-list <2000-2699> (deny|permit) any host MAC
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) any host MAC
(<1-65535>|NUM|)

mac access-list <2000-2699> (deny|permit) any MAC MASK
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) any MAC MASK
<1-65535>|NUM|)

mac access-list <2000-2699> (deny|permit) host MAC MAC MASK
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) host MAC MAC MASK
(<1-65535>|NUM|)

mac access-list <2000-2699> (deny|permit) host MAC any
(<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) host MAC any
(<1-65535>|NUM|)
```

mac access-list <2000-2699> (deny|permit) host MAC host MAC (<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) host MAC host MAC (<1-65535>|NUM|)

mac access-list <2000-2699> (deny|permit) any any (<1-65535>|NUM|)
no mac access-list <2000-2699> (deny|permit) any any (<1-65535>|NUM|)

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<2000-2699>: standard MAC ACL label range.

MAC MASK MAC MASK: source MAC + MASK destination MAC+ MASK.

(<1-65535>|NUM|): Ethernet type. Hexadecimal/hexadecimal input.

【Description】

Configure a MAC address based ACL, and when the message matches the issued rule, the configured action is executed.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#MAC access-list 2001 deny any any 0x8100//Configure a message ACL that discards the MAC address of Ethernet type 0x8100
Switch(config)#no mac access-list 2001 deny any any 0x8100 //// delete a message ACL that discards a MAC address of Ethernet type 0x8100
```

17.13View All Configured MAC ACL

【Command】

show mac access-list

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

None

【Instance】

```
Switch> enable
Switch# show mac access-list
```

17.14Time-range and MAC ACL Binding

【Command】

```
mac  access-list <2000-2699>  time-range WORD
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

Bind a time-range to an ACL and perform the MAC ACL action within the setting time. An MAC ACL can only bind one time-range, and one time-range can bind multiple MAC ACL. When deleted, if the time-range is referenced, the time-range is not allowed to be deleted and its subitems are allowed to be modified.

【Instance】

```
Switch(config)#mac access-list 2001 time-range ad // bind the standard MAC ACL numbered 2001 to time-range ad.
Switch(config)#no mac access-list 2001 time-range ad // unbind the standard MAC ACL numbered 2001 to time-range AD.
```

17.15Activate MAC ACL

【Command】

mac-access-group <2000-2699> in

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

<2000-2699>: MAC ACL rule group ID

in: indicates the direction of ingress.

【Description】

ACLS configured with time-range also need to be activated, meeting the rule of first activation first effect.

A port can only activate one IP address ACL and one MAC address ACL.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#mac-access-group 2001 in
```

17.16View All Activated ACL

【Command】

show access-group

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

View the currently activated ACL port.

【Instance】

```
Switch> enable
Switch#show access-group
```

18 802.1X Authentication Configuration

18.1 Global802.1X Authentication Enablement

【Command】

[no] dot1x system-auth-ctrl

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

dot1x system-auth-ctrl: command is used to enable global dot1x authentication function.

no dot1x system-auth-ctrl: command is used to disable global dot1x authentication function.

By default, global dotlx authentication function is disabled.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#dot1x system-auth-ctrl
```

18.2 802.1X Authentication Port Authorization Mode

【Command】

dot1x port-control (auto | force-authorized | force-unauthorized)

no dot1x port-control

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

auto: set port to enable 802.1x authentication mode and it is unauthorized mode by default.

force-authorized: set the port to forced authorized mode.

force-unauthorized: set the port to force-unauthorized mode

【Description】

dot1x port-control: command is used to set the access control mode of 802.1x on the specified port.

no dot1x port-control: the command is used to delete port 802.1x authentication function.

The port is not configured with 802.1x authentication by default.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x port-control auto
```

18.3 802.1X Authentication Port Controlled Direction

【Command】

dot1x port-control dir (both | in)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

both: the controlled direction is bi-directional

in: the controlled direction is ingress.

【Description】

dot1x port-control dir: command is used to configure port controlled directions.

