S3400-48T4SP Switch CLI Reference Guide

Model: S3400-48T4SP

CLI REFERENCE GUIDE

Contents

Chapter 1 Basic Configuration Commands

1.1 Commands for Managing Configuration Files

Commands for managing configuration files are shown in the following:

- copy
- delete
- dir
- ip address
- ip route
- show configuration
- format
- More

1.1.1 Copy

To read files from the TFTP server to the switch, run copy.

copy tftp<:filename> {**flash**<:filename>|rom} [ip_addr]

Parameters

Parameters	Description
tftp<:filename>	Reads files from the TFTP server. The filename parameter shows the corresponding file name. If the filename parameter is not designated, you are prompted to enter the file name after the copy command is run.
flash <:filename>	Writes files into the flash of the switch. The filename parameter shows the corresponding file name. If the filename parameter is not designated, you are prompted to enter the file name after the copy command is run.
rom	Updates the bootrom of the switch.
ip_addr	Means the IP address of the TFTP server. If this parameter is not designated, you are prompted to enter the IP address after the copy command is run.

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

None

Example

```
monitor#copy tftp:switch.bin flash:switch.bin 192.2.2.1
```

The example shows how to copy the switch.bin files from the TFTP server to the flash of the switch.

Related Command

None

1.1.2 Delete

To delete a file, run delete.

delete file-name

Parameters

Parameters	Description
file-name	Means a file name with up to 20 characters.

Default Value

If the file name is not entered, the startup-config files will be deleted by default.

Command Mode

Monitoring Mode

Usage Guidelines

None

Related Command

None

1.1.3 IP Address

To designate the IP address of the Ethernet port, run ip address in monitor status.

ip address ip-address mask

Parameters

Parameters	Description
ip-address	IP address
mask	Mask of the IP network

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

None

Example

```
monitor#ip address 192.168.1.1 255.255.255.0
```

Related Command

ip route

ping

1.1.4 IP Route

To designate a default gateway, run ip route in monitor status.

ip route default gw_ip_addr

Parameters

Parameters	Description
gw_ip_addr	Stands for a default gateway address.

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

None

Example

```
monitor#ip route default 192.168.1.3
```

Related Command

ip address

1.1.5 Show Configuration

To display the current configuration file of the system, run show configuration.

Parameters

None

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

None

Related Command

None

1.1.6 Format

To format the file system, run format in EXEC mode.

format

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

If the format command is used, all files in the file system will be lost.

Related Command

None

1.1.7 More

To display the content of a file, run more in EXEC mode.

more file-name

Parameters

Parameters	Description
file-name	Means a file name with up to 20 characters.

Default Value

None

Command Mode

EXEC

Usage Guidelines

If all characters in the file are legible, they are displayed in the ASCII code; otherwise, it will be displayed in the binary system.

Related Command

None

1.2 Basic System Management Commands

Basic System Management Commands

- bootflash
- cd
- chinese
- english

- date
- md
- pwd
- rd
- rename
- reboot
- show break
- alias
- boot system flash
- help
- show
- history
- show alias

1.2.1 boot flash

To start a device from the designated file in monitor mode, run the following command.

boot flash filename

Parameters

Parameters	Description
filename	Stands for the name of the designated file.

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

After a user enters the monitor state, you can use this command to start a device.

Example

```
monitor#boot flash switch.bin
```

Related Command

None

1.2.2 cd

To change the current directory, run the following command in the monitoring mode.

cd directory|.

Parameters

Parameters	Description
directory	Means a file name with up to 20 characters.
..	Parent directory

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

None

Example

```
monitor#cd my_dir
```

Related Command

pwd

1.2.3 chinese

To switch the command prompt to Chinese mode, use the chinese command.

Parameters

None

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

None

Example

None

Related Command

None

1.2.4 date

To set system absolute time, run command "date".

Parameters

None

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

This command is used to set the absolute time for the system. For the switch with a battery-powered clock, the clock will be powered by the battery. If the clock doesn't keep good time, you need to change the battery.

For the switch without a battery-powered clock, the system date is configured to Jan 1st,1970 after the reboot of the switch, and user needs to set the current time each time when starting the switch.

Example

```
monitor#date
The current date is 2000-7-27 21:17:24
Enter the new date(yyyy-mm-dd):2000-7-27
Enter the new time(hh:mm:ss):21:17:00
```

Related Command

None

1.2.5 english

To switch the command prompt to english mode, use the english command.

Parameters

None

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

None

Example

None

Related Command

None

1.2.6 md

md directory

Parameters

Parameters	Description
directory	Means a file name with up to 20 characters.

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

The command can be used to set a directory.

Related Command

None

1.2.7 pwd

Parameters

None

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

The command can be used to display the current directory.

Related Command

None

1.2.8 rd

rd directory

Parameters

Parameters	Description
directory	Means a file name with up to 20 characters.

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

The system prompts if the directory is not empty. The system prompts if the directory doesn't exist. To delete a command, use the rd command.

Related Command

None

1.2.9 rename

To rename a file in a file system, use the rename command.

rename old_file_name new_file_name

Parameters

Parameters	Description
old_file_name	The original filename.
new_file_name	The new filename.

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

None

Related Command

None

1.2.10 reboot

Parameters

None

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

The command can be used to reboot the switch.

Related Command

None

1.2.11 alias

alias alias_name command_line

Parameters

Parameters	Description
alias_name	Name the alias name.
command_line	The command of naming the alias name.

Default Value

None

Command Mode

Configuration mode

Usage Guidelines

The command can be used to replace "command_line" with "alias_name". For instance, alias update1 copy tftp:BDMSU8508_4.0.0B.bin flash:switch.bin 10.168.30.188. The command "copy tftp:BDMSU8508_4.0.0B.bin flash:switch.bin 10.168.30.188 " will automatically run on the switch only update 1 is input.

Example

Replace the command "copy tftp:MSU8508_4.0.0B.bin flash:switch.bin 10.168.30.188" with "update1".

alias update1 copy tftp:MSU8508_4.0.0B.bin flash:switch.bin 10.168.30.188

Related Command

None

1.2.12 boot system flash

To designate the systematic mirror file that will be executed when the system is started, run the following first command; to cancel this settings, run the following second command.

boot system flash filename

no boot system flash filename

Parameters

Parameters	Description
filename	Means a file name with up to 20 characters.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

If the user doesn't configure the command, the system will execute the first system mirror file of the flash file system. If the user configures with multiple commands, the system executes the mirror documents in turn. If the document doesn't exist or occurs mirror. The next file will be executed consecutively. If the file doesn't run successfully, the system enters the monitor mode.

Example

```
config#boot system flash switch.bin
```

Related Command

None

1.2.13 help

help

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

The command can be used to show the help system of the switch.

Example

The following example shows how to show the help system of the switch.

```
switch# help
```

Help may be requested at any point in a command by entering a question mark '?', If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument(e.g.'show ?') and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'interface e?'.)

Related Command

None

1.2.14 history

To show history command, run the following command. To return to the default setting, use the no form of this command.

[no] history [+ <count> | - <count> | clear]

Parameters

Parameters	Description
+ <count>	To display the count<1-20> historical command from the beginning to the end.
- <count>	To display the count<1-20> historical command from the end to the beginning.

Default Value

If there are no more than 20 commands executed, all historical command lines will be displayed from the beginning to the end. If there are more than 20 commands executed, all historical command lines will be displayed from the beginning to the end.

Command Mode

Any command mode

Usage Guidelines

The modularized switch can save up to 20 historical commands. You can invoke these commands with the "up" or “down” key or directly use it after edition. The command can be used to browse the history command. You can run the [no] history command to delete the history command.

Example

The following example shows how to display the latest 5 history commands from the end to the beginning.

```
switch#history - 5
config
int e1/1
no ip addr
ip addr 192.2.2.49 255.255.255.0
exit
```

Related Command

None

1.2.15 show

To display the relevant information of the system, which or specific ones of which can be filtered through the filter, run the following command:

show <sub-command> [| <begin | include | exclude | redirect> <WORD> [SEPARATOR WORD]]

Parameters

Parameters	Description
sub-command	Stands for a child command.
|	Uses the output filter.
begin	Means to show the result of the show command starting with a specific word.
include	Means to show the lines of the result of the show command containing a specific word.
exclude	Means not to show the lines of the result of the show command containing a specific word.
redirect	Redirects the result of the show command to the file in the designated file system.
WORD	Stands for a designated word, which is the designated filename as to the redirect command.
SEPARATOR WORD	Stands for the designated separator, which is space by default to separate the words.

Default Value

None

Command Mode

The EXEC mode or the configuration mode

Usage Guidelines

This command can be used to filter the useless information in the result of the show command, especially when the result is too much to read. For example, if you want to browse a designated MAC address in a MAC address table, which contains a lot of MAC addresses, this command will give you convenience for you.

Example

The following example shows how to display the lines, in which the word "interface" is contained, in the result of show running-config.

```
Switch#show running-config | include interface
Building configuration...



Current configuration:
!
interface GigaEthernet0/1
interface GigaEthernet0/2
interface GigaEthernet0/3
interface GigaEthernet0/4
interface GigaEthernet0/5
interface GigaEthernet0/6
interface GigaEthernet0/7
interface GigaEthernet0/8
```

Related Command

None

1.2.16 show alias

To display all aliases or the designated alias, run the following command.

show alias [<alias name>]

Parameters

Parameters	Description
alias name	Name the alias name.

Default Value

Display all aliases according the format "alias name=command line".

Command Mode

The EXEC mode or the configuration mode

Usage Guidelines

None

Example

The following example shows how to display all aliases of the current system:

```
switch_config#show alias
hualab=date
router=snmp
```

Related Command

alias

1.2.17 show break

It is used to display the abnormal information of the system. The system stores all abnormal information in the latest running. The abnormal information contains the times of abnormity, the stack content and the invoked functions when abnormity occurs.

Parameters

None

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

The command is only used for debugging.

Related Command

None

1.3 Telnet Configuration Commands

The chapter describes telnet and relative commands. The telnet command is used to establish a session with the remote server. The telnet command is always working at the UNIX operating systems. Option negotiation is required. Telnet does not provide itself the login authentication. Telnet is different from Rlogin because telnet does not provide itself password check.

The telnet configuration commands include:

- telnet
- ip telnet
- where
- disconnect
- resume
- clear Telnet
- show Telnet
- debug Telnet

1.3.1 telnet

To establish a telnet session, run the following command:

telnet *server-ip-addr/server-host-name* [**/port** *port*][**/source-interface** *interface*] [**/local** *local-ip-addr*] [**/debug**] [/**echo | /noecho**] [**/script** *scriptname*]

Parameters

Parameters	Description
server-ip-addr	Dotted-decimal IP address of the remote server
server-host-name	Name of the remote server, which is configured by the ip host command
Port	Telnet port of the remote server
interface	Local interface where the telnet connection is originated
local-ip-addr	Local IP address where the telnet connection is originated
/debug	A negotiation process for enabling the debug at the client side and printing the connection
/echo/noecho	Enable or disable the local echo. The default value is noecho.
Script name	A script name used for auto login

Default Value

The default port number is 23. The interface has no default number.

Command Mode

EXEC and global configuration mode

Usage Guidelines

You can use one of the following command lines to establish a remote login.

telnet server-ip-addr/server-host-name

In this case, the application program directly sends the telnet login request to port 23 of the remote server. The local IP address is the IP address which is nearest to the peer and found by the routing table.

telnet server-ip-addr/server-host-name /port port

In this case, the application program sends a telnet login request to the port of the peer.

telnet server-ip-addr/server-host-name /source-interface interface

In this case, the application program uses the IP address on the interface ass the local IP address.

telnet server-ip-addr/server-host-name /debug

In this case, the application program opens the debug and exports the connection at the client side.

telnet server-ip-addr/server-host-name echo/noecho

In this case, the application program enables or disables the local echo. The local echo is disabled by default. Only when the server is not in charge of echo is the local echo enabled.

telnet server-ip-addr/server-host-name /script scriptname

Before executing the automatic login command of the script, run the command ip telnet script to configure the script.

The previous commands can be used together.

During the session with the remote server, you can press the Q button to exit the session. If the session is not manually quit, the session will be complete after a10-second timeout.

Example

Suppose you want to telnet server 192.168.20.124, the telnet port of the server is port 23 and port 2323, and the local two interfaces are e1/1(192.168.20.240) and s1/0(202.96.124.240). You can run the following operations to complete the remote login.

1. telnet 192.168.20.124 /port 2323

In this case, the telnet connection with port 2323 of the peer is to be established. The local IP address of the peer is 192.168.20.240.

2. telnet 192.168.20.124 /source-interface vlan2

In this case, the telnet connection with port 23 of the peer is to be established. The local IP address of the peer is 202.96.124.240.

3. telnet 192.168.20.124 /local 192.168.20.240

In this case, the telnet connection with port 23 of the peer is to be established. The local IP address of the peer is 192.168.20.240.

4. telnet 192.168.20.124 /debug

In this case, the telnet connection negotiation with port 23 of the peer will be printed out.

5. telnet 192.168.20.124 /echo

In this case, the local echo is enabled. If the echo is also enabled at the server side, all input will be echoed twice.

6. telnet 192.168.20.124 /script s1

Use login script S1 for automatic login.

1.3.2 ip telnet

To establish a telnet session, run the following command.

ip telnet max-user num

ip telnet enable

ip telnet source-interface vlan value

ip telnet access-class accesslist

ip telnet listen-port start-port [end-port]

ip telnet script scriptname 'user_prompt' user_answer 'pwd_prompt' pwd_answer

Parameters

Parameters	Description
num	telnet maximum connections
value	Local interface where the telnet request is originated
accesslist	Access list name to limit the source address when the local client receives the connection
start-port	Starting port number designated at the listening port area
end-port	End port number designated at the listening port area
scriptname	Name of the login script
user_prompt	Username prompt returned by the telnet server
user_answer	Username response information from the client side
pwd_prompt	Password prompt returned by the telnet server
pwd_answer	Password response information submitted by the client side

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

• Run the following command to configure the local interface for originating the telnet connection:

ip telnet source-interface interface

In this case, all telnet connections originated afterwards are through the interface. The configuration command is similar to the command telnet source-interface interface. However, the telnet command has no interface parameters followed. When the configured interface and the telnet command has interface parameters, it will use the interface followed the telnet command.

• Run the following command to configure the name of the access list which performs limitation on local telnet connection reception.

ip telnet access-class accesslist

In this case, the access list will be checked when the server accepts all telnet connections.

• Run the following command to configure a port, except the default port 23, to receive the telnet service.

ip telnet listen-port start-port [end-port]

NOTE: If the end port number is not designated, the listening will be executed at a specific port. The number of the designated ports cannot be bigger than 16 and the port number ranges between 3001 and 3999.

• Run the following command to configure the telnet login script.

ip telnet script s1 'login:' switch 'Password:' test

NOTE: When the script is configured, the username prompt and password prompt and their answers must be correctly matched, especially the prompt information is capital sensitive and has inverted comma ('). If one of them is wrongly configured, the automatic login cannot be performed.

NOTE: You can add the NO prefix on the above four commands and then run them to cancel previous configuration.

Example

1. ip telnet source-interface vlan1

In this case, the s1/0 interface will be adopted to originate all telnet connections afterwards.

2. ip telnet access-class abc

In this case, all the received telnet connections use access list abc to perform the access list check.

3. ip telnet listen-port 3001 3010

Except port 23, all ports from port 3001 to port 3010 can receive the telnet connection.

4. ip telnet script s1 'login:' switch 'Password:' test

The login script s1 is configured. The username prompt is login: and the answer is switch. The password prompt is Password: and the answer is test.

1.3.3 ctrl-shift-6+x (the current connection is mounted)

To mount the current telnet connection, run the following command:

ctrl-shift-6+x

Parameters

None

Default Value

None

Command Mode

Any moment in the current telnet session

Usage Guidelines

You can use the shortcut key to mount the current telnet connection at the client side.

Example

```
switchA>telnet 192.168.20.1
Welcome to Multi-Protocol 2000 Series switch
switchB>ena
switchB#(press ctrl-shift-6+x)
switchA>
You press ctrl-shift-6+x to mount the telnet connection to switch B and return to the current state of switch A.
```

1.3.4 where

To check the currently mounted telnet session, run the following command:

where

Parameters

None

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to check the mounted outward telnet connection at the client side. The displayed information contains the serial number, peer address, local address and local port.

NOTE: The **where** command is different from the **show telnet** command. The former is used at the client side and the displayed information is the outward telnet connection.

Example

```
switchA>telnet 192.168.20.1
Welcome to Multi-Protocol 2000 Series switch
switchB>ena
switchB#(press ctrl-shift-6+x)
switchA> telnet 192.168.20.2
Welcome to Multi-Protocol 2000 Series switch
switchC>ena
switchC#(press ctrl-shift-6+x)
switch A>where
NO.          Remote Addr      Remote Port          Local Addr      Local Port
  1        192.168.20.1               23     192.168.20.180           20034
  2        192.168.20.2               23     192.168.20.180           20035
```

Enter where at switch A. The mounted outward connection is displayed.

1.3.5 **resume** To resume the currently mounted outward telnet connection, run the following command:

resume no

Parameters

Parameters	Description
no	Number of the currently mounted telnet session that is checked through the where command

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to resume the currently mounted outward telnet connection at the client side.

Example

```
switch A>telnet 192.168.20.1
Welcome to   Multi-Protocol 2000 Series switch
switch B>ena
switch B#(press ctrl-shift-6+x)
switch A> telnet 192.168.20.2
Welcome to Multi-Protocol 2000 Series switch
switch C>ena
switch C#(press ctrl-shift-6+x)
switch A>where
NO.        Remote Addr      Remote Port        Local Addr       Local Port
  1        192.168.20.1              23    192.168.20.180            20034
  2        192.168.20.2              23    192.168.20.180            20035
switch A>Resume 1
  [Resuming connection 1 to 192.168.20.73. . . ]
(enter)
switchB#
```

After you enter where at switch A and the mounted outward connection of switch A is displayed, enter Resume1.You will be prompted that connection 1 is resumed. The command prompts of switch B are displayed after the Enter key is pressed.

1.3.6 disconnect

To clear the currently mounted outward telnet session, run the following command:

disconnect no

Parameters

Parameters	Description
no	Number of the currently mounted telnet session that is checked through the where command

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to clear the currently mounted outward telnet connection at the client side.

NOTE: The **disconnect** command is different from the **clear telnet** command. The former is used at the client side and clears the outward telnet connection. The latter is used at the server and clears the inward telnet connection.

Example

```
switch A>telnet 192.168.20.1
        Welcome to Multi-Protocol 2000 Series switch
Switch B>ena
switchB#(press ctrl-shift-6+x)
switch A> telnet 192.168.20.2
        Welcome to Multi-Protocol 2000 Series switch
Switch C>ena
Switch C#(press ctrl-shift-6+x)
switch A>where
NO.     Remote Addr     Remote Port     Local Addr      Local Port
 1      192.168.20.1        23          192.168.20.180     20034
 2      192.168.20.2        23          192.168.20.180     20035
switch A>disconnect 1
<Closing connection to 192.168.20.1> <y/n>y

 Connection closed by remote host.
switch A>
```

After you enter where at switch A and the mounted outward connection of switch A is displayed, enter disconnect 1. You will be prompted whether the connection of switch B is closed. After you enter Y, the connection is closed.

1.3.7 clear telnet

To clear the telnet session at the server, run the following command:

clear telnet no

Parameters

Parameters	Description
no	Number of the telnet session that is displayed after the show telnet command is run

Default Value

None

Command Mode

EXEC

Usage Guidelines

The command can be used to clear the telnet session at the server.

Example

clear telnet 1

The telnet session whose sequence number is 1 is cleared at the server (192.168.20.220:1097).