By default, the controlled direction of the port is ingress.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x port-control dir both
```

18.4 802.1X Authentication EAPOL Protocol Version

【Command】

```
dot1x protocol-version (1| 2)
no dot1x protocol-version
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

1: Configure EAPOL to 1

2: Configure EAPOL to 2.

【Description】

dot1x protocol-version: command is used for the EAPOL protocol version of dot1x.

no dot1x protocol-version: command is used for the default EAPOL protocol version of dot1x.

By default, the EAPOL protocol message version is 2.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x protocol-version 2
```

18.5 802.1X Authentication Port Silent Time

【Command】

dot1x quiet-period <1-65535>

no dot1x quiet-period

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

1-65535: the silent time of the port, ranging from 1-65535 seconds, defaults to 60 seconds

【Description】

dot1x quiet-period: the command is used for the quiet period of the dot1x port.

no dot1x quiet-period: command is used for the default quiet time of the dot1x port.

By default, the silence time of the dot1x port is 60 seconds.

【Instance】

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#interface ge1
Switch(config-ge1)#dot1x quiet-period 120
```

18.6 802.1x Authorization Port Reauthentication Interval

【Command】

dot1x timeout re-authperiod <1-4294967295>

no dot1x timeout re-authperiod

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

1-4294967295: re-authentication interval for port, the range is 1-4294967295 seconds, the default value is 3600 seconds.

【Description】

dot1x timeout re-authperiod: command is used for re-authentication intervals on the dot1x port.

no dot1x timeout re-authperiod: command is used for the default re-authentication interval of dot1x port.

By default, the re-authentication interval on dot1x port is 3600 seconds.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x timeout re-authperiod 1200
```

18.7 802.1X Authorization Server Timeout Time

【Command】

dot1x timeout server-timeout <1-65535>

no dot1x timeout server-timeout

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

1-65535: the server timeout of the port, ranging from 1- 65535 seconds, defaults to 30 seconds.

【Description】

dot1x timeout server-timeout: The command is used for the server timeout on the dot1x port.

no dot1x timeout server-timeout: command is for the default server timeout of the dot1x port.

By default, the server timeout on dot1x port is 30 seconds.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x timeout server-timeout 60
```

18.8 802.1X Authorization Client Timeout Time

【Command】

dot1x timeout supp-timeout ***<1-65535>***

no dot1x timeout supp-timeout

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

1-65535: the client timeout of the port, ranging from 1- 65535 seconds, defaults to 30 seconds

【Description】

dot1x timeout supp-timeout: command is used for the client timeout on the dot1x port.

no dot1x timeout supp-timeout: command is for the default clinet timeout of the dot1x port.

By default, the client timeout on dot1x port is 30 seconds.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x timeout supp-timeout 60
```

18.9 802.1X Authorization Message Retransmission Interval

【Command】

dot1x timeout tx-period *<1-65535>*

no dot1x timeout tx-period

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

1-65535: the retransmission interval of the port, the range is 1-65535 seconds, the default is 30 seconds

【Description】

dot1x timeout tx-period: command is used for retransmission intervals on the dot1x port.

no dot1x timeout tx-period: command is used for the default retransmission interval of the dot1x port.

By default, the retransmission interval on dot1x port is 30 seconds.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x timeout tx-period 60
```

18.10 802.1X Authorization Message Retransmission Interval

【Command】

dot1x reauthMax <*1-10*>

no dot1x reauthMax

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

1-65535: the number of retransmission of request/id message of the port, ranging from 1 to 10 seconds, it is 3 times by default

【Description】

dot1x reauthMax: command is used for the times of retransmissions of the dot1x port.

no dot1x reauthMax: command is used for the default times of retransmissions

By default, the times of retransmissions on dot1x port is 3.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x reauthMax 4
```

18.11 802.1x Authorization Port Reauthentication Mode

【Command】

dot1x reauthentication

no dot1x reauthentication

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

dot1x reauthentication: command is used to enable re-authentication on the dot1x port.

no dot1x reauthentication: command is used to disable the re-authentication feature on the dot1x port.

By default, the re-authentication interval on dot1x port is 3600 seconds.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x reauthentication
```

18.12 802.1X Authentication Port Initialization

【Command】

dot1x initialize

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

dot1x initialize: command is used to initialize and unauthorize the dot1x port and attempt to re-authenticate on the dot1x port.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x initialize
```

18.13 802.1X Authorization Key Encryption Function

【Command】

dot1x keytxenabled (enable | disable)

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

dot1x keytxenabled enable: command is used to enable key encryption on the dot1x port (when clients interact with EPAOL messages).

dot1x keytxenabled disable: command is used to disable key encryption on the dot1x port.

Key encryption on the dot1x port is disabled by default.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#dot1x keytxenabled enable
```

18.14Display 802.1X Authentication Global Information

【Command】

show dot1x

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show dot1x: command is used to display dot1x global information and radius client information.

【Instance】

```
Switch> enable
Switch#show dot1x
802.1X Port-Based Authentication Enabled
  RADIUS client address: not configured
```

18.15Display 802.1X Authentication Detailed Information

【Command】

show dot1x all

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show dot1x all: command is used to display dot1x global information and radius client information, as well as port information.

【Instance】

```
Switch> enable
Switch#show dot1x all
802.1X Port-Based Authentication Enabled
  RADIUS client address: not configured
802.1X info for interface ge4
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 90
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connecting - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 0
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
```

18.16Display 802.1X Authentication Port Information

【Command】

show dot1x interface <IFNAME>

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

Ifname:specifies the port name

【Description】

show dot1x interface: command is used to display dot1x information for the specified port.

【Instance】

```
Switch> enable
Switch#show dot1x interface ge4
802.1X info for interface ge4
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 92
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connecting - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 0
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
```

18.17Display 802.1X Authentication Port Diagnosis Information

【Command】

show dot1x diagnostics interface <IFNAME>

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

Ifname:specifies the port name

【Description】

show dot1x diagnostics interface: command is used to display dot1x diagnostics information for the specified port.

【Instance】

```
Switch> enable
Switch#show dot1x diagnostics interface ge4
802.1X Diagnostics for interface ge4
 authEnterConnecting: 707
 authEaplogoffWhileConnecting: 355
 authEnterAuthenticating: 0
 authSuccessWhileAuthenticating: 0
 authTimeoutWhileAuthenticating: 0
 authFailWhileAuthenticating: 0
 authEapstartWhileAuthenticating: 0
 authEaplogoggWhileAuthenticating: 0
 authReauthsWhileAuthenticated: 0
 authEapstartWhileAuthenticated: 0
 authEaplogoffWhileAuthenticated: 0
 BackendResponses: 0
 BackendAccessChallenges: 0
 BackendOtherrequestToSupplicant: 0
 BackendAuthSuccess: 0
 BackendAuthFails: 0
```

18.18Display 802.1X Authentication Port Session Information

【Command】

show dot1x sessionstatistics interface <IFNAME>

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

Ifname:specifies the port name

【Description】

show dot1x sessionstatistics interface: command is used to display dot1x sessionstatistics information for the specified port.

【Instance】

```
Switch> enable
Switch#show dot1x sessionstatistics interface ge4
802.1X session statistics for interface ge4
session authentication method: Local server
session time: 0 secs
session user name:
 session terminate cause: Port failure
```

18.19Display 802.1X Authentication Port Message Statistics

【Command】

show dot1x statistics interface <IFNAME>

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

Ifname:specifies the port name

【Description】

show dot1x statistics interface: command is used to display dot1x message for the specified port.

【Instance】

```
Switch> enable
Switch#show dot1x statistics interface ge4
802.1X statistics for interface ge4
  EAPOL Frames Rx: 0 - EAPOL Frames Tx: 0
  EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
  EAP Rsp/Id Frames Rx: 0 - EAP Response Frames Rx: 0
  EAP Req/Id Frames Tx: 719 - EAP Request Frames Tx: 0
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
  EAPOL Last Frame Version Rx: 0 - EAPOL Last Frame Src:
0000.0000.0000
```

18.20 RADIUS Server Regeneration Interval

【Command】

radius-server deadtime <0-1440>

no radius-server deadtime

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

0-1440: the regeneration interval of RADIUS, ranging from 0-1440 minutes, and the default value is 0

【Description】

radius-server deadtime: command is used to configure the interval between the radius unreachable is restored to reachable.

no radius-server deadtime: command is used to delete the interval.