1.3.8 show telnet

To display the telnet session at the server, run the following command:

show telnet

Parameters

None

Default Value

None

Command Mode

All command modes except the user mode

Usage Guidelines

The command can be used to display the telnet session at the server. The displayed information includes the sequence number, peer address, peer port, local address and local port.

Example

```
Switch# show telnet
If you run the previous command, the result is shown as follows:
NO.       Remote Addr      Remote Port      Local Addr      Local Port
1      192.168.20.220          1097      192.168.20.240          23
2      192.168.20.180         14034      192.168.20.240          23
```

1.3.9 debug telnet

The following is a format of the debug command for the telnet session:

debug telnet

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

The command can be used to enable the switch of the telnet debug.

If the switch of the telnet debug is enabled, the negotiation processes of all the incoming telnet sessions are printed on the window that the debug command invokes. The debug telnet command is different from the telnet debug command. The former is to export the debug information of the telnet session connected to the server. The latter is to export the debug information of the telnet session that the client originates.

Example

debug telnet

The debug information of the telnet session that is connected to the server is displayed.

1.4 Terminal Configuration Commands

The terminal configuration commands include:

- attach-port
- auto command
- clear line

- connect
- disconnect
- exec-timeout
- length
- line
- location
- login authentication
- monitor
- no debug all
- password
- resume
- show debug
- show line
- terminal-type
- terminal monitor
- terminal width
- terminal length
- where
- width

1.4.1 attach-port

To bind the telnet listening port to the line vty number and enable the telnet connection at a specific port generates vty according to the designated sequence number, run the following command:

[no] attach-port PORT

Parameters

Parameters	Description
Port	Listening port of the telnet server (3001-3999)

Default Value

None

Command Mode

Line configuration mode

Example

Bind listening port 3001 to line vty 2 3.

```
switch_config# line vty 2 3
switch_config_line#attach-port 3001
```

1.4.2 auto command

To set the automatically-run command when user logs in to the terminal, run the following command. The connection is cut off after the command is executed.

auto command LINE

no auto command

Parameters

Parameters	Description
LINE	Command to be executed

Command Mode

Line configuration mode

Example

```
switch_conf#line vty 1
switch_conf_line#autocommand pad 123456
```

After you successfully log in, the host whose X.121 address is 123456 will be automatically padded.

1.4.3 clear line

To clear the designated line, run the following command:

clear line [console | vty] [number]

Parameters

Conform to the line command

Command Mode

EXEC

Example

```
switch#clear line vty 0
```

1.4.4 connect

To connect Telnet server, run the following command:

connect *server-ip-addr/server-host-name* {[/**port** *port*][/**source-interface** *interface*] [/**local** *local-ip-addr*]} [/**script** *word*]

Parameters

Parameters	Description
server-ip-addr/server-host-name	IP address or host name of the server
Port	Port number
interface	Interface name where the Telnet connection is originated
local-ip-addr	Local IP address where the telnet connection is originated
word	Name of the script

Command Mode

All Configuration Modes

Example

```
switch# connect 192.168.20.1
```

1.4.5 disconnect

To delete the suspended telnet session, run the following command:

disconnect N

Parameters

Parameters	Description
N	number of the suspended telnet dialog

Command Mode

All Configuration Modes

Example

```
switch#disconnect 1
```

1.4.6 exec-timeout

To set the max idle time of the terminal, run the following command:

[no] exec-timeout [time]

Parameters

Parameters	Description
time	Idle time in seconds Value range: 0-86400

Default Value

0 (no time-out limit)

Command Mode

Line configuration mode

Example

The following example shows how to set the idle time of the line to 1 hour.

switch_config_line#exec-timeout 3600

1.4.7 length

To set the line number on the screen of the terminal, run the following command:

[no] length [value]

Parameters

Parameters	Description
value	Value range: 0 to 512. The value 0 means there is no pause.

Default Value

24

Command Mode

Line configuration mode

1.4.8 line

To enter the line configuration mode, run the following command:

line [console |vty] [number]

Parameters

Parameters	Description
console	Monitoring line, which has only one number 0
vty	Virtual lines such as Telnet, PAD and Rlogin
number	Number in the line of the type

Command Mode

Global configuration mode

Example

The following example shows how to enter the line configuration mode of VTY 0 to 10.

```
switch_config#line vty 0 10
```

1.4.9 location

To record the description of the current line, run the following command:

location [LINE]

no location

Parameters

Parameters	Description
LINE	Description of the current line

Command Mode

Line configuration mode

1.4.10 login authentication

To set line login authentication, run the following command:

[no] login authentication [default | WORD]

Parameters

Parameters	Description
default	Default authentication mode
WORD	Name of the authentication list

Command Mode

Line configuration mode

Example

```
switch_conf_line#login authentication test
```

The above example shows how to set the authentication list of the line to test.

1.4.11 monitor

To export the log and debugging information to the line, run the following command:

[no] monitor

Parameters

None

Command Mode

Line configuration mode

Example

```
switch_config_line#monitor
```

1.4.12 no debug all

To shut down all debugging output of the current VTY, run the following command:

no debug all

Parameters

None

Command Mode

EXEC

Example

```
switch#no debug all
```

1.4.13 password

To set the password for the terminal, run the following command:

password {password | [encryption-type] encrypted-password}

no password

Parameters

Parameters	Description
password	Password configured on the line, which is entered in the plaintext form and whose maximum length is 30 bits.
[encryption-type] encrypted-password	encryption-type means the encryption type of the password. Currently, products only support two encryption modes: 0 and 7. The number 0 means the password is not encrypted and the plaintext of password is directly entered. It is the same as the way of directly entering the password. The number 7 means the password is encrypted through an algorithm. You need to enter the encryption text for the encrypted password. The encryption text can be copied from the configuration files of other switches.

For password encryption, refer to the explanation of the commands service **password-encryption and enable password.**

Command Mode

Line configuration mode

Example

```
switch_conf#line vty 1
switch_conf_line#password test
```

The above example shows how to set the login password of VTY1 to test.

1.4.14 resume

To resume the mounted telnet session, run the following command:

resume N

Parameters

Parameters	Description
N	number of the suspended telnet dialog

Command Mode

All Configuration Modes

Example

```
switch#resume 1
```

1.4.15 show debug

To display all debugging information of the current VTY, run the following command:

show debug

Parameters

None

Command Mode

EXEC or global configuration mode

Example

```
Switch# show debug
http authentication debug is on
http cli debug is on
http request debug is on
http response debug is on
http session debug is on
http erro debug is on
http file debug is on
TELNET:
Incoming Telnet debugging is on
```

1.4.16 show line

To display the status of the current effective line, run the following command:

show line {[console | **vty**] [number]}

Parameters

If there is no parameter followed, the status of all effective lines will be displayed.

The definition of other parameters is similar to that of the line command.

Command Mode

Non-user mode

1.4.17 terminal length

To change the line number on the current terminal screen, run the following command. The parameter can be obtained by the remote host. The rlogin protocol uses the parameter to notify the remote UNIX host. Run the no terminal length command to resume the default value:

terminal length length

no terminal length

Parameters

Parameters	Description
length	Line number displayed on each screen Value range: 0-512

Default Value

Pause when 24 lines are displayed on the screen.

Command Mode

Global configuration mode

Usage Guidelines

This command only takes effect on the current terminal. When a session is terminated, the attributes of this terminal are also gone.

Example

```
switch#terminal length 40
```

Related Command

line

1.4.18 terminal monitor

To display the output debug and the system error information, run the following command. To shutdown the monitor, use the no form of this command.

terminal monitor

no terminal monitor

Parameters

None

Default Value

The system's console port is enabled by default, while other terminals are disabled by default.

Command Mode

Global configuration mode

Usage Guidelines

This command only takes effect on the current terminal. When a session is terminated, the attributes of this terminal are also gone.

Example

```
switch#terminal monitor
```

Related Command

line

debug

1.4.19 terminal width

In default settings, the switch is to export 80 characters in each line. If the default settings cannot meet your requirements, you can reset it. The parameter can be obtained by the remote host. To set the character number in each line, run the following command. To return to the default setting, use the no form of this command.

terminal width number

no terminal width

Parameters

Parameters	Description
number	Character number of each line

Default Value

80 characters in each line

Command Mode

Global configuration mode

Usage Guidelines

This command only takes effect on the current terminal. When a session is terminated, the attributes of this terminal are also gone.

Example

```
switch#terminal width 40
```

Related Command

line

1.4.20 terminal-type

To set the terminal type, run the following command:

[no] terminal-type [name]

Parameters

Parameters	Description
name	Terminal name (Terminal types currently supported are VT100, ANSI andVT100J.)

Default Value

ANSI

Command Mode

Line configuration mode

1.4.21 where

To check the currently mounted telnet session, run the following command:

where

Parameters

None

Command Mode

All Configuration Modes

Example

```
switch#where
```

1.4.22 width

To set the terminal width of the line, run the following command:

[no] width [value]

Parameters

Parameters	Description
value	Value range: 0 to 256. The value 0 means no execution.

Default Value

80

Command Mode

Line configuration mode

1.5 Network Testing Tool Commands

1.5.1 ping

To test host accessibility and network connectivity, run the following command. After the ping command is run, an ICMP request message is sent to the destination host, and then the destination host returns an ICMP response message.

ping [-a][-d][-f] [-i {source-ip-address}] [-m {source-interface}] [-j host1 [host2 host3 …]] [–k host1 [host2, host3 …]] [-l length] [-n number] [-r hops] [-s tos] [-t ttl] [-v] [-w waittime] [–b interval] [-c] host

Parameters

Parameters	Description
-a	Sets the ping command keeping running until it is interrupted.
-d	Sets the direct routing to the port without checking the routing table when forwarding the packet.
-f	Sets the DF digit (message is not segmented). If the message required to be sent is larger than the MTU of the path, the message will be dropped by the routing switch on the path and the routing switch will then return an ICMP error message to the source host. If network performance has problems, one node in the network may be configured to a small MTU. You can use the –f option to decide the smallest MTU on the path. Default value: No resetting
-i	Sets the source IP address of the message or the IP address of an interface. Default value: Main IP address of the message-sending interface
source-ip-address	Source IP address adopted by the message
source-interface	Message takes the IP address of the source-interface interface as the source address.
-j host1 [host2 host3…]	Sets the relaxation source route. Default: Not set
-k host1 [host2 host3…]	Sets the strict source route Default: Not set
-l length	Sets the length of ICMP data in the message. Default: 56 bytes
-n number	Sets the total number of messages. Default: 5 messages
-r hops	Records routes. Up to hops routes are recorded. Default: not record
-s tos	Sets IP TOS of the message to tos. Default Value:0.
-t ttl	Sets IP TTL of the message to ttl. Default Value:255.
-v	Detailed output
-w waittime	Time for each message to wait for response Default Value:2seconds.
-b interval	Sets the time interval of sending ping packet. Unit: 10ms; Value range: 0-65535; Default Value: 0.
-c	Simple output
host	Destination host

Command Mode

EXEC and global configuration mode

Usage Guidelines

The command supports that the destination address is the broadcast address or the multicast address. If the destination address is the broadcast address (255.255.255.255) or the multicast address, the ICMP request message is sent on all interfaces that support broadcast or multicast. The routing switch is to export the addresses of all response hosts. By pinging multicast address224.0.0.1, you can obtain the information about all hosts in directly-connected network segment that support multicast transmission.

Press the Q key to stop the ping command.

Simple output is adopted by default.

Parameters	Description
!	A response message is received.
.	Response message is not received in the timeout time.
U	The message that the ICMP destination cannot be reached is received.
Q	The ICMP source control message is received.
R	The ICMP redirection message is received.
T	The ICMP timeout message is received.
P	The ICMP parameter problem message is received.

The statistics information is exported:

Parameters	Description
packets transmitted	Number of transmitted messages
packets received	Number of received response messages, excluding other ICMP messages
packet loss	Rate of messages that are not responded to
round-trip min/avg/max	Minimum/average/maximum time of a round trip (ms)

Example

```
switch#ping -l 10000 -n 30 192.168.20.125
PING 192.168.20.125 (192.168.20.125): 10000 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 192.168.20.125 ping statistics ---
30 packets transmitted, 30 packets received, 0% packet loss
round-trip min/avg/max = 50/64/110 ms
```

1.5.2 traceroute

To detect which routes have already reached the destination, run the following command.

You can transmit to the destination the UDP packets (or ICMP ECHO packets) of different TTLs to confirm which routes have come to the destination. Each router on this path has to deduct 1 from the TTL value before forwarding ICMP ECHO packets. Speaking from this aspect, TTL is an effective hop count. When the TTL value of a packet is deducted to zero, the router sends back to the source system the ICMP timeout message. Send the first response packet whose TTL is 1 and send TTL plus 1 subsequently until the target reaches to the max TTL.

By checking the ICMP timetout message sent back by inter medial routers, you can confirm the routers. At the arrival of the destination, the traceroute sends a UPD packet whose port ID is larger than 30000; the destination node hence can only transmit back a Port Unreachable ICMP message. This reception of this message means the arrival of destination.

traceroute [-i source-ip-address] [-m source-interface}] [-j host1 [host2 host3 …]] [–k host1 [host2, host3 …]] [-p port-number] [-q probe-count] [-r hops] [-t ttl] [-w waittime] [-x icmp] host

Parameters

Parameters	Description
-i source-ip-address	Sets the source IP address of packet.
-m source-interface	Sets the packet-transmitted port.
-j host1 [host2 host3…]	Sets the relaxation source route. Default: Not set
-k host1 [host2 host3…]	Sets the strict source route Default: Not set
-p port-number	Sets the ID of destination port that transmits UDP packets. Default value: 33434 Default: 33434
-q probe-count	Sets the number of packets that you detect each time. Default: 3 messages
-r hops	Records routes. Up to hops routes are recorded. Default: not record
-t ttl	Sets IP TTL of the message to ttl. Default: the minimum and maximum TTLs are 1 and 30 respectively.
-w waittime	Time for each message to wait for response Default: 3 seconds
-x icmp	Sets the detection packet to be the ICMP ECHO packet. Default: UDP packet
host	Destination host

Command Mode

EXEC and global configuration mode

Usage Guidelines

The UDP packet is used for detection by default, but you can run –x icmp to replace it with ICMP ECHO for detection.

If you want to stop traceroute, press q or Q.By default, the simple output information is as follows.

Simple output is adopted by default.

Parameters	Description
!N	Receives an ICMP-route unreachable packet.
!H	Receives an ICMP-host unreachable packet.
!P	Receives an ICMP-protocol unreachable packet.
!F	Receives an ICMP unreachable (need to be fragmented) packet.
!S	Receive an ICMP unreachable (failing to detect the source-station route) packet.

The statistics information is exported:

Parameters	Description
hops max	Means the maximum detection hops (the threshold of ICMP).
byte packets	Stands for the size of each detection packet.

Example

```
switch#traceroute 90.1.1.10
traceroute to 90.1.1.10 (90.1.1.10), 30 hops max, 36 byte packets
 1   90.2.2.1   0 ms   0 ms   0 ms
 2   90.1.1.10   0 ms   0 ms   0 ms
```

1.1.8 dir

To display a file and a directory, run dir.

dir file-name

Parameters

Parameters	Description
file-name	Means a file name with up to 20 characters.

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

None

Related Command

None

1.6 Fault Diagnosis Commands

The chapter describes the commands used for fault diagnosis. All the following commands are used to detect the reason of the fault. You can use other commands to remove the fault, such as the debug command.

The chapter only introduces the universal diagnosis commands. For more details, please refer to the Fault Diagnosis White Paper.

The fault diagnosis commands include:

- logging
- logging buffered
- logging console
- logging facility
- logging monitor
- logging on
- logging trap
- logging command
- logging source-interface
- logging history alerts
- logging history critical
- logging history debugging
- logging history emergencies
- logging history errors
- logging history informational
- logging history notifications
- logging history warnings
- logging history rate-limit

- logging history size
- service timestamps
- clear logging
- show break
- show debug
- show logging

1.6.1 logging

To display the state of logging (syslog), run the following command. To return to the default setting, use the no form of this command.

logging A.B.C.D level

no logging A.B.C.D level

Parameters

Parameters	Description
A.B.C.D	IP address of the syslog server
level	Level of log information on the server Refer to table 1.

Default value

The log information is not recorded to the server.

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to record the log information to the designated syslog server. The command can be used for many times to designate multiple syslog servers.

Example

logging 192.168.1.1 errors

Related Command

logging trap

1.6.2 logging buffered

To record the log information to the memory of the switch, run the following command.

logging buffered [size | level | dump]

no logging buffered

Parameters

Parameters	Description
size	Size of memory cache Value range: 4096-2147483647 Unit: byte
level	Information level of the log recorded to memory cache Refer to table 1.
dump	When the system has abnormality, the information in the current memory is currently recorded to the flash and the information is resumed after the system is restarted.

Default Value

The information is not recorded to the memory cache.

Command Mode

Global configuration mode

Usage Guidelines

The command records the log information to the memory cache of the switch. The memory cache is circularly used. After the memory cache is fully occupied, the latter information will cover the previous information.

You can use the show logging command to display the log information recorded in the memory cache of the switch.

Do not use big memory for it causes the shortage of memory.

Table 1 Level of log recording

Prompt	Level	Description	Syslog definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Related Command

clear logging

show logging

1.6.3 logging console

To control the information volume displayed on the console, run the following command.

To forbid the log information to be displayed on the console, use the no form of this command.

logging console level

no logging console

Parameters

Parameters	Description
level	Information level of the logs displayed on the console Refer to table 2.

Default Value

The log level displayed on the console port is debugging by default.

Command Mode

Global configuration mode

Usage Guidelines

After the information level is specified, information of this level or the lower level will be displayed on the console.

Run the command show logging to display the currently configured level and the statistics information recorded in the log.

Table 2 Level of log recording

Prompt	Level	Description	Syslog definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

logging console alerts

Related Command

logging facility

show logging

1.6.4 logging facility

To record specified error information, run the following command. To restore to local7, use the no form of this command.

logging facility facility-type

no logging facility

Parameters

Parameters	Description
facility-type	Facility type Refer to table 3.

Default Value

local7

Command Mode

Global configuration mode

Usage Guidelines

Table 3 Facility type

Type	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Reserved for locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Example

logging facility kern

Related Command

logging console

1.6.5 logging monitor

To control the information volume displayed on the terminal line, run the following command.

To forbid the log information to be displayed on the terminal line, use the no form of this command.

logging monitor level

no logging monitor

Parameters

Parameters	Description
level	Information level of the logs displayed on the terminal line Refer to table 4.

Default Value

debugging

Command Mode

Global configuration mode

Usage Guidelines

Table 4 Level of log recording

Prompt	Level	Description	Syslog definition
emergencies	0	System is unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

logging monitor errors

Related Command

terminal monitor

1.6.6 logging on

To control the recording of error information, run the following command.

To forbid all records, use the no form of this command.

logging on

no logging on

Parameters

None

Default Value

logging on

Command Mode

Global configuration mode

Example

```
switch_config# logging on
switch_config# ^Z
switch#
Configured from console 0 by DEFAULT
switch# ping 192.167.1.1

switch#ping 192.167.1.1
PING 192.167.1.1 (192.167.1.1): 56 data bytes
!!!!!
--- 192.167.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/4/10 ms
switch#IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending
IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending
IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending
IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending
IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd
IP: s=192.167.1.111 (local), d=192.167.1.1 (FastEthernet0/0), g=192.167.1.1, len=84, sending
IP: s=192.167.1.1 (FastEthernet0/0), d=192.167.1.111 (FastEthernet0/0), len=84,rcvd

switch_config# no logging on

switch_config# ^Z
switch#
switch# ping 192.167.1.1
PING 192.167.1.1 (192.167.1.1): 56 data bytes
!!!!!
--- 192.167.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/4/10 ms
```

Related Command

logging

logging buffered

logging monitor

logging console

1.6.7 logging trap

To control the information volume recorded to the syslog server, run the following command.