By default, the regeneration interval is 0.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#radius-server deadtime 5
```

18.21 RADIUS Server

【Command】

radius-server host <HOSTNAME> **{key** STRING **| auth-port** PORTNO **| timeout** SEC **| retransmit** RETRIES**}**

no radius-server host <HOSTNAME> **(auth-port** PORTNO **|)**

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

hostname: IP address or host name of RADIUS server

STRING: Shared key with RADIUS server

PORTNO: UDP port of RADIUS authentication, the value range is 0-65535

SEC: timeout interval of RADIUS server, value range is 1-1000, the default value is 5 seconds

RETRIES: the number of times the RADIUS server retransmits over the timeout，the value range is 1-100, which is 3 times by default

【Description】

radius-server host: command is used to configure the RADIUS server.

no radius-server host: command is used to configure the RADIUS server.

By default, theRADIUS server is not configured.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#radius-server host 192.168.1.100 key 123456
auth-port 1812
```

19 Alarm Configuration

19.1 Enable Port Alarm

【Command】

system alarm enable

【View】

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

Enabling port up/down the alarm light on the panel will be lit immediately when the port down occurs. When the port up occurs, the alarm light on the panel will be turned off. By default, it is turned off. However, the warning light will also be turned on when the power alarm is enabled, so it is recommended not to turn them on at the same.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge 1
Switch(config-ge1)#system alarm enable
```

19.2 Disable Port Alarm

【Command】

system alarm disable

【View】

ge (Gigabit Ethernet) port view

xe (10 Gigabit Ethernet) port view

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

Enabling port up/down the alarm light on the panel will be lit immediately when the port down occurs. When the port up occurs, the alarm light on the panel will be turned off. By default, it is turned off. However, the warning light will also be turned on when the power alarm is enabled, so it is recommended not to turn them on at the same.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge 1
Switch(config-ge1)#system alarm disable
```

19.3 Enable Power Alarm

【Command】

power <1-2> **alarm enable**

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<1-2>: means power supply 1, 2

【Description】

Enabling power<1- 2>alarm, light on the panel will be lit immediately when the port is down. When power is specified to up, the alarm light on the panel will be turned off. By default, it is turned off. However, the warning light will also be turned on when the port alarm is enabled, so it is recommended not to turn them on at the same.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#power 1 alarm enable
```

19.4 Power off Warning

【Command】

power <1-2> **alarm disable**

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<1-2>: means power supply 1, 2

【Description】

Enabling power<1- 2>alarm, light on the panel will be lit immediately when the port is down. When power is specified to up, the alarm light on the panel will be turned off. By default, it is turned off. However, the warning light will also be turned on when the port alarm is enabled, so it is recommended not to turn them on at the same.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#power 1 alarm disable
```

20 RMON Configuration

20.1 RMON Alarm Group

【Command】

```
rmon alarm <Index> <alarm-variable> interval <Seconds> {absolute | delta} rising-threshold <RISING_THRES> event <event_Index> falling-threshold <FALL_THRES> event <event_Index> ( owner <name>|)
no rmon alarm <Index>
```

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

Index: warning group index, the range is 1-65535.

alarm-variable: the format is etherStatsEntry.n.n

Seconds: sampling time interval ranging from 1-4294967295.

Delta: sampling type is variable value (the current sample value of the selected variable relative to the last sample value)

absolute: the sampling type is absolute.

rising-threshold RISING_THRES: upper threshold, the value range is 0 ~ 2147483647.

event_Index: the index of event groups corresponding to the upper threshold, the range is 1-65535.

falling -threshold FALL_THRES: lower threshold, the value range is 0 ~ 2147483647.

event_Index: the index of event groups corresponding to the lower threshold, the range is 1-65535.

name: character string, creator of the row.

【Description】

rmon alarm: command is used to configure alarm group.

no rmon alarm: command is used to delete alarm group.

By default alarm group is not configured.