To forbid the information to be recorded to the syslog server, use the no form of this command.

logging trap level

no logging trap

Parameters

Parameters	Description
level	Information level of the logs displayed on the terminal line Refer to table 5.

Default Value

Informational

Command Mode

Global configuration mode

Usage Guidelines

Table 5 Level of log recording

Prompt	Level	Description	Syslog definition
emergencies	0	System is unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Example

logging 192.168.1.1

logging trap notifications

Related Command

logging

1.6.8 logging command

To enable the command execution recording, run logging command. After this function is enabled will be generated for each of all entered commands, in which the line to execute this command, the command line, the execution result, the login line and the login address will be recorded.

To disable this function, use the no form of this command.

Parameters

None

Default Value

no logging command

Command Mode

Global configuration mode

Example

```
Switch_config#logging command
Switch_config#Jul 11 15:26:56 %CMD-6-EXECUTE: `logging command ` return 0, switch (vty 0, 192.168.25.42).
```

Related Command

logging

1.6.9 logging source-interface

To set the source port of log exchange, run the following command.

You can use no logging source-interface to disable this function.

Parameters

None

Default Value

no logging source-interface

Command Mode

Global configuration mode

Example

```
Switch_config# logging source-interface vlan 1
```

Related Command

logging

1.6.10 logging history alerts

To set the level of the historical log table to alerts (need to act immediately), run the following command.

Parameters

None

Default Value

logging history warnings

Command Mode

Global configuration mode

Example

```
Switch_config#logging history alerts
```

Related Command

logging

1.6.11 logging history critical

To set the level of the historical log table to critical, run the following command.

Parameters

None

Default Value

logging history warnings

Command Mode

Global configuration mode

Example

```
Switch_config#logging history critical
```

Related Command

logging

1.6.12 logging history debugging

This command is used to set the level of the historical log table to debugging.

Parameters

None

Default Value

logging history warnings

Command Mode

Global configuration mode

Example

```
Switch_config#logging history debugging
```

Related Command

logging

1.6.13 logging history emergencies

To set the level of the historical log table to emergencies, run the following command:

Parameters

None

Default Value

logging history warnings

Command Mode

Global configuration mode

Example

```
Switch_config#logging history emergencies
```

Related Command

logging

1.6.14 logging history errors

This command is used to set the level of the historical log table to errors.

Parameters

None

Default Value

logging history warnings

Command Mode

Global configuration mode

Example

```
Switch_config#logging history errors
```

Related Command

logging

1.6.15 logging history informational

This command is used to set the level of the historical log table to informational.

Parameters

None

Default Value

logging history warnings

Command Mode

Global configuration mode

Example

```
Switch_config#logging history informational
```

Related Command

logging

1.6.16 logging history notifications

This command is used to set the level of the historical log table to notifications.

Parameters

None

Default Value

logging history warnings

Command Mode

Global configuration mode

Example

```
Switch_config#logging history notifications
```

Related Command

logging

1.6.17 logging history warnings

To set the level of the historical log table to warnings, run the following command:

Parameters

None

Default Value

logging history warnings

Command Mode

Global configuration mode

Example

```
Switch_config#logging history warnings
```

Related Command

logging

1.6.18 logging history rate-limit

To set the log output rate, run the following command.

Parameters

Parameters	Description
<1-512>	Stands for the number of logs which are exported each second.

Default Value

logging history rate-limit 0

Command Mode

Global configuration mode

Example

```
Switch_config#logging history rate-limit 256
```

Related Command

logging

1.6.19 logging history size

To set the number of entries in the historical log table, run the following command.
logging history size

Parameters

Parameters	Description
<0-500>	Stands for the number of historical log entries.

Default Value

logging history size 0

Command Mode

Global configuration mode

Example

```
Switch_config#logging history size 256
```

Related Command

logging

1.6.20 service timestamps

To set configure the time stamp that is added when the system is debugged or records the log information, run the following command.

To cancel the time stamp that is added when the system is debugged or records the log information, use the no form of this command.

service timestamps [log|debug] [uptime| datetime]

no service timestamps [log|debug]

Parameters

Parameters	Description
log	Adds the time stamp before the log information.
debug	Adds the time stamp before the debug information.
uptime	Duration between the startup of the switch and the current time
datetime	Real-time clock time

Default Value

service timestamps log date

service timestamps debug date

Command Mode

Global configuration mode

Usage Guidelines

The time stamp in the uptime form is displayed like HHHH:MM:SS, meaning the duration from the start-up of the switch to the current time.

The time stamp in the date form is displayed like YEAR-MON-DAY HH:MM:SS, meaning the real-time clock time.

Example

service timestamps debug uptime

1.6.21 clear logging

To clear the log information recorded in the memory cache, run the following command.

clear logging

Parameters

None

Command Mode

EXEC

Related Command

logging buffered

show logging

1.6.22 show break

To display the information about abnormal breakdown of the switch, run the following command.

show break

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

The command can be used to display the information about abnormal breakdown of the switch, helping to find the cause of the abnormality.

Example

```
switch#show break
Exception Type:1400-Data TLB error
BreakNum: 1 s date: 2000-1-1    time: 0:34:6
r0          r1          r2          r3          r4          r5          r6
00008538-01dbc970-0054ca18-00000003-80808080-fefefeff-01dbcca1-
r7          r8          r9          r10         r11         r12         r13
```

```
00000000-00009032-00000000-7ffffff0-00008588-44444444-0054c190-
r14         r15         r16         r17         r18         r19         r20
000083f4-000083f4-00000000-00000000-00000000-00000000-00000000-
r21         r22         r23         r24         r25         r26         r27
00000000-0000000a-00000001-00000000-00000000-004d6ce8-01dbd15c-
r28         r29         r30         r31         spr8        spr9        ip
00000002-00467078-00010300-00000300-00000310-00008588-00000370-
Variables :
00008538-44444444-01dbd15c-01dbcaac-00000002-00000000-004d6ce8-
01dbca18-
 00008538 ---   do_chram_mem_sys_addr---bspcfg.o
 0001060c ---   subcmd---cmdparse.o---libcmd.a
 000083e4 ---   do_chram_mem_sys---bspcfg.o
 0000fb24 ---   lookupcmd---cmdparse.o---libcmd.a
 0000f05c ---   cmdparse---cmdparse.o---libcmd.a
 003e220c ---   vty---vty.o---libvty.a
 00499820 ---   pSOS_qcv_broadcast---ksppc.o---os\libsys.a
```

The whole displayed content can be divided into six parts:

1. RROR:file function. map not found

The prompt information means that the system has not been installed the software function.map, which does not affect the system running.

If the version of the software function.map is not consistent with that of the switch, the system prompts that the version is not consistent.

2. Exception Type—Abnormal hex code plus abnormal name

3. BreakNum

It is the current abnormal number. It means the number of abnormalities that the system has since it is powered on in the latest time. It is followed by the time when the abnormality occurs.

4. Content of the register

The common content of the register is listed out.

5. Variable area

The content in the stack is listed out.

6. Calling relationship of the number

If the map file is not installed on the system, only the function's address is displayed. If the map file is installed on the system, the corresponding function name, .o file name and .a file name are displayed.

The calling relationship is from bottom to top.

1.6.23 show debug

To display all the enabled debugging options of the switch, run the following command.

show debug

Parameters

None

Command Mode

EXEC

Example

```
switch# show debug

Crypto Subsystem:
  Crypto Ipsec debugging is on
  Crypto Isakmp debugging is on
  Crypto Packet debugging is on
```

Related Command

debug

1.6.24 show logging

To display the state of logging (syslog), run the following command.

show logging

Parameters

None

Command Mode

EXEC

Usage Guidelines

The command can be used to display the state of logging (syslog), including the login information about the console, monitor and syslog.

Example

```
switch# show logging

Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
      Console logging: level debugging, 12 messages logged
      Monitor logging: level debugging, 0 messages logged
      Buffer logging: level debugging, 4 messages logged
      Trap logging: level informations, 0 message lines logged

Log Buffer (4096 bytes):
2000-1-4 00:30:11 Configured from console 0 by DEFAULT
2000-1-4 00:30:28 User DEFAULT enter privilege mode from console 0, level = 15
```

Related Command

clear logging

1.7 SSH Configuration Commands

1.7.1 ip sshd enable

Syntax

ip sshd enable

no ip sshd enable

Parameters

None

Default Value

Disabled

Usage Guidelines

The command can be used to generate the rsa encryption key and then monitor the connection to the ssh server. The process of generating encryption key is a process of consuming the calculation time. It takes one or two minutes.

Command Mode

Global configuration mode

Example

In the following example, the SSH service is generated.

```
switch_config#ip sshd enable
```

1.7.2 ip sshd timeout

Syntax

ip sshd timeout time-length

no ip sshd timeout

Parameters

Parameters	Description
time-length	Maximum time from the establishment of connection to the authentication approval; Value range: 60-65535

Default Value

180 seconds

Usage Guidelines

To prevent the illegal user from occupying the connection resources, the connections that are not approved will be shut down after the set duration is exceeded.

Command Mode

Global configuration mode

Example

In the following example, the timeout time is set to 360 seconds

```
switch_config#ip sshd timeout 360
```

1.7.3 ip sshd auth-method

Syntax

ip sshd auth-method method

no ip sshd auth-method

Parameters

Parameters	Description
method	Sets authentication method list. The length of the authentication method's name is no more than 20 characters.

Default Value

The default authentication method list is used.

Usage Guidelines

The ssh server uses the authentication method list of the login type.

Command Mode

Global configuration mode

Example

In the following example, an auth-ssh authentication method list is configured and it is applied to the ssh server:

```
switch_config#aaa authentication login auth-ssh local
switch_config#ip sshd auth-method auth-ssh
```

1.7.4 ip sshd access-class

Syntax

ip sshd access-class access-list

no ip sshd access-class

Parameters

Parameters	Description
access-list	Standard IP access list. The length of the access list's name is no more than 20 characters.

Default Value

No access control list

Usage Guidelines

The command can be used to configure the access control list for the ssh server. Only the connections complying with the regulations in the access control list can be approved.

Command Mode

Global configuration mode

Example

In the following example, an ssh-accesslist access control list is configured and applied in the ssh server:

```
switch_config# ip access-list standard ssh-accesslist
switch_config_std#deny 192.168.20.40
switch_config#ip sshd access-class ssh-accesslist
```

1.7.5 ip sshd auth-retries

Syntax

ip sshd auth-retries times

no ip sshd auth-retries

Parameters

Parameters	Description
times	Maximum re-authentication times; Value range: 0-65535

Default Value

6 times

Usage Guidelines

The connection will be shut down when the re-authentication times exceeds the set times.

Command Mode

Global configuration mode

Example

In the following example, the maximum re-authentication times is set to five times:

```
switch_config#ip sshd auth-retries 5
```

1.7.6 ip sshd clear

Syntax

ip sshd clear ID

Parameters

Parameters	Description
ID	Number of the SSH connection to the local device; Value range: 0-15

Default Value

None

Usage Guidelines

The command can be used to disable the incoming ssh connection with the specified number compulsorily. You can run the command show ssh to check the current incoming connection's number.

Command Mode

Global configuration mode

Example

In the following example, the No.0 incoming connection is mandatorily closed:

```
switch_config#ip sshd clear 0
```

1.7.7 ip sshd silence-period

Syntax

ip sshd silence-period time-length

no ip sshd silence-period

Parameters

Parameters	Description
time-length	Means the time of the silence, which ranges from 0 to 3600.

Default Value

60s

Usage Guidelines

The command can be used to set the login silence period. After the accumulated login failures exceed a certain threshold, the system regards that there exist attacks and disables the SSH service in a period of time, that is, the system enters the login silence period.

The silence period is set by the ip sshd silence-period command. The default silence period is 60 seconds. The allowable login failures are set by the ip sshd auth-retries command, whose default value is 6.

Command Mode

Global configuration mode

Example

The following example shows how to set the silence period to 200 seconds.

```
switch_config#ip sshd silence-period 200
```

1.7.8 ip sshd sftp

Syntax

ip sshd sftp

no ip sshd sftp

Parameters

None

Default Value

None

Usage Guidelines

The command can be used to enable the SFTP function. The SFTP function refers to the secure file transmission system based on SSH, of which the authentication procedure and data transmission are encrypted. Though it has low transmission efficiency, network security is highly improved.

Command Mode

Global configuration mode

Example

The following example shows how to enable the SFTP function.

```
switch_config#ip sshd sftp
```

1.7.9 ip sshd save

Syntax

ip sshd save

no ip sshd save

Parameters

None

Default Value

None

Usage Guidelines

The command can be used to save the initial key. When the SSH server is restarted, the key will be first read from the flash; if the key reading is successful, the recalculation of key will be avoided and the startup time will be shortened.

Command Mode

Global configuration mode

Example

The following example shows how to enable the key protection function.

```
switch_config#ip sshd save
```

1.7.10 ip sshd disable-aes

Syntax

ip sshd disable-aes

no ip sshd disable-aes

Parameters

None

Default Value

The AES encryption algorithm is forbidden.

Usage Guidelines

The command can be used to decide whether to use the AES algorithm during the encryption algorithm negotiation. The AES algorithms such as aes128-cbc and aes256-cbc are not used by default.

Command Mode

Global configuration mode

Example

The following example shows how to disable the AES encryption algorithm.

```
switch_config#ip sshd disable-aes
```

1.7.11 ssh

Syntax

ssh –l *userid* **–d** *destIP* **[-c {des|3des|blowfish }] [-o** *numberofpasswdprompts***] [-p** *port***] [-v** {1|2}**]**

Parameters

Parameters	Description
–l userid	User account on the server
–d destIP	Destination IP address in the dotted decimal system
-o numberofpasswdprompts	Re-authentication times after the first authentication fails; Actual re-authentication times is the set value plus the smallest value set on the server. Its default value is three times. Value range: 0-65535
-p port	Port number that the server monitorsIts default value is 22. Value range: 0-65535
-c {des|3des|blowfish}	Encryption algorithm used during communicationThe encryption algorithm is 3des by default.
-v version	Specified version number

Default Value

None

Usage Guidelines

The command can be used to create a connection with the remote ssh server.

Command Mode

Privileged mode

Example

The following example shows how a connection with the ssh server whose IP address is 192.168.20.41 is created. The account is zmz and the encryption algorithm is blowfish:

```
switch#ip ssh –l zmz –d 192.168.20.41 –c blowfish
```

1.7.12 show ssh

Syntax

show ssh

Parameters

None

Default Value

None

Usage Guidelines

The command can be used to display the sessions on the ssh server.

Command Mode

Privileged mode

Example

The following example shows the sessions on the ssh server:

```
switch#show ssh
```

1.7.13 show ip sshd

Syntax

show ip sshd

Parameters

None

Default Value

None

Usage Guidelines

The command can be used to display the current state of the ssh server.

Command Mode

Privileged mode

Example

In the following example, the current state of the ssh server is displayed:

```
switch#show ip sshd
```

Chapter 2 Network Management Configuration

2.1 SNMP Commands

SNMP commands are listed below:

- snmp-server community
- snmp-server contact
- snmp-server engine ID local
- snmp-server group
- snmp-server host/hostv6
- snmp-server location
- snmp-server packet size
- snmp-server queue-length
- snmp-server trap-source
- snmp-server trap-timeout
- snmp-server user
- snmp-server view
- snmp-server source-addr
- snmp-sever udp-port
- snmp-server encryption
- Snmp-server trap-add-hostname
- snmp-server trap-logs
- snmp-server set-snmp-dos-max
- snmp-server keep-alive
- snmp-server necode
- snmp-server event-id
- snmp-server getbulk-timeout
- snmp-server getbulk-delay
- show snmp
- debug snmp

2.1.1 smp-server community

Syntax

To set the community access string of the accessible SNMP protocol, run **snmp-server community** in global configuration mode. To delete the specified community character string, run the no form of this command.

snmp-server community [0|7] *string* [**view** *view-name*] [**ro | rw**] [*word*]

no snmp-server community *string*

no snmp-server community

Parameters

Parameters	Description
0	Sets the community string of the text.
7	Sets the encrypted public string of the text.
string	Means the community string of the accessible SNMP protocol, which is similar to the password.
view view-name	(optional) stands for the previously defined view's name. In this view, the MIB objects, which are effective to the community, are defined.
ro	(Optional) Designates the read-only permission. Those authorized workstations can only read the MIB objects.
rw	(Optional) Designates the read-write permission. Those authorized workstations can read and modify the MIB objects.
word	(optional) Specifies the name of IP ACL of the SNMP proxy, which can be accessed by the community string.

Default Value

By default, the SNMP community string allows the read-only permission to all objects.

Command Mode

Global configuration mode

Usage Guidelines

The following command shows how to delete a designated community.

no snmp-server community *string*

The following command shows how to delete all communities.

no snmp-server community

Example

The following example shows how to distribute the "comaccess" string to SNMP, allow the read-only access and designate IP ACL to use the community string.

```
snmp-server community comaccess ro allowed
```

The following example shows how to distribute the "mgr" string to SNMP, allow to read and write the objects in the Restricted view

```
snmp-server community mgr view restricted rw
```

The following example shows how to delete the "comaccess" community.

```
no snmp-server community comaccess
```

Related Command

access-list

snmp-server view

2.1.2 snmp-server contact

Syntax

To set the information about the contact person in a management node, run snmp-server contact text. To delete the contact information, use the no form of this command.

snmp-server contact *text*

no snmp-server contact

Parameters

Parameters	Description
text	Means the string of the information about the contact person.

Default Value

The information about contact person is not set.

Command Mode

Global configuration mode

Usage Guidelines

It corresponds to the sysContact of the MIB variable in the System group.

Example

The following example shows the information about the contact person in a node.

```
snmp-server contact Dial_System_Operator_at_beeper_#_27345
```

2.1.3 snmp-server engineID local

Syntax

To configure the local agent SNMP engine ID, run the following command in the global configuration mode. To return to the default setting, use the no form of this command.

snmp-server engineID local *engineID*

no snmp-server engineID local *engineID*

Parameters

Parameters	Description
engineID	SNMP engine ID.

Default Value

SNMP engine ID is not set.

Command Mode

Global configuration mode

Usage Guidelines

The command is used to configure the SNMP engine ID of the local agent.

Example

```
snmp-server engineID local 80000cf80300e00f3f56e3
```

2.1.4 snmp-server group

Syntax

To create or update a snmp-server group in global configuration mode, run the following first command; to cancel this SNMP group, run the following second command. Format of the command is as follows:

snmp-server group [*groupname* { **v3 [auth | noauth | priv**]}][**read** readview][**write** writeview] [**notify** notifyview] [**access** access-list]

Parameters

Parameters	Description
groupname	Stands for the name of the created or modified SNMP group.
v3	Means the version ID of the SNMP protocol.
auth|noauth|priv	Stands for the lowest security level of users in the SNMPv3 group.
readview	Means the access permission of GET operations, which is defined by the view.
writeview	Means the access permission of SET operations, which is defined by the view.
notifyview	Stands for the access permission during the transmission of Trap packets, which is defined by the view.
access-list	Allows users in the SNMP group to get through the IP access control list.

Default value

The readview allows all leaves of the Internet sub-tree to be accessed.

Command mode:

Global configuration mode

Usage Guidelines

The SNMP group is used to designate the access permission of the users in this group.

Example

In the following example, an SNMP group is set and named as setter, the version ID of the SNMP protocol is 3, the security level is authentication and encryption, and the view that is accessed by the set operation is v-write.

```
snmp-server group setter v3 priv write v-write
```

Related Command

snmp-server view

snmp-server user

2.1.5 snmp-server [host|hostv6]

Syntax

To specify the receiver of SNMP trap operation, run the first of the following commands in global configuration mode. To cancel this designated host, run the following second command.

snmp-server host|hostv6 *host* **[vrf** *word***] [udp-port** *port-num***] [permit|deny** *event-id***] {{version [v1 | v2c | v3]} | {[informs | traps] | [auth |noauth]}}** *community-string/user* **[authentication | configure| snmp]**

no snmp-server host *host community-string*

Parameters

Parameters	Description
host|hostv6	Sets the IPv4 or IPv6 trap host.
host	Means the host's name or the address of the Internet. uses ipv4 address in host uses ipv6 address in hostv6
[vrf *word***]**	(Optional) binds VRF.
[udp-port *port-num***]**	(Optional) Specifies the ID of the UDP port, which transmits the traps.
[permit|deny *event-id***]**	(Optional) Allows or blocks to transmit a designated event.
{version [v1|v2c|v3]}	(Optional) Means the version ID of the SNMP protocol, which is used to transmit traps.
[informs | traps]	(Optional) Specifies the type of trap for version V2C. Informs: means the type of trap is "informs". Traps: means the type of trap is "traps".
[auth |noauth]	Specifies the trap authentication mode for version V3. auth: authentication noauth: non-authentication
community-string/user	Means a community string in version 1 and version 2c which is similar to the password and sent with the trap operations or means the username in version 3.
[authentication | configure| snmp]	(optional) if no trap is designated, all generated traps will be sent to the host. authentication: allows to transmit those authentication-error traps. configure: allows to transmit the SNMP-configure traps. snmp: allows to transmit the SNMP traps.

Default Value

This command is invalid in default settings. That is to say, no trap will be sent by default. If no command with any key word is entered, all traps with v1 standard are not sent by default.

Command Mode

Global configuration mode

Usage Guidelines

If this command is not entered, the traps will not be sent. In order to enable a switch to send the SNMP traps, you must run snmp-server host. If the keyword "trap-type" is not contained in this command, all kinds of traps of this host will be activated. If the keyword "trap-type" is contained in this command, all trap types related with this keyword are activated. You can specify multiple trap types in this command for each host.

If you designate multiple snmp-server host commands on the same host, the SNMP trap messages that are sent to the host will be decided by the community string and the trap type filtration in this command. (Only one trap type can be configured for a same host and a same community string).

The availability of the trap-type option depends on the switch type and the attributes of routing software, which is supported by this switch.

Example

The following example shows how to transmit the RFC1157-defined SNMP traps to host 10.20.30.40. The community string is defined as comaccess.

```
snmp-server host 10.20.30.40 comaccess snmp
```

The following example shows that the switch uses the public community string to send all types of traps to host 10.20.30.40.

```
snmp-server host 10.20.30.40 public
```

The following example shows that only the authentication traps are effective and can be sent to host bob.

```
snmp-server host bob public authentication
```

Related Command

snmp-server queue-length

snmp-server trap-source

snmp-server trap-timeout

snmp-server event-id

snmp-server user

2.1.6 snmp-server location

Syntax

To set the location string of a node, run the first one of the following two commands in global configuration mode. To cancel this designated host, run the following second command.

snmp-server location *text*

no snmp-server location

Parameters

Parameters	Description
text	The location string of a node is not set by default.

Default Value

The location string of a node is not set by default.

Command Mode

Global configuration mode

Usage Guidelines

It corresponds to the sysLocation of the MIB variable in the System group.

Example

The following example shows how to define the actual location of a switch.

snmp-server location Building_3/Room_214

Related Command

snmp-server contact

2.1.7 snmp-server packet size

Syntax

To define the maximum size of the SNMP packet when the SNMP server receives requests or responds, run the following first command in global configuration mode.

snmp-server packetsize *byte-count*

no snmp-server packetsize

Parameters

Parameters	Description
byte-count	Stands for the integer bytes between 484 and 17940. The default value is 3000 bytes.

Default Value

3000 bytes

Command Mode

Global configuration mode

Usage Guidelines

It corresponds to the sysLocation of the MIB variable in the System group.

Example

The following example shows how to set up a filter to filter those packets whose maximum length is 1024 bytes.

```
snmp-server packet size 1024
```

Related Command

snmp-server queue-length

2.1.8 snmp-server queue-length

Syntax

To set the queue length for each trap host, run the following first command in global configuration mode.

snmp-server queue-length *length*

no snmp-server queue-length

Parameters

Parameters	Description
length	Stands for the number of trap events which can be saved in the queue (1-1000).

Default Value

10 trap events.

Command Mode

Global configuration mode

Usage Guidelines

This command is used to set the queue length for each trap host. Once the trap messages are successfully transmitted, the switch will empty the queue.

Example

The following example shows how to set up a message queue which can capture four events.

```
snmp-server queue-length 4
```

Related Command

snmp-server packet size

2.1.9 snmp-server trap-source

Syntax

To designate an interface to be the source address of all traps, run the following first command in global configuration mode. To cancel this interface, run the following second command.

snmp-server trap-source *interface*

no snmp-server trap-source

Parameters

Parameters	Description
interface	Stands for the interface where SNMP traps generate. The parameters include the interface type and interface ID of the syntax mode of specific platform.

Default Value

The interface is not designated.

Command Mode

Global configuration mode

Usage Guidelines

When the SNMP server sends out a SNMP trap on whichever interface, the SNMP trap shall carry a trap address. If you want to use the trap address for tracking, you can use this command.

Example

The following example shows how to designate interface vlan1 as the source address of all traps.

```
snmp-server trap-source vlan1
```

Related Command

snmp-server queue-length

snmp-server host

2.1.10 snmp-server trap-timeout

Syntax

To set the timeout value of retransmitting traps, run the following first command in global configuration mode. To return to the default setting, use the no form of this command.

snmp-server trap-timeout *seconds*

no snmp-server trap-timeout

Parameters

Parameters	Description
seconds	Means an interval for retransmitting traps, whose unit is second (1-1000).

Default Value

30 seconds

Command Mode

Global configuration mode

Usage Guidelines

Before switch software tries to send traps, it is used to look for the route of destination address. If no routes exists, traps will be saved in the retransmission queue. The server trap-timeout command decides the retransmission interval.

Example

The following example shows how to set the retransmission interval to 20 seconds:

```
snmp-server trap-timeout 20
```

Related Command

snmp-server host

snmp-server queue-length

2.1.11 snmp-server user

Syntax

To create or update an**snmp-server user** in global configuration mode, run the following first command; to cancel this SNMP user, run the following second command. If the remote parameter is designated, a remote user will be configured; when a remote user is configured, the SNMP engine ID that corresponds to the IP address of this management station must exist. Format of the command is as follows:

snmp-server user *username groupname* **{ v3 [encrypted | auth] [md5 | sha]** *auth-password* **}**

Parameters

Parameters	Description
username	Stands for the name of the created or modified SNMP user.
groupname	Stands for the group where the user is.
v3	Stands for the SNMP version.
[encrypted | auth]	Encryption type: **encrypted**: Encrypted: packet encryption **auth**: packet authentication
[md5 | sha]	Means the method of encryption authentication.
auth-password	Stands for the authentication password of the user. If this password is localized, it will be used as the authentication key and the encryption key of SNMPv3.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

This command is used to set the username and the password.

Example

In the following example, an SNMP user is created, whose name is set-user and which belongs to setter, the version of the SNMP protocol is version 3, the security level is authentication and encryption, the password is 12345678, and MD5 is used as the harsh algorithm.

```
snmp-server user set-user setter v3 encrypted auth md5 12345678
```

Related Command

snmp-server view

snmp-server group

2.1.12 snmp-server view

Syntax

To create or update a MIB view, run the first one of the following two commands in global configuration mode. To cancel a view in the SNMP server, run the second one of the following two commands.

snmp-server view *view-name oid-tree* {**included | excluded**}

no snmp-server view *view-name*

Parameters

Parameters	Description
view-name	Updates or creates the label of a view.
oid-tree	Means the object IDs of the ASN.1 sub-tree that must be contained or excepted from a view. The identifier sub-tree is used to designate a numeral-contained string, e.g., 1.3.6.2.4 or a system sub-tree. The sub-tree name can be found in all MIB trees. Means the view type. The parameter "included" or "excluded" must be specified.
included | excluded	Means the view type. The parameter "included" or "excluded" must be specified.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

If other SNMP commands need a view as a parameter, you can use this command to create a view. By default, you need not define the view and you can see all the views, equivalent to Cisco-predefined everything views. The command is used to define the object the view sees.

Example

The following example shows how to create the views of all objects in the MIB-II sub-tree.

```
snmp-server view mib2 mib-2 included
```

The following example shows how to create the views of all objects, including those objects in the system group.

```
snmp-server view phred system included
```

The following example shows how to create the views of all objects that includes the objects in the system groups but excludes the objects in system7(sysServices.7) and interface 1.

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
```

Related Command

snmp-server community

2.1.13 snmp-server source-addr

Syntax

To specify a source address for answering all SNMP requests, run the second one of the following two commands in global configuration mode. To cancel this interface, run the following second command.

snmp-server source-addr *a.b.c.d*

no snmp-server source-addr

Parameters

Parameters	Description
a.b.c.d	Means the source address for all SNMP requests to be answered. Designate the source address of SNMP generating packets. The parameter is the IP address the device has set.

Default Value

The default source address is the nearest routing address.

Command Mode

Global configuration mode

Usage Guidelines

When the SNMP server transmits an SNMP request, you can run this command to designate a special source address.

Example

The following example shows how to designate the IP address "1.2.3.4" of the designated interface as the source address of all SNMP packets.

```
snmp-server source-addr 1.2.3.4
```

Related Command

None

2.1.14 snmp-server udp-port

Syntax

To specify the port number for the SNMP agent to receive packets, run the following first command in global configuration mode.

snmp-server udp-port *portnum*

no snmp-server udp-port

Parameters

Parameters	Description
udp-port	Stands for the ID of the destination port to which SNMP traps are sent, which cannot be a command port ID.

Default Value

It is the listening port of SNMP agent by default, that is, port 162.

Command Mode

Global configuration mode

Usage Guidelines

The SNMP agent will listen to this port when SNMP server transmits SNMP packets.

Example

The following example shows how to specify the listening port of SNMP agent to port 1234.

```
snmp-server udp-port 1234
```

Related Command

None

2.1.15 snmp-server encryption

Syntax

To display the configured SNMP community, the SHA encryption password and the MD5 encryption password, run snmp-server encryption in global mode. This command is a once-for-all command, which cannot be saved or canceled by its negative form. Format of the command is as follows:

snmp-server encryption

Parameters

None

Default Value

The default settings is to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text.

Command Mode

Global configuration mode

Usage Guidelines

This command is used to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text. In this way, the security of the password is guaranteed.

Example

The following example shows how to show in the plain text the SNMP community, the SHA encryption password and the MD5 encryption password, which are set for host 90.0.0.3.

```
snmp-server encryption
```

Related Command

snmp-server community

snmp-server user

2.1.16 snmp-server trap-add-hostname

Syntax

To add the host name to the binding variable when SNMP sends traps, run the first one of the following two commands.

snmp-server trap-add-hostname

no snmp-server trap-add-hostname

Parameters

None

Default Value

The hostname is not added to the binding variable list when traps are being transmitted.

Command Mode

Global configuration mode

Usage Guidelines

This command is a great help in some cases when the NMS needs to locate which host sends these traps.

Example

The following example shows how to enable the trap-to-hostname binding function.

```
Router_config# snmp-server trap-add-hostname
```

2.1.17 snmp-server trap-logs

Syntax

To write the trap transmission records into logs, run the first one of the following two commands.

snmp-server trap-logs

no snmp-server trap-logs

Parameters

The command has no parameters or keywords.

Default Value

The transmitted traps are not recorded by default.

Command Mode

Global configuration mode

Usage Guidelines

After this function is enabled, the trap transmission records of a device can be sent to the log server and then you can know more about the running state of the device.

Example

The following example shows how to the trap logs function.

```
Router_config# snmp-server trap-logs
```

2.1.18 snmp-server set-snmp-dos-max

Syntax

To set the incorrect community login retry times in five minutes on the SNMP server, run the first one of the following two commands.

snmp-server set-snmp-dos-max *retry times*

no snmp-server set-snmp-dos-max

Parameters

The retry times parameter stands for the login times for a user to conduct the incorrect community login in five minutes.

Default Value

The incorrect community login times is not limited.

Command Mode

Global configuration mode

Usage Guidelines

This command can be used to prevent those SNMP host from guessing the device's community viciously, which lessening unnecessary CPU consumption of the device.

Example

The following example shows how to enable the refuse service function and set the max trying times to 10 in five minutes.

```
Router_config# snmp-server set-snmp-dos-max 10
```

2.1.19 snmp-server keep-alive

Syntax

To set the timely sending heartbeat trap, run **snmp-server keep-alive** in global configuration mode. The time interval is times.

snmp-server keep-alive *times*

no snmp-server keep-alive

Parameters

Parameters	Description
times	The time interval of heartbeat trap.

Default Value

The command is not configured by default.

Command Mode

Global configuration mode

Usage Guidelines

The command must be used with snmp-server host.

Example

The following example shows how to set the device sending heartbeat trap every 3 seconds.

```
snmp-server keep-alive 3
```

Related Command

snmp-server host

snmp-server hostv6

2.1.20 snmp-server necode

Syntax

To set the information about the management node (the unique identifier of the device), run snmp-server necode text. To delete the identifier information, use the no form of this command.

snmp-server necode *text*

no snmp-server necode

Parameters

Parameters	Description
text	Sets the information about the management node (the unique identifier of the device).

Default Value

The node identifier is not set.

Command Mode

Global configuration mode

Usage Guidelines

The command is corresponding to the snmp private MIB variable.

Example

The following example shows the information about the node.

```
snmp-server necode Dial_System_Operator_at_beeper_#_27345
```

2.1.21 snmp-server event-id

Syntax

To create and set event list, run command snmp-server event-id in the global configuration mode. To delete the event list, use the no form of this command.

snmp-server event-id *number* **trap-oid** *oid*

no snmp-server event-id *number* [**trap-oid** *oid*]

Parameters

Parameters	Description
number	The only identifier of event-id.
oid	trap OID included in event-id.

Default Value

The event list information is not set by default.

Command Mode

Global configuration mode

Usage Guidelines

The command is used in host configuration.

Example

The following example shows how to set trap whose trap OID is 1.2.3.4.5 to event ID 1.

```
snmp-server event-id 1 trap-oid 1.2.3.4.5
```

2.1.22 snmp-server getbulk-timeout

Syntax

To set the timeout of processing getbulk request, run command snmp-server getbulk-timeout in the global configuration mode. If all getbulk requests cannot be processed in timeout, the system will return to the current result directly. To delete the configuration, use the no form of this command.

snmp-server getbulk-timeout *seconds*

no snmp-server getbulk-timeout

Parameters

Parameters	Description
seconds	The timeout of processing getbulk request.

Default Value

The timeout of processing getbulk request is not set by default.

Command Mode

Global configuration mode

Usage Guidelines

The command is used to set the timeout of processing getbulk request. If all getbulk requests cannot be processed in timeout, the system will return to the current result directly.

Example

The following example shows how to set getbulk-timeout and set the timeout to 5 seconds.

```
snmp-server getbulk-timeout 5
```

2.1.23 snmp-server getbulk-delay

Syntax

To set getbulk-delay time to prevent snmp occupying excessive cpu when snmp agent processing getbulk request, run command snmp-server getbulk-delay in the global configuration mode. The unit is 0.01 seconds. To delete the configuration, use the no form of this command.

snmp-server getbulk-delay *ticks*

no snmp-server getbulk-delay

Parameters

Parameters	Description
ticks	Sets CPU interval time in processing getbulk request. The unit is 0.01s.

Default Value

The command is not configured when CPU is processing getbulk request in full load.

Command Mode

Global configuration mode

Usage Guidelines

The command is used to set getbulk-delay time to prevent snmp from occupying excessive CPU when snmp agent processing getbulk request. The unit is 0.01s.

Example

The following example shows how snmp agent pauses one ticks when getting one result in configuring getbulk.

```
snmp-server getbulk-delay 1
```

2.1.24 show snmp

Syntax

To monitor SNMP input and output statistics, including illegal community character strings, the number of errors and request variables, run command show snmp. To show SNMP engine information, run command show snmp engineID. To show SNMP trap host information, run command show snmp host. To show SNMP view information, run command **show snmp view**. To show snmp mibs registration information, run command **show snmp mibs**. To show snmp group information, run command show snmp group. To show SNMP user information, run command show snmp user.

show snmp [engineID |host | view | mibs |group|user]

Parameters

Parameters	Description
engineID	Shows SNMP engine information.
host	Shows SNMP trap host information.
View	Shows SNMP view information.
mibs	Shows SNMP MIB registration information.
group	Shows SNMP group information.
user	Shows SNMP user information.

Default Value

None

Command Mode

EXEC and global configuration mode

Usage Guidelines

The command **show snmp** is used to show SNMP input and output statistics.

To show SNMP engine information, run command show snmp engine ID.

The command **show snmp host** is used to show SNMP trap host information.

The command **show snmp view** is used to show SNMP view information.

The command **show snmp mibs** is used to show mib registration information.

The command **show snmp group** is used to show SNMP group information.

The command **show snmp user** is used to show SNMP user information.

Example

The following example shows how to list SNMP input and output statistics.

```
#show snmp
37 SNMP packets input
0 Bad SNMP version errors
4 Unknown community name
0 Illegal operation for community name supplied
0 Snmp encoding errors
24 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
28 Get-next PDUs
0 Set-request PDUs
78 SNMP packets output
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
24 Get-response PDUs PDUs
13 SNMP trap PDUs
```

Meaning of statistics information of SNMP Agent receiving and sending packets:

Displayed Information	Meaning
Unknown community name	Unknown community name
Illegal operation for community name supplied	Illegal operation
Encoding errors	Encoding errors
Get-request PDUs	Get-request PDUs
Get-next PDUs	Get-next PDUs
Set-request PDUs	Set-request PDUs
Too big errors	The packets are too big to generate response packets.
No such name errors	No such name errors

Displayed Information	Meaning
Bad values errors	Bad values errors
General errors	General errors
Get-response PDUs	Get-response PDUs
Trap PDUs	SNMP trap packets

The following example shows how to show SNMP trap host information.

```
#show snmp host
Notification host: 192.2.2.1        udp-port: 162      type: trap
user: public          security model: v1
```

The following example shows how to show SNMP view information.

```
#show snmp view
mib2        mib-2     -          included          permanent          active
```

Related Command

snmp-server host

snmp-server view

2.1.25 debug snmp

Syntax
To show SNMP event, packet sending and receiving process and error information, run command **debug snmp**.

debug snmp [*error* | *event* | *packet*]

To stop showing the information, run command **no debug snmp**.

no debug snmp

Parameters

Parameters	Description
error	Enable the debug OLT of SNMP error information.
event	Enable the debug OLT of SNMP event information.
packet	Enable the debug OLT of SNMP input/output packets.

Command Mode

EXEC

Usage Guidelines

The command is used to enable SNMP debug information switch and output SNMP event, information of sending and receiving packets, which is helpful for SNMP fault diagnosis.

Example

The following example shows how to debug SNMP receiving and sending packets.