The alarm variable format support string format (not OID format), formats are etherStatsEntry.integer.instance or etherStatsString.instance, integer the range is 1-21, corresponding to the etherStatsString below respectively.

etherStatsString supports the following:

"etherStatsIndex"

"etherStatsDataSource"

"etherStatsDropEvents"

"etherStatsOctets"

"etherStatsPkts"

"etherStatsBroadcastPkts"

"etherStatsMulticastPkts"

"etherStatsCRCAlignErrors"

"etherStatsUndersizePkts"

"etherStatsOversizePkts"

"etherStatsFragments"

"etherStatsJabbers"

"etherStatsCollisions"

"etherStatsPkts64Octets"

"etherStatsPkts65to127Octets"

"etherStatsPkts128to255Octets"

"etherStatsPkts256to511Octets"

"etherStatsPkts512to1023Octets"

"etherStatsPkts1024to1518Octets"

"etherStatsOwner"

"etherStatsStatus"

Instance is an interface index.

【Instance】

```
Switch> enable
Switch#configure terminal
```

```
Switch(config)#rmon alarm 1 etherStatsIndex.1 interval 20 delta
rising-threshold 200 event 1 falling-threshold 20 event 1
```

20.2 RMON Statistical Group

【Command】

```
rmon collection stats <INDEX>
no rmon collection stats <INDEX>
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

INDEX:statistics group Index, the range is 1-65535.

【Description】

rmon collection stats: command is used to configure the port statistics group.

no rmon collection stats: command is used to cancel the port statistics group.

The port is not configured with statistics group by default.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#rmon collection stats 1
```

20.3 RMON History Group

【Command】

```
rmon collection history <INDEX> {buckets <NUMBER> | interval
<SECONDS> | owner <NAME> | }
no rmon collection history <INDEX>
```

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

INDEX: statistics group index, the range is 1-65535.

NUMBER: set the historical table capacity corresponding to the history group, ranging from 1-65535.

SECONDS: sets the historical group statistical cycle value in the range of 1-3600 seconds.

NAME: creator of the row.

【Description】

rmon collection history: command is used to configure the port history group.

no rmon collection stats: command is used to delete the port statistics group.

The port is not configured with history group by default.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#interface ge1
Switch(config-ge1)#rmon collection history 1 buckets 10 interval
60
```

20.4 RMON Event Group

【Command】

rmon event <INDEX> **{description** <STRING> **| log | trap** <COMMUNITY>**}**
(owner <NAME> **|)**
no rmon event <INDEX>

【View】

Ethernet port configuration mode

【Default Level】

2: Configuration level

【Parameter】

INDEX: event group index, the range is 1-65535.

Log: log events. When events are triggered, the system logs them.

STRING: event description.

community: Trap event. When the event is triggered, the system will send it with community as the group name

NAME: creator of the row.

【Description】

rmon event: command is used to configure the event group.

no rmon event: command is used to cancel the event group.

The port is not configured with event group by default.

【Instance】

```
Switch> enable
Switch#configure terminal
Switch(config)#rmon event 2 log
```

20.5 Display RMON Alarm Group Information

【Command】

show rmon alarm

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show rmon alarm: command is used to display alarm group information.

【Instance】

```
Switch> enable
Switch#show rmon alarm
 alarm Index = 1
alarm status = VALID
       alarm Interval = 20
```

```
        alarm Type is Delta
        alarm Value  = 0
        alarm Rising Threshold = 200
        alarm Rising Event = 1
        alarm Falling Threshold = 20
        alarm Falling Event = 1
        alarm Owner is RMON_SNMP

 alarm Index = 2
alarm status = VALID
        alarm Interval = 20
        alarm Type is Delta
        alarm Value  = 0
        alarm Rising Threshold = 200
        alarm Rising Event = 1
        alarm Falling Threshold = 20
        alarm Falling Event = 1
        alarm Owner is RMON_SNMP
```

20.6 Display RMON Statistics Information

【Command】

show rmon statistics

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show rmon statistics: command is used to display statistics group information.

【Instance】