```
switch#debug snmp packet
Received 49 bytes from 192.168.0.29:1433
0000: 30 82 00 2D   02 01 00 04   06 70 75 62   6C 69 63 A0     0..-.....public.
```

```
0016: 82 00 1E 02   02 7D 01 02   01 00 02 01   00 30 82 00    .....}.......0..
0032: 10 30 82 00   0C 06 08 2B   06 01 02 01   01 03 00 05    .0.....+........
0048: 00
Sending 52 bytes to 192.168.0.29:1433
0000: 30 82 00 30   02 01 00 04   06 70 75 62   6C 69 63 A2    0..0.....public.
0016: 82 00 21 02   02 7D 01 02   01 00 02 01   00 30 82 00    ..!..}.......0..
0032: 13 30 82 00   0F 06 08 2B   06 01 02 01   01 03 00 43    .0.....+.......C
0048: 03 00 F4 36                                            ...6
Received 51 bytes from 1192.168.0.29:1434
0000: 30 82 00 2F   02 01 00 04   06 70 75 62   6C 69 63 A0    0../.....public.
0016: 82 00 20 02   02 6B 84 02   01 00 02 01   00 30 82 00    .. ..k........0..
0032: 12 30 82 00   0E 06 0A 2B   06 01 02 01   02 02 01 02    .0.....+........
0048: 01 05 00                                               ...
Sending 62 bytes to 192.168.0.29:1434
0000: 30 82 00 3A   02 01 00 04   06 70 75 62   6C 69 63 A2    0..:.....public.
0016: 82 00 2B 02   02 6B 84 02   01 00 02 01   00 30 82 00    ..+..k........0..
0032: 1D 30 82 00   19 06 0A 2B   06 01 02 01   02 02 01 02    .0.....+........
0048: 01 04 0B 45   74 68 65 72   6E 65 74 30   2F 31          ...Ethernet0/1                .
```

Domain	Description
Received	Stands for SNMP receiving packets
192.168.0.29	Stands for source IP address
1433	Stands for source address port number
51 bytes	Stands for the length of receiving packets
30 82 00 2D 02 01 00 04 06 70 75 62 6C 69 63 A0 82 00 1E 02 02 7D 01 02 01 00 02 01 00 30 82 00 10 30 82 00 0C 06 08 2B 06 01 02 01 01 03 00 05 00	Stands for packets after SNMP ASN encoding
0..-.....public. .....}.......0.. .0.....+........ .	Stands for ASCII character of receiving packets. "." means not in the range of ASCII character.
sending	SNMP sending packets
192.168.0.29	Stands for the destination IP address
1433	Stands for the source address port number
52 bytes	Stands for the length of sending and receiving packets
30 82 00 30 02 01 00 04 06 70 75 62 6C 69 63 A2 82 00 21 02 02 7D 01 02 01 00 02 01 00 30 82 00 13 30 82 00 0F 06 08 2B 06 01 02 01 01 03 00 43 03 00 F4 36	Stands for packets after SNMP ASN encoding
0..0.....public. ..!..}.......0.. .0.....+.......C ...6	Stands for ASCII character of sending and receiving packets. "." means not in the range of ASCII character.

The following example shows how to debug SNMP events.

```
switch#debug snmp event
Received SNMP packet(s) from 192.2.2.51
  SNMP: GETNEXT request
   -- ip.ipReasmFails.0
  SNMP: Response
   >> ip.ipFragOKs.0 = 1
Received SNMP packet(s) from 192.2.2.51
  SNMP: GETNEXT request
  -- ip.ipFragOKs.0
  SNMP: Response
   >> ip.ipFragFails.0 = 0
  SNMP: GETNEXT request
   -- ip.ipFragFails.0
  SNMP: Response
>> ip.ipFragCreates.0 = 2
```

Domain	Description
SNMP	Stands for the current debug SNMP protocol.
GETNEXT request	SNMP getnext request
RESPONSE	SNMP response
--	Stands for receiving packets
>>	Transmitting packets
ip.ipReasmFails.0	Stands for MIB OID of access request
ip.ipFragOKs.0 = 1	Stands for being accessed MIB OID and the return value

2.2 RMON Configuration Commmands

RMON configuration commands include:

• rmon alarm

• rmon event

• rmon collection stat

• rmon collection history

• show rmon

2.2.1 rmon alarm

Syntax

To configure a rmon alarm entry, run the following command.

rmon alarm *index variable interval* {absolute | delta} rising-threshold *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [repeat] [owner *string*]

Parameters

Parameters	Description
index	Stands for the index of the event table Value range: 1-65535
variable	Stands for the object needs to be monitored. Value range: oid of the monitored object.
interval	Stands for the sampling interval Value range: 1~ 2147483647
value	Stands for the alarm threshold Value range: -2147483648~ 2147483647.
eventnumber	Stands for the event index generated after reaching the threshold. Value range: 1~65535.
repeat	Stands for the repeat trigger event.
string	Stands for the owner description information Value range: the length of the character string is 1~31.

Default Value

eventnumber is not set by default.

repeat is not set by default.

Usage Guidelines

The command is used to monitor the value of specified object. The certain event will be triggered when the value exceeds the threshold.

Example

The following example shows how to set an alarm entry to monitor the object ifInOctets.2 and the sampling interval is 10. When the sampling interval increases more than15, the event 1 will be triggered. When the sampling interval decreases more than 25, the event 2 will be triggered.

```
rmon alarm 1 1.3.6.1.2.1.2.2.1.10.2 10 absolute rising-threshold 15 1 falling-threshold 25 2 repeat owner switch
```

2.2.2 rmon event

Syntax

To configure a rmon event entry, run the following command.

rmon event *index* [description *des-string*] [log] [owner *owner-string*] [trap *community*] [ifctrl *interface*]

Parameters

Parameters	Description
index	Stands for the index of the event table Value range: 1-65535
des-string	Stands for the event description character string. Value range: 1~127.
owner-string	Stands for the owner character string. Value range: 1~31.
community	Stands for the community name when generating trap. Value range: 1~31.
interface	Stands for the shutdown port that the event controls.

Default Value

None

Usage Guidelines

The command is used to set a rmon event entry. It is used for alarm.

Example

The following example shows to set one rmon event entry to 6 and the description character string to example; add one item in the log entry when triggering the event and generates trap with public as the community name.

```
rmon event 6 log trap public description example owner switch
```

2.2.3 rmon collection stats

Syntax

To set rmon statistics function, run the following command.

rmon collection stats *index* [*owner string*]

Parameters

Parameters	Description
index	Stands for the index of the statistics entry. Value range: 1~65535.
string	Stands for the owner character string. Value range: the length of the character string is 1~31.

Default Value

None

Usage Guidelines

The command must be configured in the interface mode.

Example

The following example shows how to enable the statistics function on gigabit Ethernet interface g0/1.

```
int g0/1
rmon collection stats 2 owner switch
```

2.2.4 rmon collection history

Syntax

To configure a history control entry, run the following command.

rmon collection history *index* [**buckets** *bucket-number*] [**interval** *second*] [**owner** *owner-name*]

Parameters

Parameters	Description
index	index Value range: 1-65535
bucket-number	The entry of all history record control entries nearest to the bucket-number need to be reserved. Value range: 1~65535.
second	Stands for the time interval. Value range: 1~3600.
owner-name	Stands for the owner character string. Value range: the length of the character string is 1~31.

Default Value

The default bucket-number is 50 and the default second is 1800.

Usage Guidelines

The command is used to configure in the interface mode. It is used for adding one entry to the history control table.

Example

The following example shows how to add the history control entry on the gigabit Ethernet interface g0/1 and save the statistics of latest 20 time intervals.(Each time interval is 10 seconds.)

```
int g0/1
rmon collection history 2 buckets 20 interval 10 owner switch
```

2.2.5 show rmon

Syntax

To show rmon configuration, run the following command.

show rmon [**alarm**] [**event**] [**statistics**] [**history**]

Parameters

None

Default Value

None

Usage Guidelines

The command is used to show rmon configuration.

Example

The following example shows how to show rmon configuration, run the following command.

```
show rmon
```

Chapter 3 AAA Configuration Commands

This Chapter describes the commands used for configuring the AAA authentication method. AAA authentication commands can be classified into authentication, authorization, accounting and local account policy configuration commands. Learn more in following sections.

3.1 Authentication Configuration Commands

This section describes the commands for configuring authentication methods. Authentication defines the access right of the users before they are allowed to access the network and network services.

Please refer to "Configuring Authentication" for information on how to use the AAA method to configure the authentication. Please refer to the last part to review the examples configured by the commands in this Chapter.

Authentication Configuration Commands include:

- aaa authentication banner
- aaa authentication fail-message
- aaa authentication username-prompt
- aaa authentication password-prompt
- aaa authentication dot1x
- aaa authentication enable default
- aaa authentication login
- aaa group server
- server
- debug aaa authentication
- enable password
- enable(enter)
- service password-encryption

3.1.1 aaa authentication banner

Syntax

To configure a personal banner, run aaa authentication banner in global mode. To delete a personal banner, run no aaa authentication banner.

aaa authentication banner *delimiter string delimiter*

no aaa authentication banner

Parameters

Parameters	Description
delimiter string delimiter	To-be-displayed text string when the user logs in; The delimiter parameter stands for the delimiter which adopts double quotation masks.

Default Value

If you do not define the login banner, the system will display the following default banner:

User Access Verification

Command Mode

Global configuration mode

Usage Guidelines

When creating a banner, you need to configure a delimiter and then to configure the text string itself. The delimiter is to notify that the following text string will be displayed as the banner. The delimiter appears repeatedly at the end of the string, meaning the banner ends.

Example

The following example shows that the banner is modified to "Welcome to AACOM system" when logging on:

```
aaa authentication banner "Welcome to system!"
```

Related Command

```
aaa authentication fail-message
```

3.1.2 aaa authentication fail-message

Syntax

To configure a personal banner when login fails, run aaa authentication fail-message in global mode. To delete a personal banner, use the no form of this command.

```
aaa authentication fail-message delimiter string delimiter
no aaa authentication fail-message
```

Parameters

Parameters	Description
delimiter string delimiter	Text string that will be displayed when user fails to log in. The delimiter adopts double quotation marks.

Default Value

If you do not define the login banner, the system will display the following default banner:

Authentication failed!

Command Mode

Global configuration mode

Usage Guidelines

When creating a banner, you need to configure a delimiter and then to configure the text string itself. The delimiter is to notify that the following text string will be displayed as the banner. The delimiter appears repeatedly at the end of the string, meaning the banner ends.

Example

The following example shows that user name prompt is changed to the following character string:

```
aaa authentication fail-message "See you later"
```

Related Command

```
aaa authentication banner
```

3.1.3 aaa authentication username-prompt

Syntax

To change the text display prompting the user name input, run command "aaa authentication username-prompt" in global mode. To return to the default setting, use the no form of this command.

```
aaa authentication username-prompt text-string
no aaa authentication username-prompt
```

Parameters

Parameters	Description
text-string	It is used to prompt the user of the text to be displayed at the time of the user name input.

Default Value

When there is no user-defined text-string, the prompting character string of the user name is "Username".

Command Mode

Global configuration mode

Usage Guidelines

The command "aaa authentication username-prompt" is used for changing the displayed character string prompting the user name input. The "no" format of the command changes the prompt of username into default value.

Username:

Some protocols (such as TACACS+) have the capability to cover the prompting information of local username. Under such circumstances, the use of the command "aaa authentication username-prompt" will not change the prompting character string of username.

NOTE:

The command "aaa authentication username-prompt" does not change any prompting information provided by remote TACACS +server.

Example

The following example shows that user name prompt is changed to the following character string:

aaa authentication username-prompt "Your Username:"

Related Command

```
aaa authentication password-prompt
```

3.1.4 aaa authentication password-prompt

Syntax

To change the text display prompting the user password input, run command "aaa authentication password-prompt" in global configuration mode. To return to the default setting, use the no form of this command.

```
aaa authentication password-prompt text-string
no aaa authentication password-prompt
```

Parameters

Parameters	Description
test-string	It is used to prompt the user of the text displayed at the time of password input.

Default Value

When the user-defined text-string is not used, the password prompt is "Password".

Command Mode

Global configuration mode

Usage Guidelines

The displayed default literal information prompting the user password input can be changed by using the command "aaa authentication password-prompt". The command not only changes the password prompt of the enable password, it also changes the password prompt of login password. The "no" format of the command restores the password prompt to default value.

Password:

The command "aaa authentication password-prompt" does not change any prompting information provided by remote TACACS+ or RADIUS server.

Example

The following Example will change the password prompt to "Your Password:"

aaa authentication password-prompt "Your Password:"

Related Command

aaa authentication username-prompt
enable password

3.1.5 aaa authentication dot1x

Syntax

To set do1x access authentication, run command aaa authentication dot1x in global configuration mode. To disable dot1x authentication, use the no form of this command.

aaa authentication dot1x {default | list-name} method1 [method2...]
no aaa authentication dot1x {default | list-name}

Parameters

Parameters	Description
Default	It uses the listed authentication method following the parameter as the default authentication method list at the time of the user's login.
list-name	It uses the listed authentication method following the parameter as the default authentication method list at the time of the user's login.
Method	It is one of the key words described in the Form 2 at the least.

Command Mode

Global configuration mode

Usage Guidelines

The default list or other naming list created by the command "aaa authentication login" will act on some specific line using the command "login authentication".

Only when the said authentication method feeds back error, other authentication methods will be used. Should the said authentication method feedback the failure, no other authentication methods will be used.

dot1x authentication method

Keyword	Description
group name	Uses the server group for authentication.
group radius	Uses RADIUS authentication.
group tacacs+	Uses group tacacs+ for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local user name authentication.
none	Uses no authentication.

Example

The following example creates an AAA authentication list called TEST. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication. (Now the authentication method either enable(line) or local can obtain a success or failure result. Therefore, the following command will not use the none method.

```
aaa authentication dot1x TEST group tacacs+ local none
```

The following example creates the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication dot1x default group tacacs+ local none
```

Related Command

None

3.1.6 aaa authentication enable default

Syntax

To enable AAA authentication to determine if a user can access the privileged command level, use the aaa authentication enable default global configuration command. To disable this authentication method, use the no form of this command.

```
aaa authentication enable default method1 [method2...]
no aaa authentication enable default
```

Parameters

Parameters	Description
method	At least one of the keywords described in Table 1.

Default Value

No authentication method is set. The authentication will succeed if it is the console port user. Otherwise, the authentication will fail.

Command Mode

Global configuration mode

Usage Guidelines

Use the aaa authentication enable default command to create a series of authentication methods that are used to determine whether a user can access the privileged command level. Method keywords are described in Table 1. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line. Only when the said authentication method feeds back error, other authentication methods will be used. Should the said authentication method feedback the failure, no other authentication methods will be used.

enable authentication method

Keyword	Description
enable	Uses the enable password for authentication.
group name	Uses the server group for authentication.
group radius	Uses RADIUS authentication.
group tacacs+	Uses tacacs+ for authentication.
line	Uses the line password for authentication.
none	Passes the authentication unconditionally.

Example

The following example creates an authentication list that first tries to contact a TACACS+ server. If no server can be found, AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication. (Now the authentication method either enable (line) or local can obtain a success or failure result. Therefore, the following command will not use the none method.

aaa authentication enable default group tacacs+ enable none

Related Command

enable password

3.1.7 aaa authentication login

Syntax

To set authentication, authorization, and accounting (AAA)authentication at login, use the aaa authentication login command in global configuration mode. To disable AAA authentication, use the no form of this command.

aaa authentication login {default | list-name} method1 [method2...]
no aaa authentication login {default | list-name}

Parameters

Parameters	Description
Default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the list of authentication methods activated when a user logs in.
method	At least one of the keywords described in Table 2.

Default Value

No authentication method is set. The authentication will succeed if it is the console port user. Otherwise, the authentication will fail.

Command Mode

Global configuration mode

Usage Guidelines

The default and optional list names that you create with the aaa authentication login command are used with the login authentication command.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line.

login authentication method

Keyword	Description
enable	Uses the enable password for authentication.
group name	Uses the server group for authentication.
group radius	Uses RADIUS authentication.
group tacacs+	Uses group tacacs+ for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
localgroup	Uses the local strategy group username database for authentication.
local-case	Uses case-sensitive local user name authentication.
none	Uses no authentication.

Example

The following example creates an AAA authentication list called TEST. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no enable password is configured on the server), the user is allowed access with no authentication.

aaa authentication login TEST group tacacs+ group radius none

The following example creates the same list, but it sets it as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication login default group tacacs+ group radius none
```

Related Command

None

3.1.8 aaa group server

Syntax

To group different RADIUS server hosts into distinct lists and distinct methods, run command aaa group server radius in global configuration mode. To remove a group server from the configuration list, use the no form of this command.

```
aaa group server {radius | tacacs+} group-name
no aaa group server {radius | tacacs+} group-name
```

Parameters

Parameters	Description
group-name	Character string used to name the group of servers.

Default Value

No default behavior or values.

Command Mode

Global configuration mode

Usage Guidelines

The command is used to enter the configuration of the server group and add the corresponding server to it. It can establish 63 server groups in maximum.

Example

```
aaa group server radius radius-group
```

The example shows how to add a radius server group named radius-group.

Related Command

server

3.1.9 server

Syntax

To add a server in an AAA server group, run the following command. To delete a server, use the no form of this command.

To add a server in a radius server group:

server {A.B.C.D | X:X:X:X::X} [**key** {*password* | {*encryption-type encrypted-password*}}] [**auth-port** *num*] [**acct-port** *num*] [**retransmit** *value*] [**timeout** *value*] [**privilege** *pri*]

To add a server to a tacacs+ server group:

server {A.B.C.D | X:X:X:X::X} [**key** {*password* | {*encryption-type encrypted-password*}}]

no server A.B.C.D

Parameters

Parameters	Description
A.B.C.D	IP address of the server
X:X:X:X::X	IPv6 address of the server
key	Key
password	key character string
encryption-type	encryption type, 0 means no encryption, and 7 means encryption.
encrypted-password	key character string corresponding to the encryption type
auth-port	authentication destination port
acct-port	accounting destination port
num	Standing for a port ID
retransmit *value*	retransmit times, the default is 2.
timeout *value*	timeout for retransmit. The default is 3 seconds.
privilege *pri*	server priority; the default is 0.

Default Value

no server

Command Mode

Server group configuration mode

Usage Guidelines

You can add 63 server groups at most,1 radius server link table and 1 tacacs+ server link table. The value of all radius server groups and servers in the server link table amounts to 64. The value of all tacacs+ server groups and servers in the server link table also amounts to 64.

Example

The following example adds a server at 12.1.1.1 to the server group:

```
server 12.1.1.1
```

Related Command

```
aaa group server
```

3.1.10 debug aaa authentication

Syntax

To track the user authentication process, run debug aaa authentication. To disable the debug information, run no debug aaa authentication.

```
debug aaa authentication
no debug aaa authentication
```

Parameters

None

Default Value

The debug information is disabled by default.

Command Mode

EXEC

Usage Guidelines

This command can be used to track the authentication process of each user to detect the cause of the authentication failure.

Example

None

Related Command

None

3.1.11 enable password

Syntax

To set a local password to control access to various privilege levels, use the enable password command. To remove the password requirement, use the no form of this command.

```
enable password { password | [encryption-type] encrypted-password } [level number]
no enable password [level number]
```

Parameters

Parameters	Description
password	Plain text of the password character string
encryption-type	Type of password encryption
encrypted-password	Encrypted password corresponding to the set encryption type
level	Privilege level parameter
number	Value of the privilege level (1-15)

Default Value

There is no password by default.

Command Mode

Global configuration mode

Usage Guidelines

The passwords configured for the device do not contain space, that is, when the enable password command is used, space cannot be entered when you enter the plain text of the password. The length of the password plain-text cannot exceed 127 characters.

When the level parameter is not entered, the default level is level 15. The higher the privilege level is, the more rights the user has. If some privilege level is not configured with password, authentication will fail when the user enters the level.

Currently, our products only support two encryption modes: 0 and 7. The number 0 means the password is not encrypted and the plaintext of password is directly entered. It is the same as the way of directly entering the password. The number 7 means the password is encrypted through an algorithm. You need to enter the encryption text for the encrypted password. The encryption text can be copied from the configuration files of other switches.

Example

The following example shows how to set the password of privilege level 10 to clever and encryption-type to 0.

```
enable password 0 clever level 10
```

The following example shows how to set the password of the default privilege level (15) to oscar and encryption-type to 7.

```
enable password 7 074A05190326
```

Suppose that the cipher text of oscar is 074A05190326, the value of the cipher text is obtained from the configuration files of other devices.

Related Command

```
aaa authentication enable default
service password-encryption
```

3.1.12 enable(enter)

Syntax

To enter the privilege mode (EXEC mode), run command enable(enter).

```
enable(enter) <1-15>
```

Parameters

Parameters	Description
<1-15>	To be obtained privilege level

Default Value

Do not enter the privileged level by default.

Command Mode

User mode

Usage Guidelines

None

Example

```
>enable(The user level is 15 by default.)
Password: (enter the password to authenticate)
#
#exi
>enable 1(To be obtained privilege level is 1)
Password: (enter the password to authenticate)
```

Related Command

```
aaa authentication enable default
enable password
```

3.1.13 service password-encryption

Syntax

To encrypt passwords, use the service password-encryption command. To return to the default setting, use the no form of this command.

```
service password-encryption
no service password-encryption
```

Parameters

None

Default Value

Related passwords in the system are not encrypted.

Command Mode

Global configuration mode

Usage Guidelines

This command is related with three commands, username password, enable password and password. If this command is not configured and the previous three commands adopt the password plain-text storage mode, the configured password's plain text can be displayed after the show running-config command is run. If this command is configured, the passwords configured for the previous three commands will be encrypted and the configured password's plain text cannot be displayed after the show running-config command is run; in this case, the password plain-text display cannot be resumed even if you run no service password-encryption. The no service password-encryption command is effective only to the password which is configured by this command, while is not effective to those passwords which are encrypted before this command is used.

Example

```
switch_config#service password-encryption
```

The example shows how to encrypt the configured plain-text password and also the plain-text password after this command is used.

Related Command

username username password
enable password

password (the configuration command under vty which can be used for line authentication)

3.2 Authorization Configuration Commands

This chapter describes the commands for authentication, authorization and accounting. AAA authorization can limit the effective service to a user. When the authorization result is effective, network access server configures the dialogue process of the user by using the authorization information fed back from authorization server. Then the user is available to services required. Only information included in the user profile provides such service.

Please refer to "Configuration Authorization" for information on how to configure authorization. Please refer to the last part to review the examples configured by the commands in this Chapter.

Authorization Configuration Commands include:

aaa authorization
debug aaa authorization

3.2.1 aaa authorization

Syntax

The global configuration command "aaa authorization" is used for setting the parameter to limit the authority of the user's access to network.
To set the parameter to limit the authority of the user's access to network, run command "aaa authorization" in global configuration mode. To return to the default setting, use the no form of this command.

aaa authorization {{commands <0-15>} | network | exec} {default | list-name} method1 [method2...]
no aaa authorization {{commands <0-15>} | network | exec} {default | list-name}

Parameters

Parameters	Description
commands	EXEC (shell) command authorization
<0-15>	To be authorized command privilege (EXEC)
network	The authorization of network type service
exec	It adapts to the attribute related to the user EXEC terminal dialogue. It determines whether XEC shell program is allowed to register or grant the privilege level of the user entering EXEC shell.
default	Default authorization methods list
list-name	Character string which is used to name the authorization method list
method	At least one of the keywords listed in the form below.

Default Value

If the user requires accounting but he does not designate the authorization method list on the corresponding path or interface, the default authorization method list will be applied. If the default method list is not defined, the authorization will not be executed.

Command Mode

Global configuration mode

Usage Guidelines

The command "aaa authorization" is used for enabling the authorization, creating authorization methods list and defining the authorization method that can be used when the user accesses to the designated functions. The authorization method list defines the authorization execution method and the order to execute these authorization methods. The method list is just a simple naming list, describing the authorization method (RADIUS or TACACS+). The method list can designate one or multiple authorization security protocols. Hence, it secures a standby method if all previous authorization methods fail. Under general condition, the listed first method is used at first in an attempt to authorize the user the authority to access to the designated network service. If the method does not work, the next method in the list shall be selected. The process shall be continued till the successful feedback of authorization results by using some authorization method or all the defined methods are used up.

Authorization method

Keyword	Description
group name	Uses the server group for authorization.
group radius	Uses RADIUS authorization.
group tacacs+	Uses tacacs+ authorization.
if-authenticated	If the user passes the authorization, the user is allowed to access the function required.
local	The local database is used for authorization.
none	No authorization

Once the authorization methods list is defined, the methods list shall be used on the designated line or interface before the defined method is executed. As a part of the authorization process, the authorization command sends a series of request packets of AV pairs to the program of RADIUS or TACACS＋server. The server is likely to execute one of the following actions:

- The request is accepted completely.
- The request is accepted and the attribute is added to limit the authority of user service.
- Request is refused and authorization fails.

Example

The following Example defines the network authorization methods list named "have a try". The methods list designates RADIUS authorization method used on the serial line employing vty. If RADIUS server makes no response, the local network authorization is executed.

aaa authorization exec have a try radius local

Related Command

aaa authentication

aaa accounting

3.2.2 debug aaa authorization

Syntax

To track the user authorization process, run debug aaa authorization command. To disable the debug information, run the no form of this command.

```
debug aaa authorization
no debug aaa authorization
```

Parameters

None

Default Value

The debug information is disabled by default.

Command Mode

EXEC

Usage Guidelines

This command can be used to track the authorization process of each user to detect the cause of the authorization failure.

Example

None

Related Command

None

3.3 Accounting Configuration Commands

This chapter describes the commands for accounting. The accounting function can track the services that user access, and at the same time track the service-consumed network resource number. When AAA accounting is activated, the system will report user's activities to the TACACS+ server or the RADIUS server in the accounting record method (It depends on the adopted security method). Each accounting record contains the attribute value peer which is stored on the access control server. The data is then applied to network management, client's accounting analysis or audit.

Authorization Configuration Commands include:

- aaa accounting
- aaa accounting update
- aaa accounting suppress null-username
- debug aaa accounting

3.3.1 aaa accounting

Syntax

To execute AAA accounting onto required services on the basis of accounting or security, run aaa accounting in global mode. You can run no aaa accounting to disable the accounting function.

aaa accounting {{**commands** *<0-15>*} **| network** | **exec** | **connection**} {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** {*groupname* | **radius | tacacs+**}} | **none** }

no aaa accounting **{** network **|** exec **|** connection**} {**default **|** ***list-name*****}**

Parameters

Parameters	Description
commands	Provide accounting for a priority level command
<0-15>	The priority level of the command
network	Provides accounting information to all PPP sessions, including packets, bytes and time numbering.
exec	Provides information about EXEC terminal session (it is not supported currently).
connection	Provides information about all egress connections from related device. Currently, only the H323 session is supported.
default	Default accounting method list
list-name	Character string which is used to name the accounting method list
start-stop	accounting in beginning and end
stop-only	accounting in the end
none	no accounting
group *groupname*	Uses the server group for accounting
group radius	Uses RADIUS for accounting
group tacacs+	Uses tacacs+ for accounting

Default Value

If the user requires accounting but he does not designate the accounting method list on the corresponding path or interface, the default accounting method list will be applied. If the default method list is not defined, the accounting will not be executed.

Command Mode

Global configuration mode

Usage Guidelines

You can use the aaa accounting command to enable the accounting function, create the accounting method list and define the applied accounting method when user sends the accounting record. The accounting method list defines the accounting execution method and the order to execute these accounting methods. The method list is just a simple naming list, describing the accounting method (RADIUS or TACACS+). The method list can designate one or multiple accounting security protocols. Hence, it secures a standby method if all previous accounting methods fail.

Related Command

```
aaa authentication
aaa accounting
```

3.3.2 aaa accounting update

Syntax

To periodically transmit temporary accounting records to the accounting server, run aaa accounting update. You can run no aaa accounting update to disable temporary accounting records.

```
aaa accounting update { newinfo | periodic number}
no aaa accounting update { newinfo | periodic}
```

Parameters

Parameters	Description
update	Activates the device to transmit temporary accounting records (It needs support from the application client. It is not supported at present.).
newinfo	Transmits temporary accounting records to the accounting server when new accounting information need be reported.
periodic	Periodically transmits temporary accounting records. The period is defined by the number parameter.
number	A parameter to define the period for temporary accounting record transmission

Default Value

Temporary accounting activity does not occur.

Command Mode

Global configuration mode

Usage Guidelines

The function runs with the support of the application client. It is not supported at present.

Related Command

aaa accounting

3.3.3 aaa accounting suppress null-username

Syntax

To stop generating accounting records for those non-user sessions, run aaa accounting suppress null-username in global mode. To return to the default setting, use the no form of this command.

aaa accounting suppress null-username
no aaa accounting suppress null-username

Parameters

None

Default Value

The accounting records will be generated for all sessions, no matter the sessions have username or not.

Command Mode

Global configuration mode

Usage Guidelines

None

Related Command

aaa accounting

3.3.4 debug aaa accounting

Syntax

To track the user process, run debug aaa accouting command. To disable the debug information, run the no form of this command.

```
debug aaa accounting
no debug aaa accounting
```

Parameters

None

Default Value

The debug information is disabled by default.

Command Mode

EXEC

Usage Guidelines

This command can be used to track the accounting process of each user to detect the cause of the accounting failure.

Example

None

Related Command

None

3.4 Local Account Policy Configuration Commands

This section introduces local account policy configuration commands. The local account policy is used for local authentication and local authorization.

Please refer to "local account policy configuration" for information on how to configure local account policy. Please refer to the last part to review the examples configured by the commands in this Chapter.

• Local Account Policy Configuration Commands include:

• local authen

• local author

• local pass

• local group

• local authen-group

• local author-group

• local pass-group

• local user

• username

• show local-users

• show aaa users

3.4.1 localauthen

Syntax

To configure local authentication policy, run the command localauthen. To return to the default setting, use the no form of this command.

localauthen WORD
no localauthen WORD

Parameters

Parameters	Description
WORD	Local authentication policy name

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

To enter local authentication configuration, run command localauthen WORD.

The max login tries within a certain time

login max-tries <1-9> try-duration 1d2h3m4s

Parameters	Description
max-tries	The max login tries
<1-9>	The max login tries ranges from 1 to 9
try-duration	Duration
1d2h3m4s	The format of day, hour, min and second.

Related Command

login max-tries
localgroup
local authen-group
username

3.4.2 localauthor

Syntax

To configure local authentication policy, run the command localauthen. To return to the default setting, use the no form of this command.

localauthor WORD
no localauthen WORD

Parameters

Parameters	Description
WORD	Local authorization policy name

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command localauthor WORD is used to enter the local authorization policy configuration. Use following command to configure local authorization policy.

To authorize priority for login users.

exec privilege {default | console | ssh | telnet} <1-15>

Parameters	Description
default	Default priority (Use the priority for authorization if there is no concrete login method.)
console	authorization priority of the login user on console port
ssh	authorization priority of the ssh login user on console port
telnet	authorization priority of the telnet login user on console port
<1-15>	Priority

Related Command

exec privilege
localgroup
local author-group
username

3.4.3 localpass

Syntax

To configure local password policy, run the command localpass in global mode. To return to the default setting, use the no form of this command.

localpass WORD
no localpass WORD

Parameters

Parameters	Description
WORD	Local password policy name

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command localpass WORD is used to enter the local password policy configuration. Use following command to configure local password policy.

The password and username is different

non-user

History password check (When the password is different from the history one or modifying the password)

non-history

Set the elements of the password

element *[number] [lower-letter] [upper-letter] [special-character]*

Parameters	Description
number	The password must include numbers.
lower-letter	The password must include lower-letters.
upper-letter	The password must include upper-letters.
special-character	The password must include special characters.

The minimum length of the password

min-length <1-127>

Parameters	Description
<1-127>	The minimum length (ranges from 1-127)

The validity of the password

validity *1d2h3m4s*

Parameters	Description
1d2h3m4s	The format of day, hour, min and second.

Related Command

non-use
non-history
element
min-length
validity
localgroup
local pass-group
username

3.4.4 localgroup

Syntax

To configure local policy group, run command localgroup in global mode. To return to the default setting, use the no form of this command.

```
localgroup WORD
no localgroup WORD
```

Parameters

Parameters	Description
WORD	Local policy group name

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command localgroup WORD is used to enter the local password policy configuration. Use following command to configure local policy group.

Stands for the local authentication configuration

```
local authen-group
```

Stands for the local authorization configuration

```
local author-group
```

Local password configuration

```
local pass-group
```

Local account configuration

```
local user
```

Configuring account

```
username
```

Related Command

```
local authen-group
local author-group
local pass-group
local user
username
localgroup
local author-group
```

3.4.5 local authen-group

Syntax

To configure local authentication policy group, run command local authen-group. It is local policy group in global mode by default. To return to the default setting, use the no form of this command.

```
local authen-group WORD
no local authen-group
```

Parameters

Parameters	Description
WORD	Local authentication policy name

Default Value

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related Command

localauthen
localgroup
local authen-group

3.4.6 local author-group

Syntax

To configure local authentication policy group, run command local author-group. It is the local policy group in global mode by default. To return to the default setting, use the no form of this command.

local author-group WORD
no local author-group

Parameters

Parameters	Description
WORD	Local authorization policy name

Default Value

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related Command

localauthor
localgroup
local author-group

3.4.7 local pass-group

Syntax

To configure local password policy group, run command local pass-group. It is the default policy group by default in global configuration mode. To return to the default setting, use the no form of this command.

local pass-group WORD
no local pass-group

Parameters

Parameters	Description
WORD	Local password policy name

Default Value

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related Command

localpass
localgroup
local pass-group

3.4.8 local user

Syntax

To configure the maximum connection numbers and freezing users, run command local user. It is the default policy group by default in global configuration mode. To return to the default setting, use the no form of this command.

local user {maxlinks <1-255>} | { freeze WORD }
no local user {maxlinks | { freeze WORD }}

Parameters

Parameters	Description
maxlinks	The maximum links to the router, the same user can create at the same time.
<1-255>	The number of links created at the same time. (value range: 1-255)
freeze	freezing user
WORD	A user name

Default Value

None

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

None

Related Command

Localgroup

3.4.9 username

Syntax

To add users in the local user database for local authentication and authorization, run this command. The command is used in local policy group configuration mode. It is the default local policy group in global configuration mode. To return to the default setting, use the no form of this command.

username *username* [**password** ***password*** **|** {encryption-type ***encrypted-password***}] [**maxlinks** *number*] [**authen-group** *WORD*] [**author-group** *WORD*] [**pass-group** *WORD*] [**auto command** *command*] [**bind-ip** *A.B.C.D*] [**bind-mac** *H:H:H:H:H:H*] [**bind-pool** *WORD*] [**bind-port** *port*][**callback-dialstring** *string*] [**callback-line** *line*] [**callback-rotary** *rotary*] [**nocallback-verify**] [**nohangup**] [**noescape**]

no username *username*

Parameters

Parameters	Description
username	Character string of username
password	User password
password	Plain text of the password character string
encryption-type	Type of password encryption
encrypted-password	Cipher text of the password which corresponds to the limited encryption type
maxlinks	The maximum links to the device, the same user can create at the same time
number	number of links
authen-group	*Set the local authentication policy*
WORD	Local authentication policy name
author-group	*Set the local authorization policy*
WORD	Local authorization policy name
pass-group	*Set the local password policy*
WORD	Local password policy name
auto command	Run the specified command when the user logs in. auto command must run at the end of the command line.
command	Run the command character string automatically.

The switch does not support following options.	
Parameters	**Description**
bind-ip	*bind user IP address (non-support)*
A.B.C.D	IP address
bind-mac	*bind user mac address (non-support)*
H:H:H:H:H:H	*48 byte hardware address of ARP record*
bind-pool	*bind user address pool (non-support)*
WORD	address pool name
bind-port	*bind user port (non-support)*
Port	Port
callback-dialstring	callback dial (non-support)
string	telephone number character string
callback-line	callback line (non-support)
line	Stands for the ID of the line.
callback-rotary	callback rotary configuration (non-support)
rotary	rotary number;
nocallback-verify：	no callback verify (non-support)
nohangup	no hangup after the user logs in and run the command automatically (non-support)
noescape	no escape character after the user logs in (non-support)

Default Value

no users

Command Mode

Global configuration mode, local policy group configuration mode

Usage Guidelines

The password is considered as empty character string when there is no password parameter.

user-maxlinks limits the session numbers the same account can establish. But the account will not be counts in if its session is not authenticated by local authentication. Command show aaa users can be used to check the basic information of each on-line user.

The passwords configured for the device do not contain space, that is, when the enable password command is used, space cannot be entered when you enter the plain text of the password.

Currently, our products only support two encryption modes: 0 and 7. The number 0 means the password is not encrypted and the plaintext of password is directly entered. It is the same as the way of directly entering the password. The number 7 means the password is encrypted through an algorithm. You need to enter the encryption text for the encrypted password. The encryption text can be copied from the configuration files of other switches.

Example

The local user is added in the Example below. The username is someone, the password is someother.

```
username someone password someother
```

The local user is added in the Example below, the username is Oscar, the password is Joan. The encryption type applied is 7, namely the encryption method, the ciphertext of the password is needed to be entered.

```
enable password 7 1105718265
```

Given the assumption that the ciphertext of Joan is 1105718265, the value of the ciphertext is obtained from the configuration files of other routers.

Related Command

```
aaa authentication login
```

3.4.10 show local-users

Syntax

To show summary information of all local AAA account, run command show local-users.

show local-users

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

The command is used to show all AAA accounts, including following information: Local group default, links, pw_present, login_tries, login_try_time, and freezing_cause.

Example

```
#show local-users
Local group default:
username          links    pw_present    login_tries    login_try_time    freezing_cause
admin             1        0s            0              0s
aaa               0        0s            0              0s
```

Domain	Description
Local group default:	The local policy group that the account belongs to
links	The connections that the account is using (represents how much users are using the account.)
pw_present	Password validity period
login_tries	login password failure times (sets the maximum failure times and 0 means no set)
login_try_time	login password failure time (sets the maximum failure times and 0 means no set)
freezing_cause	reason of the account being frozen

Related Command

Username

3.4.11 show aaa users

Syntax

To display the summary information about all online AAA users, run show aaa users.

```
show aaa users
```

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

After this command is run, the following information about online users can be displayed: port, username, service, online duration time and peer_address.

Example

```
#show aaa users
Port        User            Service         Duration         Peer Address
=================================================================
console 0       zjl                 exec        04:14:03            unknown
vty 0       aaa             exec            00:12:24          172.16.20.120
```

Domain	Description
Port	ID of the interface where user lies, or index number of VTY
User	Character string of username
Service	Service applied by the user
Duration	Online duration time of the user
Peer Address	IP address of the remote host where the user lies

Related Command

Username

3.5 RADIUS Configuration Commands

This chapter introduces the commands for RADIUS configuration. RADIUS is a distributed client/server system capable of denying the unauthorized network access. RADIUS client is running on the router and sends the request of authentication, authorization and accounting to the central RADIUS server containing the authentication of all the user and the information of network service access.

Please refer to "RADIUS Configuration" about how to configure RADIUS information and learn more about configuration examples.

RADIUS Configuration commands include:

• debug radius

• ip radius source-interface

• radius-server challenge-noecho

• radius-server deadtime

• radius-server host

• radius-server key

• radius-server optional-passwords

• radius-server retransmit

• radius-server timeout

• radius-server vsa send

• radius-server attribute

• radius-server directed-resquest

3.5.1 debug radius

Syntax

To track RADIUS event or packet, run command debug radius. To disable the debug information, run the no form of this command.