```
Switch> enable
Switch#show rmon statistics
   rmon collection index 1
```

```
    stats->ifindex = 5002
    input packets 00, bytes 00, dropped 00, multicast packets 00
    output packets 00, bytes 3406566434058944, multicast packets
00 broadcast packets 00
```

20.7 Display RMON History Group Information

【Command】

show rmon history

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show rmon history: command is used to display history group information.

【Instance】

```
Switch> enable
Switch#show rmon history
       history index = 1
       data source ifindex = 5002
       buckets requested = 50
       buckets granted = 50
       Interval = 1800
       Owner RMON_SNMP
```

20.8 Display RMON Event Group Information

【Command】

show rmon event

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None

【Description】

show rmon event: command is used to display event group information.

【Instance】

```
Switch> enable
Switch#show rmon event
 event Index = 1
      Description RMON_SNMP
       Event type Log
      Last Time Sent = 07:43:20
      Owner  RMON_SNMP
```

21 Log Configuration

21.1 Log File Size Limit

【Command】

log file size <10-10000>

no log file size

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

<10-10000>: log file size, the unit is KB.

【Description】

log file size: the command is used to set the maximum size of logfile in KB.

no log file size: the command is used to delete the setting of logfile size and restore it to the default size, namely 2M.

【Instance】

```
# Configure the logfile size to 5M
Switch> enable
Switch#configure terminal
Switch(config)#log file size 5000

#Delete settings of logfile size
Switch> enable
```

```
Switch#configure terminal
Switch(config)#no log file size
```

21.2 Log stdout Display

【Command】

log stdout

no log stdout

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

No.

【Description】

log stdout: the command is used to open the switch and display the log information in stdout.

no log stdout: the command is used to close the switch and not to display the log information in stdout.

【Instance】

```
# Configure to open the log information displayed in stdout
Switch> enable
Switch#configure terminal
Switch(config)#log stdout

# close the log information displayed in stdout
Switch> enable
Switch#configure terminal
Switch(config)#no log stdout
```

21.3 LogInformation Highest Display Level

【Command】

Log trap (alerts | critical | debugging | emergencies | errors | informational | notifications | warnings)

no log trap

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

No.

【Description】

log trap: the command sets the maximum display level of log information.

no log trap: the command is used to remove the settings for the highest display level of log information and restore it to the default level, which is the "debug" level.

【Instance】

```
# set the log information for the highest level "informational”
Switch> enable
Switch#configure terminal
Switch(config)#log trap informational

# Delete the highest level Settings for log information
Switch> enable
Switch#configure terminal
Switch(config)#no log trap
```

21.4 Log Level Record Display

【Command】

log record-priority

no log record-priority

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

No.

【Description】

log record-priority: the command is used to open the level of log information, that is, to display the information according to the level of log information.

no log record-priority: the command is used to close the level of log information, and all log information is unified as debug level.

【Instance】

```
# Configure to open log information record-priority
Switch> enable
Switch#configure terminal
Switch(config)#log record-priority

# Close log information record-priority
Switch> enable
Switch#configure terminal
Switch(config)#no log record-priority
```

21.5 Syslog Server Download Log

【Command】

log syslog server <A.B.C.D> [<PORT>]

no log syslog server

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D: syslog server IP address

PORT: The port used by the syslog server.

【Description】

log syslog server: the command is used to set the IP address of the remote syslog server. After executing the command, the log information of the system will be sent to the syslog server with the specified IP address for processing remotely. The parameter A.B.C.D specifies the IP address used by the syslog server, and the parameter PORT specifies the port used by the syslog server.

no log syslog server: the command is used to delete the configuration of the remote syslog server. After executing the command, the system will no longer send log information to any remote syslog server, but only save the log information locally.

【Instance】

```
# configuration sends log information to syslog server 192.168.1.1
on port 8848
Switch> enable
Switch#configure terminal
Switch(config)#log syslog server 192.168.1.1 8848

#Disable the log sending function to the remote syslog server
Switch> enable
Switch#configure terminal
Switch(config)#no log syslog
```

22 NTP Configuration

22.1 NTP Server

【Command】

ntp server <A.B.C.D>
no ntp server <A.B.C.D | **all**>

【View】

Global configuration mode

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D: ntp server IP address.

【Description】

ntp server <A.B.C.D>: used to configure the IP address of ntp server and start the ntp service. The default ntp service is not enabled. Only one ntp server is currently supported.

no ntp server <A.B.C.D/all> : delete the configured ntp server IP address and disable the ntp service. A.B.C.D is the address of the NTP server that need to be deleted. Since the system currently supports at most one ntp server IP configuration, the two forms of this command achieve the same effect: delete all ntp server IP addresses and disable the ntp service.

【Instance】

```
# Enable ntp service and configure ntp server ip to 192.168.1.1
```

```
Switch> enable
Switch#configure terminal
Switch(config)#ntp server 192.168.1.1

# Delete all configured ntp server IP and disable the ntp service
(1)
Switch> enable
Switch#configure terminal
Switch(config)#no ntp server 192.168.1.1

# Delete all configured ntp server IP and disable the ntp service
(2)
Switch> enable
Switch#configure terminal
Switch(config)#no ntp server all
```

23 Network Diagnose Configuration

23.1 Ping Test

【Command】

ping WORD
ping ip WORD
ping ipv6 WORD
ping

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

WORD: the target IP address that needs to be checked for connectivity.

Ipv6: supported ipv6.

【Description】

None

【Instance】

```
Switch> enable
Switch#ping 192.168.1.188
PING 192.168.1.188 (192.168.1.188): 56 data bytes
64 bytes from 192.168.1.188: seq=0 ttl=128 time=1.493 ms
64 bytes from 192.168.1.188: seq=1 ttl=128 time=13.077 ms
```

```
--- 192.168.1.188 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 1.493/7.285/13.077 ms

*Switch#ping ipv6 fe80::01 (Ipv6 address needs to be configured
to fe80::02/64)
Output Interface: vlanif1
PING fe80::01 (fe80::1): 56 data bytes
64 bytes from fe80::1: seq=0 ttl=128 time=0.536 ms
64 bytes from fe80::1: seq=1 ttl=128 time=0.483 ms

--- fe80::01 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.483/0.509/0.536 ms
```

23.2 Traceroute Test

【Command】

```
traceroute ip WORD
traceroute ipv6 WORD
```

【View】

Privileged Exec Mode

【Default Level】

1: View level

【Parameter】

WORD: the connected destination IP address that needs to be checked.

Ipv6: supported ipv6.

【Description】

None

【Instance】

```
Switch> enable
Switch#traceroute ip 192.168.1.254
traceroute to 192.168.1.254 (192.168.1.254), 30 hops max, 38 byte
packets
 1  192.168.1.254 (192.168.1.254)  0.036 ms  0.033 ms  0.013 ms
```

```
*Switch#traceroute ipv6 fe80::01 (Ipv6 address needs to be
configured to fe80::02/64 )
Output Interface: vlanif1
traceroute to fe80::01 (fe80::1), 30 hops max, 16 byte packets
 1  fe80::1 (fe80::1)  1.144 ms  0.440 ms  0.346 ms
```

23.3 Port Loopback

【Command】

loopback IFNAME **internal mac**
loopback IFNAME **internal phy**
no loopback IFNAME **internal**

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

IFNAME: Specify the test port name.

Internal: represents an internal ring test.

mac/phy: the loop need to test is in the MAC layer or phy layer

【Description】

When the port loopback test is enabled, the port link light will be on, no execution will cancel the test, and the port link light will be off.

【Instance】

```
Switch> enable
Switch#loopback ge1 internal mac
Switch#no loopback ge1 internal
```

24 System Management

24.1 Device Information Display

24.1.1 Display System Version

【Command】

show version

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

None.

【Description】

show version: the command displays the current system version information.

【Instance】

```
# Display System Current Version Information
Switch> enable
Switch#show version
```

24.1.2 Display Product Information

【Command】

show product-info [<NAME>]

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

NAME: product information name, no parameters by default.

【Description】

show product-info [<NAME>]: the command is used to display the product information value of the given name, and all product information will be displayed when no parameters are provided.

【Instance】