```
debug radius { event | packet }
no debug radius { event | packet }
```

Parameters

Parameters	Description
event	Tracing RADIUS event.
packet	Tracing RADIUS packets.

Default Value

None

Command Mode

EXEC

Usage Guidelines

The command can be used for network system debug and finding the reason of user authentication failure.

Example

The following example shows how to enable RADIUS event track:

```
debug radius event
```

3.5.2 ip radius source-interface

Syntax

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the ip radius source-interface command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the no form of this command.

```
ip radius source-interface interface-name
no ip radius source-interface
```

Parameters

Parameters	Description
interface-name	Name of the interface that RADIUS uses for all of its outgoing packets.

Default Value

No default behavior or values

Command Mode

Global configuration mode

Usage Guidelines

Use this command to set the IP address of a subinterface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the subinterface is in the up state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses. This command is especially useful in cases where the device has many subinterfaces and you want to ensure that all RADIUS packets from a particular device have the same IP address.

The specified subinterface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in the down state, then RADIUS reverts to the default. To avoid this, add an IP address to the subinterface or bring the subinterface to the up state.

Example

The following example shows how to configure RADIUS to use the IP address of vlan 1 for all outgoing RADIUS packets:

```
ip radius source-interface vlan 1
```

Related Command

```
ip tacacs source-interface
```

3.5.3 radius-server attribute

Syntax

To designate some attributes to be transmitted during radius authentication and charging, run radius-server attribute. To disable AAA authentication, use the no form of this command.

```
radius-server attribute {4 | 32 | 95}
no radius-server attribute {4 | 32 | 95}
```

Parameters

Parameters	Description
4	Transmits the following address as attribute 4 (NAS ip address) during radius operation.
32	Transmits attribute 32 (NAS identifier) during radius authentication or request.
95	Transmits the following address as attribute 95 (NAS ipv6 address) during radius operation.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

This command is used to designate a specific attribute to be transmitted during radius authentication or radius request.

The radius-server attribute 4 command is used to configure attribute 4 (NAS ip address) in radius and transmit it in the RADIUS packets.

The radius-server attribute 32 command is used to designate attribute 32 (NAS ID) to be transmitted in Radius authentication or charging.

The radius-server attribute 95 command is used to configure attribute 95 (NAS ipv6 address) in radius and transmit it in the RADIUS packets.

Example

The radius-server attribute 4 X.X.X.X command is used when attribute 4 need be transmitted in the Radius packets and attribute 4 serves as the attribute value of X.X.X.X.

The radius-server attribute 32 in-access-req command is used when the NAS identifier need be transmitted in the authentication request.

The radius-server attribute 32 in-account-req command is used when the NAS identifier need be transmitted in the charging request.

radius-server attribute 32 *identifier* configuring NAS identifier

The radius-server attribute 95 X:X:X:X::X command is used when attribute 95 need be transmitted in the Radius packets and X:X:X:X::X serves as the attribute value.

Related Command

None

3.5.4 radius-server challenge-noecho

Syntax

The command "radius-server challenge-noecho" shall be used for not showing the user data under the Access-Challenge Mode.

radius-server challenge-noecho
no radius-server challenge-noecho

Parameters

None

Default Value

The user data is shown under the Access-Challenge.

Command Mode

Global configuration mode

Usage Guidelines

None

Example

```
radius-server challenge-noecho
```

3.5.5 radius-server deadtime

Syntax

The global configuration command "radius-server dead-time" shall be used for improving the echo time of RADIUS when some servers are not workable. The command allows the system to skip the unworkable servers. The "no" format of the command can be used for setting dead-time as 0, namely, all the servers are thought to be workable.

```
radius-server deadtime minutes
no radius-server deadtime
```

Parameters

Parameters	Description
minutes	The time length of RADIUS server thought to be unworkable, the maximum length is 1440 minutes (24 hours)

Default Value

The unworkable time is set as 0, meaning that the server is thought to be workable all the time.

Command Mode

Global configuration mode

Usage Guidelines

The command is used for labeling those RADIUS servers that do not respond to the authentication request as "dead", which avoids too long waiting for the response before using the next server. The RADIUS server labeled as "dead" is skipped by all the requests during the set minutes unless otherwise all the servers are labeled as "dead".

Example

The following Example designates 5-minute dead time for the RADIUS server that does not respond to the request.

```
radius-server deadtime 5
```

Related Command

```
radius-server host
radius-server retransmit
radius-server timeout
```

3.5.6 radius-server directed-resquest

Syntax

To enable the user to set RADIUS server with the format of '@server', run command radius-server directed-resquest in global mode. To return to the default setting, use the no form of this command.

```
radius-server directed-resquest [restricted]
no radius-server directed-resquest [restricted]
```

Parameters

Parameters	Description
restricted	The user can only use the format of '@server' to set RADIUS server.

Default Value

It does not support using the format of '@server' to set RADIUS server.

Command Mode

Global configuration mode

Usage Guidelines

None

Example

```
radius-server directed-resquest
```

Related Command

None

3.5.7 radius-server host

Syntax

The global configuration command "radius-server host" is used for designating IP address of radius server. The "no" format of the command is used for deleting the designated RADIUS host.

```
radius-server host ip-address|ipv6-address [auth-port port-number1] [acct-port port-number2]
no radius-server host ip-address|ipv6-address
```

Parameters

Parameters	Description
ip-address	the ip address of RADIUS server
ipv6-address	the IPv6 address of RADIUS server
auth-port	(optional item) Designating UDP destination port for authentication request.
port-number1	(optional item) The port number of authentication request.
acct-port	(optional item) Designating UDP destination port for accounting request.
port-number2	(optional item) The port number of accounting request.

Default Value

Any RADIUS host is not designated.

Command Mode

Global configuration mode

Usage Guidelines

The command "radius server" can be used repeatedly for designating multiple servers. The polling can be made under the order of configuration when necessary.

Example

The Example below designates RADIUS host whose IP address is 1.1.1.1. The default port is used for accounting and authentication.

```
radius-server host 1.1.1.1
```

The following Example designates Port 12 as the destination port of authentication request on the RADIUS host whose IP address is 1.2.1.2. Port 16 is used as the destination port of accounting request.

```
radius-server host 1.2.1.2 auth-port 12 acct-port 16
```

Related Command

```
aaa authentication
radius-server key
tacacs server
username
```

3.5.8 radius-server key

Syntax

The global configuration command shall be used for setting encryption key for RADIUS communication between the router and RADIUS server. The "no" format of command can be used for invalidating the encryption key.

radius-server key *string* | {encryption-type encrypted-password}

no radius-server key

Parameters

Parameters	Description
string	The secret key used for encrypting. The secret key shall match with the one used by RADIUS server.
encryption-type	encryption type, 0 means no encryption, and 7 means encryption.
encrypted-password	The ciphertext of the password corresponding to the encryption type limited by "encryption-type".

Default Value

The key is empty character string.

Command Mode

Global configuration mode.

Usage Guidelines

The key must correspond to the key used by RADIUS server. All start empty blank will be ignored. The key cannot include the empty character.

Example

The following example shows how to set encryption key to "firsttime":

```
radius-server key firstime
```

Related Command

```
radius-server host
tacacs server
username
```

3.5.9 radius-server optional-passwords

Syntax

To specify that the first RADIUS request to a RADIUS server be made without password verification, use the radius-server optional-passwords command in global configuration mode. To return the default setting, use the no form of this command.

```
radius-server optional-passwords
no radius-server optional-passwords
```

Parameters

The command has no parameters or keywords.

Default Value

optional-password is not used by default.

Command Mode

Global configuration mode

Usage Guidelines

When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the RADIUS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The RADIUS server must support authentication for users without passwords to make use of this feature.

Example

The following example configures the first login to not require RADIUS verification:

```
radius-server optional-passwords
```

Related Command

```
radius-server host
```

3.5.10 radius-server retransmit

Syntax

To specify the number of times the software searches the list of RADIUS server hosts before giving up, use the radius-server retransmit command in global configuration mode. To disable retransmission, use the no form of this command.

```
radius-server retransmit retries
no radius-server retransmit
```

Parameters

Parameters	Description
retries	Maximum number of retransmission attempts. The default is 2 attempts.

Default Value

2 attempts

Command Mode

Global configuration mode

Usage Guidelines

This command is generally used with the radius-server timeout command, indicating the interval for which a router waits for a server host to reply before timing out and the times of retry after timing out.

Example

The following example specifies a retransmit counter value of five times:

```
radius-server retransmit 5
```

Related Command

```
radius-server timeout
```

3.5.11 radius-server timeout

Syntax

To set the interval for which a router waits for a server host to reply, use the radius-server timeout command in global configuration mode. To return the default setting, use the no form of this command.

```
radius-server timeout seconds
no radius-server timeout
```

Parameters

Parameters	Description
seconds	Number that specifies the timeout interval, in seconds. The default is 5 seconds.

Default Value

3 seconds

Command Mode

Global configuration mode

Usage Guidelines

This command is generally used with the radius-server retransmit command.

Example

The following example shows how to set the number of seconds a router waits for a server host to reply before timing out.

```
radius-server timeout 10
```

Related Command

None

3.5.12 radius-server vsa send

Syntax

To configure the network access server to recognize and use vendor-specific attributes, use the command radius-server vsa send. To return to the default setting, use the no form of this command.

```
radius-server vsa send [authentication]
no radius-server vsa send [authentication]
```

Parameters

Parameters	Description
authentication	(Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes.

Default Value

Disabled

Command Mode

Global configuration mode

Usage Guidelines

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The radius-server vsa send command enables the network access server to recognize and use both accounting and authentication vendor-specific attributes. Use the authentication keyword with the radius-server vsa send command to limit the set of recognized vendor-specific attributes to just authentication attributes.

Example

The following example configures the network access server to recognize and use vendor-specific accounting attributes:

radius-server vsa send authentication

Related Command

radius-server host

3.6 TACACS+ Configuration Commands

This chapter describes the commands for configuring TACACS+ security protocols. TACACS+ can be used for authenticating the identity of the user, authorization of service authority and the accounting of the execution process of user service.

Please refer to "TACACS+ Configuration" about how to configure TACACS+ information and learn more about configuration examples.

TACACS+ configuration commands include:

• debug tacacs

• ip tacacs source-interface

• tacacs-server host

• tacacs-server key

• tacacs-server timeout

3.6.1 debug tacacs

Syntax

To trace TACACS+protocol event or checking the packets received or sent, run command "debug tacacs". To return to the default setting, use the no form of this command.

debug tacacs {event | packet}
no debug tacacs {event | packet}

Parameters

Parameters	Description
event	Tracing TACACS+ event
packet	Tracing TACACS+ packet

Default Value

The debug information is disabled by default.

Command Mode

EXEC

Usage Guidelines

The command is only used for the debugging of the network to find out the cause of failure of AAA service.

Example

The following example shows how the debugging of the network to find out the cause of failure of AAA service.

debug tacacs event

Related Command

None

3.6.2 ip tacacs source-interface

Syntax

To apply IP address of the designated interface to all the TACACS＋ packets, run command "ip tacacs source-interface" in global mode. To return to the default setting, use the no form of this command.

```
ip tacacs source-interface subinterface-name
no ip tacacs source-interface
```

Parameters

Parameters	Description
subinterface-name	Interface name corresponding to the source IP address of all TACACS＋ packets.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to set source IP address for all TACACS＋ packets by designating the source interface. So long as the interface is under "up" state, all TACACS+ packets will use IP address of the interface as the source address, thus ensuring that TACACS+ packet of each router will have the same source IP address. So TACACS＋ server will not need to maintain the address list containing the IP address. That is to say, in order to ensure all TACACS＋ packets coming from the specific router to have the same source IP address, the command will work when the router has many interfaces.

The designated interface shall have the IP address linked to the interface. If the designated interface has no IP address or is under a "down" state, the default value will be restored, namely the source IP address shall be determined on the real condition. In order to avoid the case, the IP address shall be added to the interface and the interface shall be ensured under the "up" state.

Example

The following Example will use IP address of the interface vlan1 as source IP address of all TACACS+ packets.

```
ip tacacs source-interface vlan1
```

Related Command

ip radius source-interface

3.6.3 tacacs-server host

Syntax

To designate TACACS+ server in global configuration mode, run command "tacacs server host". To return to the default setting, use the no form of this command.

tacacs-server host *ip-address* [**single-connection**|**multi-connection**] [**port** *integer1*] [**timeout** *integer2*] [**key** *string*]

no tacacs-serve *ip-address*

Parameters

Parameters	Description
ip-address	IP address of the server
single-connection	(optional) Designating router to maintain the single and open TCP connection for the confirmation from AAA/TACACS+ server.
multi-connection	(Optional) Designating router to maintain the different TCP connection for the different confirmation from AAA/TACACS+ server
Port	(optional) Designating port number of server. The option covers the default port number 49.
integer1	(optional) The port number of the server. The range of valid port number is 1 to 65536.
timeout	(optional) Designating the timeout of waiting for server response. It will cover the global timeout set for the server by using the command "tacacs timeout"
integer2	(optional) Setting the value of timeout timer. It is calculated on second.
key	(optional) Designating authentication and encryption key. The secret key shall match with the one used by the program of TACACS+ server. Designating this. It will cover all keys set for the server by command "tacacs key".
string	(optional) Specifying the encrypted key.

Default Value

Disabled

Command Mode

Global configuration mode

Usage Guidelines

The command can be used to search a host according to the specified order by command tacacs-server plus host. As some parameters of tacacs-server host will cover all configurations of commands "tacacs-server timeout" and "tacacs-server key" in global mode, the command can set the communication attribute of each TACACS+ server exclusively. Thus, the security of the network enhanced.

Example

The following example shows how the designated server negotiates with TACACS+ server whose IP address is 1.1.1.1 and carries out AAA authentication. The command can also designate the TCP port number of the server to 51, the timeout is 3 seconds and the encryption key is tacacs-server key.

```
tacacs -server host 1.1.1.1 single-connection port 51 timeout 3 key a_secret
```

3.6.4 tacacs-server key

Syntax

To set the encryption key of the communication process between the device and TACACS+ server, run command tacacs-server key in global mode. To return to the default setting, use the no form of this command.

```
tacacs-server key
no tacacs-server key
```

Parameters

Parameters	Description
key	Uses for setting encryption key. The secret key shall match with the one used by the program of TACACS+ server.

Command Mode

Global configuration mode

Usage Guidelines

You must set the encryption key by command tacacs-server key before running TACACS+ protocol. The key must correspond to the key used by TACACS+ server program. All sentence-initial spaces will be ignored and there cannot be any space in the middle of the key.

Example

The following example shows how to set the encryption key as test key.

```
tacacs-server key test key
```

3.6.5 tacacs-server timeout

Syntax

To set the timeout of TACACS+ waiting for a server reply, run command tacacs-server timeout in global configuration mode. To return to the default setting, use the no form of this command.

```
tacacs-server timeout seconds
no tacacs-server timeout
```

Parameters

Parameters	Description
seconds	The timeout in seconds (ranges from 1 to 600) The default value is 5 seconds.

Default Value

5 seconds

Command Mode

Global configuration mode

Usage Guidelines

If the command tacacs-server sets timeout, it will cover the global timeout set by the command before.

Example

The following example shows how to change the timeout to 10 seconds:

```
tacacs-server timeout 10
```

Chapter 4 HTTP Configuration Commands

4.1 ip http language

Syntax

[no] ip http language {english}

Sets the language of prompt messages during command configuration.

Parameters

Parameters	Description
english	Set web configuration prompt language to English

Default Value

None

Usage Guidelines

Configure this command in global configuration mode.

Example

Set the web configuration prompt language to English.

```
Switch_config#ip http language english
```

4.2 ip http port

Syntax

ip http port { portNumber }

Set the HTTP service port.

no ip http port

Restore the HTTP service port to the default port 80.

Parameters

Parameters	Description
portNumber	HTTP service port, valid range <1-65535>

Default Value

80

Usage Guidelines

Configure this command in global configuration mode.

Example

Set the http service port to 1234.

```
Switch_config#ip http port 1234
```

4.3 ip http secure-port

Syntax

ip http secure-port {portNumber}

Set the HTTPS service port.

no ip http secure-port

Restore the HTTPS service port to the default port of 443.

Parameters

Parameters	Description
portNumber	HTTP service port, valid range <1-65535>

Default Value

443

Usage Guidelines

Configure this command in global configuration mode.

Example

Set the https service port to 1234.

```
Switch_config# ip http secure-port 1234
```

4.4 ip http server

Syntax

[no] ip http server

Open http service

Usage Guidelines

Configure this command in global configuration mode.

Example

Open http service

```
Switch_config# ip http server
```

4.5 ip http http-access enable

Syntax

[no] ip http http-access enable

Configure the http access mode.

Usage Guidelines

Configure this command in global configuration mode. This command is used to access the http: // website.

Example

Set the http access mode.

```
Switch_config# ip http http-access enable
```

4.6 ip http ssl-access enable

Syntax

[no] ip http ssl-access enable

Configure https access mode.

Usage Guidelines

Configure this command in global configuration mode. This command is used to access the https: // website.

Example

Set the https access mode.

```
Switch_config# ip http ssl-access enable
```

4.7 ip http web max-vlan

Syntax

ip http web max-vlan { max-vlan }

Configure the maximum number of VLAN entries displayed on the web page.

no ip http web max-vlan

Restores the maximum number of Vlan entries displayed in the web page to the default value of 100.

Parameters

Parameters	Description
max-vlan	The maximum number of Vlan entries displayed in the Web page, valid range <1-4094>

Default Value

100

Usage Guidelines

Configure this command in global configuration mode.

Example

Set the maximum number of Vlan entries displayed in the web page to 123.

```
Switch_config# ip http web max-vlan 123
```

4.8 ip http web igmp-groups

Syntax

ip http web igmp-groups { igmp-groups }

Configure the maximum number of multicast entries displayed on the web page.

no ip http web igmp-groups

Restores the maximum number of multicast entries displayed on the Web page to the default value of 15.

Parameters

Parameters	Description
igmp-groups	Maximum number of multicast entries displayed on the Web page, valid Range <1-100>

Default Value

15

Usage Guidelines

Configure this command in global configuration mode.

Example

Set the maximum number of multicast entries displayed on the web page to 12.

```
Switch_config#ip http web igmp-groups 12
```

4.9 show ip http

Syntax

show ip http

Usage Guidelines

Used to see if the http server is open

Example

```
Switch_config#show ip http
Http server is running
```

Chapter 5 Interface Configuration Commands

5.1 Interface Configuration Commands

The interface configuration commands include:

• interface

• description

• bandwidth

• delay

• shutdown

• show interface

• show running-config interface

5.1.1 interface

Syntax

To enter the interface configuration mode, run this command. If the logical port is inexistent, you have to create this port first and then enter the port mode. If the physical port is inexistent, the command will fail to be executed. The negative form of this command has different functions for the physical port and the logical port.

[no] interface *port*

To return to the default settings of the physical port, run this command.

no interface *physical-port*

To delete the logic interface, run this command.

no interface *logical-port*

Parameters

Parameters	Description
Port	Stands for the existent physical or logical port.

Default Value

The default mode is not the port mode.

Usage Guidelines

When you execute this command in configuration mode, you have to enable this command to be in port configuration mode first. When the port command is configured, you shall use the exit command to exit from the port mode.

Example

The following example shows how to enter the port mode of port g0/1.

```
Switch_config#
Switch_config#interface gigaEthernet0/1
Switch_config_g0/1#exit
Switch_config#
```

5.1.2 description

Syntax

To set the description information of a port, run the following command.

[no] description *line*

Parameters

Parameters	Description
line	Stands for the character string of the description information, among which space may exist.

Default Value

There is no description information by default.

Usage Guidelines

The command must be configured in port configuration mode.

Example

The following example shows how to set the description information of port g01/1 to up link.