```
# Display Product Information:
Switch> enable
Switch(config)#show product-info
```

24.2 System Software Upgrade

【Command】

copy tftp package <A.B.C.D> <WORD>

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D:tftp server ip address.

WORD: the name of the upgrade file

【Description】

copy tftp package: the command is used to upgrade the system software, in which the parameter A.B.C.D is the IP address of the tftp server, and WORD is the file name of “xxx.bin” for upgrade.

When files are uploaded and downloaded, the tftpd32 software can be used as the tftp server on the PC. When transferring files, make sure the TFTP server is enabled and the correct file path is used.

【Instance】

```
# Upgrade system WEB and product information
Switch> enable
Switch#copy tftp package 192.168.1.1 packetweb.bin

# Upgrade System Software
Switch> enable
Switch#copy tftp package 192.168.1.1 packetapp.bin
```

24.3 Configuration File Import and Export

24.3.1 Import Configuration File

【Command】

copy tftp startup-config <A.B.C.D> <WORD>

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D: tftp server ip address

WORD: the name of the upgraded configuration file.

【Description】

copy tftp startup-config: the command is used to upgrade the system configuration file, in which the parameter A.B.C.D is the IP address of the tftp server, and WORD is the name of the configuration file used for the upgrade.

【Instance】

```
# Upgrade System Configuration File
Switch> enable
Switch#copy tftp startup-config 192.168.1.1 SWOS.conf
```

24.3.2 Configure File Export

【Command】

copy flash startup-config <A.B.C.D> (WORD|)

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D: : tftp server ip address.

WORD: the name of the upgraded configuration file.

【Description】

copy tftp startup-config: the command is used to download starp-config files to the tftp server, in which the parameter A.B.C.D is the IP address of the tftp server, and WORD is the file name used when saving to the tftp server.

【Instance】

```
# upload startup-config to tftp server "192.168.1.1" and name it
"SWOS.conf”
Switch> enable
Switch#copy flash startup-config 192.168.1.1 SWOS.conf
```

24.4 Log File Export

【Command】

copy flash logfile <A.B.C.D> (WORD|)

【View】

Privileged Exec Mode

【Default Level】

2: Configuration level

【Parameter】

A.B.C.D: tftp server ip address.

WORD: the name of the upgraded configuration file.

【Description】

copy flash logfile: the command is used to download logfile to the tftp server, in which the parameter A.B.C.D is the IP address of the tftp server, and WORD is the file name used when saving to the tftp server.

【Instance】

```
# download logfile to tftp server "192.168.1.1" and name it
"message.log”
Switch> enable
Switch#copy flash logfile 192.168.1.1 message.log
```

24.5 Save Configuration

【Command】

copy running-config startup-config
write
do write

【View】

Privileged Exec Mode

Any

【Default Level】

2: Configuration level

【Parameter】

No.

【Description】

copy running-config startup-config: the command is used to cover the startup-config file with running-config, that is, to save running-config. running-config is the configuration file that is currently running, and startup-config is the configuration file that is currently saved. copy running-config startup-config is to execute a "write" and save the configuration file.

do write: command can perform the save configuration in any mode (except Privileged Exec Mode).

【Instance】

```
# Save running-config
Switch> enable
Switch#copy running-config startup-config
#or
Switch> enable
Switch#configure terminal
Switch(config)#do write
Building configuration...
[OK]
```

24.6 Reboot the Device

【Command】

reboot

【View】

Privileged Exec Mode

【Default Level】

1: view level

【Parameter】

None

【Description】

Reboot the device

【Instance】

```
Switch> enable
Switch#reboot
reboot system? (y/n): y
```

24.7 Restore Factory Settings

【Command】

erase startup-config
rm startup-config

【View】

Privileged Exec Mode

【Default Level】

1: Configuration level

【Parameter】

None

【Description】

Delete current configuration file.

【Instance】

```
Switch> enable
Switch#erase startup-config
erase startup-config ? (y/n): y
Switch#reboot
```

3onedata

3onedata Co., Ltd.

Headquarter Address:	3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China
Technology Support:	tech-support@3onedata.com
Service Hotline:	4008804496
Official Website:	http://www.3onedata.com