```
Switch_config# interface gigaEthernet0/1
Switch_config_g0/1# description uplink
```

5.1.3 bandwidth

Syntax

To set the bandwidth of an interface, run the following command.

[no] bandwidth *kilobps*

Parameters

Parameters	Description
kilobps	port bandwidth, the value ranges from 1 to 10000000(kbps).

Default Value

The default value of the 100M port is 100000 and the default value of gigabit port is 1000000.

Usage Guidelines

The command must be configured in port configuration mode.

NOTE: The configured bandwidth does not mean the actual bandwidth of a port, but is used by some protocol to calculate the port cost.

Example

The following example shows how to set port g0/1 to 10000000.

```
Switch_config # interface gigaEthernet0/1
Switch_config_g0/1# bandwidth 10000000
```

5.1.4 delay

Syntax

To set the delay of an interface, run the following command.

[no] delay *tensofmicroseconds*

Parameters

Parameters	Description
tensofmicroseconds	port delay, the value ranges from 1 to 10000000 (10 microseconds)

Default Value

The default value of the delay is 1.

Usage Guidelines

This command is configured in port configuration mode.

Example

The following example shows how to set the delay of an interface to 10.

```
Switch_config_g0/1# delay 10
```

5.1.5 shutdown

Syntax

To enable the port, run this command.

[no] shutdown

Parameters

None

Default Value

The physical port is in enabled shutdown status by default.

Usage Guidelines

This command can be used in port mode to enable or disable port.

Example

The following example shows how to enable port g0/1.

```
Switch_config_g0/1#
Switch_config_g0/1# no shutdown
Switch_config_g0/1#
```

5.1.6 show interface

Syntax

To browse the state of an interface, run the following command.

show interface <*port*>

Parameters

Parameters	Description
Port	Name of an interface If a specific port is not in the command, the system will show the statuses of all ports.

Default Value

None

Usage Guidelines

This command can be used in EXEC and configuration modes to show the physical status and packet reception statistics of a port.

Example

The following example shows the information about port g0/1:

```
Switch_config# show interface gigaEthernet 0/1
GigaEthernet0/1 is administratively down, line protocol is down
Hardware is Giga-Combo-FX, address is 00e0.0fe4.d083 (bia 00e0.0fe4.d083)
MTU 1500 bytes, BW 1000000 kbit, DLY 10 usec
Encapsulation ARPA
Auto-duplex,      Auto-speed
low-control off
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
Received 0 packets, 0 bytes
0 broadcasts, 0 multicasts
0 discard, 0 error, 0 PAUSE
0 align, 0 FCS, 0 symbol
0 jabber, 0 oversize, 0 undersize
0 carriersense, 0 collision, 0 fragment
0 L3 packets, 0 discards, 0 Header errors
Transmited 0 packets, 0 bytes
0 broadcasts, 0 multicasts
0 discard, 0 error, 0 PAUSE
0 sqettest, 0 deferred
0 single, 0 multiple, 0 excessive, 0 late
0 L3 forwards
```

5.1.7 show running-config interface

Syntax

To display the settings of a port, run the following command.

show running-config interface *port*

Parameters

Parameters	Description
Port	Stands for the existent port.

Default Value

None

Usage Guidelines

This command can be executed in EXEC or configuration mode to browse the settings of a port.

Example

The following example shows the settings of port g0/1:

```
Switch_config#show running-config interface g0/1
Building configuration...

Current configuration:
!
interface GigaEthernet0/1
shutdown
description uplink
bandwidth 10000000
delay 10
Switch_config#
```

5.2 Configuration Example

The following example shows how to create a VLAN port, set its description information and IP address and browse the status and settings of this port. To browse the port status and configuration, run show command.

```
Switch_config#
Switch_config# interface vlan1
Switch_config_v1# description uplink
Switch_config_v1#
Switch_config_v1# ip address 192.168.1.1 255.255.255.0
Switch_config_v1# exit
Switch_config#
Switch_config# show running-config interface vlan1
Building configuration...
Current configuration:
!
interface VLAN1
description uplink
ip address 192.168.1.1 255.255.255.0
Switch_config# show interface vlan1
VLAN1 is up, line protocol is down
Description: uplink
Hardware is EtherSVI, Address is 00e0.0fe4.d06a(00e0.0fe4.d06a)
Interface address is 192.168.1.1/24
  BYTES bytes, BW 1000000 kbit, DLY 2000 usec
Encapsulation ARPA
ARP type: ARPA, ARP timeout 04:00:00
Peak input rate 0 pps, output 0 pps
0 packets input, 0 bytes
Received 0 broadcasts, 0 multicasts
0 mpls unicasts, 0 mpls multicasts, 0 mpls input discards
0 input errors, 0 input discards
0 packets output, 0 bytes
Transmited 0 broadcasts, 0 multicasts
0 mpls unicasts, 0 mpls multicasts, 0 mpls output discards
0 output errors, 0 discards
Switch_config#
```

Chapter 6 Interface Range Commands

6.1 Interface Range

Syntax

interface range *type slot/<port1-port2 | port3>*[, *<port1-port2|port3>*]

Parameters

Name	Usage Guidelines	Value Range
type	Port type	All reasonable port types, except the manager port on the main control board of the cabinet-like switch
slot	Slot number	All legal slot numbers
port1	Starting value of the port numbers	All legal port numbers on a slot
port2	Ending value of the port numbers	All legal port numbers on a slot which are no smaller than port 1
port3	An independent port	All legal port numbers on a slot

Default Value

None

Usage Guidelines

The command can be used to enter the interface range mode.

Example

The following example shows how to enter the port configuration mode of gigabit Ethernet port 1, 2, 3 or 4 on slot 0.

```
switch_config# interface range gigaEthernet 0/1-4
switch_config_if_range#
Note:
There is no space at the neither side of the symbol "_" and the symbol ",".
```

Chapter 7 Port Physical Characteristic Configuration Commands

7.1 Port Physical Characteristic Configuration Commands

Configuration commands are shown as follows:

• speed

• duplex

• flow-control

7.1.1 speed

Syntax

To set the speed of the interface, ran speed {10| 100 | 1000 | auto}.

speed {*10* | *100* | *auto* } (TX port)

speed {*100* | *1000* | *auto* } (Optical port)

no speed

Parameters

Parameters	Description
10, 100,1000	Sets the speed of an interface to 10M, 100M or 1000M.
auto	Sets the speed of the interface to auto.

Default Value

The speed of the electrical interface is auto, the speed of the 100M optical interface is 100M and the speed of the 1000M optical interface is 1000M.

Usage Guidelines

This command is configured in layer-2 interface configuration mode.

NOTE: The optical interface speed is fixed. The gigabit optical interface enables auto-negotiation function by default. The optical/electric port cannot support the gigabit and full-duplex at the same time. The ordinary TX port does not support speed 1000.

Example

The following example shows how to set the speed of interface g0/1 to 100M.

```
Switch_config# interface g0/1
Switch_config_g0/1# speed 100
```

7.1.2 duplex

Syntax

To set the duplex mode of an interface, run duplex {auto | full | half}.

duplex {*auto* | *full* | *half* }

no duplex

Parameters

Parameters	Description
auto	Automatic negotiation
full	Full duplex
half	Half duplex

Default Value

The electrical interface is in automatic negotiation mode, while the optical interface is in full duplex mode.

Usage Guidelines

This command is configured in layer-2 interface configuration mode.

NOTE: The duplex mode of the optical interface is fixed, that is, the duplex mode of all optical interfaces is the full duplex mode. The optical/electric port cannot support the gigabit and full-duplex at the same time. There is backpressure in half-duplex mode.

Example

The following example shows how to set the interface g0/1 to the full duplex mode.

```
Switch_config# interface g0/1
Switch_config_g0/1# duplex full
```

7.1.3 flow-control

Syntax

To configure flow control for an interface, run the following command.

flow-control { **on | off | auto**}

Parameters

Parameters	Description
on	Enables the flow control.
off	Disables the flow control.
auto	Auto-negotiation Mode

Default Value

The flow control function is disabled by default.

Usage Guidelines

The command must be configured in L2 port configuration mode.

NOTE: The difference between “flow-control auto” and “flow-control on” is in the “auto” mode the device sends flow control frame only when it negotiates successfully with the opposite end as the system is compelled to receive flow control frame in both modes.

Example

The following example shows how to enable the flow control function for port g0/1.

```
Switch_config#int g0/1
Switch_config_g0/1#flow-control on
```

Chapter 8 Port Additional Characteristics Configuration Commands

8.1 Configuring Port Isolation

8.1.1 port-protected

Syntax

To configure a port isolation group, run the following command. To return to the default setting, use the no form of this command.
port-protected *group-id*
[no] port-protected *group-id*

Parameters

Parameters	Description
group-id	Configures port isolation group 1 to 28.

Default Value

None

Usage Guidelines

The command can be used to configure the group isolation in global configuration mode.

Example

The following example shows how to set ID of the isolation group to 1.

```
Switch_config#port-protected 1
```

8.1.2 Description

Syntax

To set the port isolation group description, run the following command. To delete the description, use the no form of this command.
description *word*
no description

Parameters

Parameters	Description
Word	*Sets the port isolation description. The description covers 31 characters at most.*

Default Value

None

Usage Guidelines

The command can be used to describe the group in global configuration mode.

Example

The following example shows how to set ID of the isolation group g1 to 1.

```
Switch-config-p1#description g1
```

8.1.3 switchport protected

Syntax

To set port isolation, run the following command. To return to the default setting, use the no form of this command.
switchport protected *<group-id>*
no switchport protected

Parameters

Parameters	Description
group-id	Selects the port isolation group 1 to 28.

Default Value

None

Usage Guidelines

The command must be configured in layer-2 port configuration mode. The system configures isolation not based on groups by default and group-id doesn't need to configure at the end. If configures isolation based on groups, it should be configured in global mode. Only deleting the isolation on all ports can you reselect isolation based on groups or not based on groups.

Example

The following example shows how to set isolation of port g0/1 not based on groups.

```
Switch_config_g0/1#switchport protected
```

8.2 Configuring the Storm Control Command

Syntax

To configure the storm control function of the port, run the following command. To return to the default setting, use the no form of this command.
storm-control {**broadcast** | **multicast** | **unicast**} **threshold** *count*
no storm-control {**broadcast** | **multicast** | **unicast**} **threshold**

Parameters

Parameters	Description
broadcast | multicast | unicast	Defines broadcast/multicast/unicast storm control.
count	Defines the threshold flux of the storm. 1-65535

Default Value

The storm control function is disabled by default.

Usage Guidelines

The command must be configured in L2 port configuration mode.

Example

The following example shows how to set the unknown unicast-frame storm to 20pps on port g0/1.

```
Switch_config#interface g0/1
Switch_config_g0/1#storm-control unicast threshold 20
```

8.3 Configuring Switchport Rate Limit

Syntax

To configure the rate limit for a port, run this command. To return to the default setting, use the no form of this command.
switchport rate-limit {*band* | ***bandwidth*** *percent*} { **ingress**|**egress**}
no switchport rate-limit{ ingress|egress}

Parameters

Parameters	Description
Band	Means the rate of the flow. The step length is 64Kbps.
percent	Means the percentage of the flow. unit 1%
ingress	Functions on the ingress port.
egress	Functions on the egress port.

Default Value

The rate of the port is not limited by default.

Usage Guidelines

Layer-2 port configuration mode

Example

The following example shows how to set the incoming flow rate to 1M on port g0/1.

```
Switch_config#interface  g0/1
Switch_config_g0/1#switchport rate-limit 16 ingress
```

8.4 Configuring Port Loop Check

Syntax

To configure the interval for a port to transmit the loop check packets, run keepalive second. To return to the default setting, use the no form of this command.
keepalive *second*
[**no**] **keepalive** *second*

Parameters

Parameters	Description
Second	Interval, unit: second.

Default Value

12 seconds

Usage Guidelines

The command must be configured in physical interface configuration mode.

Example

The following example shows how to set the transmission interval to 10 seconds on interface g0/1.

```
Switch_config#interface g0/1
Switch_config_g0/1#keepalive 10
```

8.5 Configuring MAC Address Learning

Syntax

To configure the MAC address learning for a port, run switchport disable-learning. To return to the default setting, use the no form of this command.
switchport disable-learning
[**no**] **switchport disable-learning**

Parameters

None

Default Value

The MAC address learning is enabled by default.

Usage Guidelines

The command must be configured in physical interface configuration mode.

Example

The following example shows how to disable the MAC address learning on interface g0/1.

```
Switch_config#interface g0/1
Switch_config_g0/1#switchport disable-learning
```

8.6 Configuring Port Security

The port security configuration commands include:
• switchport port-security mode
• switchport port-security dynamic
• switchport port-security static
• switchport port-security sticky

8.6.1 switchport port-security mode

Syntax

To set the interface security mode, run the following command. To return to the default setting, use the no form of this command.
switchport port-security mode {**dynamic | static** *accept*|*reject* **| sticky**}
[**no**] **switchport port-security mode**

Parameters

None

Default Value

The port security is disabled by default.

Usage Guidelines

The command must be configured in physical interface configuration mode.

Example

The following example shows how to set interface g0/1 to the dynamic port security mode.

```
Switch_config#inter g0/1
Switch_config_g0/1#switchport port-security mode dynamic
```

8.6.2 switchport port-security dynamic

Syntax

To configure the maximum number of MAC addresses when the port is in dynamic security mode, run switchport port-security dynamic maximum. To return to the default setting, use the no form of this command.
switchport port-security dynamic maximum *dynamic_number*
[**no**] **switchport port-security dynamic maximum**

Parameters

Parameters	Description	Value Range
dynamic_number	The maximum address number that can be learned	1-2048

Default Value

The number of MAC addresses that can be learned is 1- the maximum number of items in the MAC address table.

Usage Guidelines

The command must be configured in physical interface configuration mode.

Example

The following example shows how to set the number of that can be learned MAC addresses of port g0/1 to 10.

```
Switch_config#inter g0/1
Switch_config_g0/1# switchport port-security dynamic maximum 10
```

8.6.3 switchport port-security static mac-address

Syntax

To configure a static security MAC address, run switchport port-security static mac-address H.H.H. To return to the default setting, use the no form of this command.
switchport port-security static mac-address H.H.H
[**no**] **switchport port-security static mac-address H.H.H**

Parameters

None

Default Value

None

Usage Guidelines

The command must be configured in physical interface configuration mode.

Example

The following example shows how to set MAC address 0001.0002.0003 to a static security MAC address.

```
Switch_config#inter g0/1
Switch_config_g0/1# switchport port-security static mac-address 1.2.3
```

8.6.4 switchport port-security sticky

Syntax

To configure the sticky characteristic of MAC address, run the following command. To return to the default setting, use the no form of this command.
switchport port-security sticky {maximum *sticky_number*| **mac-address** H.H.H| **aging-time** *aging_time* | **absolute-aging | inactivity-aging}**
[no] switchport port-security sticky {maximum_| mac-address H.H.H| aging-time | absolute-aging | inactivity-aging}

Parameters

Parameters	Description
sticky_number	The maximum address number that can be learned. The default is 100 and the value range is from 1 to 2048.
H.H.H	Mac Address
aging_time	aging time Unit: minute, the default value is 0 and the value range is 0 to 100.

Default Value

There is no sticky of mac address by default.

Usage Guidelines

The command must be configured in physical interface configuration mode.

Example

The following example shows how to set mac: 4433.0002.0021 to the sticky mac.

```
Switch_config#inter g0/1
Switch_config_g0/1# switchport port-security sticky mac-address 4433.0002.0021
```

8.7 Configuring Port Binding

Syntax

To bind a MAC address to a IP address, run switchport port-security bind|block {ip|arp|both-arp-ip ip-addr| ipv6 ipv6-addr | mac mac-addr }.
To cancel the address binding one by one or to exit the port binding state by cancelling all addresses on the port, run no switchport port-security bind|block {ip|arp| both-arp-ip ip-addr | ipv6 ipv6-addr | mac mac-addr}.
switchport port-security bind|block {**ip|arp|both-arp-ip** *ip-addr*| **ipv6** *ipv6-addr* | **mac** *mac-addr* }
no switchport port-security bind|block {**ip|arp| both-arp-ip** *ip-addr* | **ipv6** *ipv6-addr* | **mac** *mac-addr*}

Parameters

Parameters	Description	Value Range
ip-addr	IP address	A.B.C.D
ipv6-addr	Stands for the IPV6 address	X:X:X:X::XX
Mac-addr	Stands for the MAC address.	H.H.H

Default Value

None

Usage Guidelines

It works in layer-2 port configuration mode.
The port binding function is forbidden by default. However, if one address is bound, the port is then in binding state unless you use the negative form of this command to clear all bound address items.

Example

The following example shows how to bind IP address 1.2.3.4 to MAC address 0001.0001.1111 on interface g0/1 to decline the IP packets and ARP packets from the bound address.
Switch_config#inter g0/1
Switch_config_g0/1# switchport port-security block both-arp-ip 1.2.3.4 mac 0001.0001.1111

8.8 SVL/IVL

Syntax

To set SVL, run the following command.
[no]vlan shared-learning

Parameters

None

Default Value

VLAN IVL on the port

Usage Guidelines

This command is run in global configuration mode.

Example

The following example shows how to set SVL.

```
Switch_config#vlan shared-learning
```

8.9 Configuring Link Scan Commands

Syntax

To set the scan interval of an interface, run the following command.
[no] Link scan [normal | fast] *interval*

Parameters

Parameters	Description
[normal | fast]	Normal means standard link scan mode. Fast means fast link scan mode.
interval	scan interval, unit 1ms, 10-1000.

Default Value

The scan interval is 500ms in standard mode by default.
Fast mode, the default interval is 10ms.

Usage Guidelines

This command is configured in global configuration mode. The Fast mode is mainly used for cooperating with the protocol, for instance, RSTP. The Normal mode is mainly used for finding up/down.

Example

The following example shows how to set the scan interval of a switch to 20ms.
Link scan normal 20

8.10 Configuring the Enhanced Link State Detection Command

Syntax

To enable/disable the enhanced link state detection command, run the following command.
[no] switchport enhanced-link

Parameters

None

Default Value

Disabled.

Usage Guidelines

The command must be configured in port configuration mode.

Example

The following example shows how to enable the enhanced link state detection on interface g0/1:

```
Switch_config#interface g0/1
Switch_config_g0/1#switchport enhanced-link
```

8.11 Configuring System MTU

Syntax

To configure the value of system mtu, run the following command.
[no] system mtu *mtu*

Parameters

Parameters	Description
mtu	Sets the value of system mtu, 1500-9216.

Default Value

The default mtu is 1500 bytes.

Usage Guidelines

This command is configured in global configuration mode.

Example

The following example shows how to set system mtu to 2000 bytes.

```
Switch#config
Switch_config#system mtu 2000
```

Chapter 9 Port Mirroring Configuration Commands

9.1 Port Mirroring Configuration Commands

Port mirroring configuration commands include:

• mirror

• show mirror

9.1.1 mirror

Syntax

To set port mirror, run this command.
[**no**] **mirror session** *session_number* {**destination** {**interface** *interface-id* } { **rspan** *vid tpid*} | **source** {**interface** *interface-id* [, | -] [**rx** | **tx** | **both**] }

Parameters

Parameters	Description
session_number	Number of port mirroring Value range: 1-4
destination	Information about destination port mirroring
vid	VID of the tag of remote mirroring
TPID	TPID of the tag of remote mirroring
source	Information about the mirrored port
rx **|** ***tx*** **|*****both***	Data flow that will be mirrored Rx means that only the input data is mirrored; tx means that only the output data is mirrored; both means both the input data and the output data are mirrored.

Default Value

None

Usage Guidelines

This command is configured in global configuration mode.

NOTE: The unknown unicast packets including the unknown unicast and the broadcast take the source whose mirroring number is 1 as the source port in output mirroring.

Example

Local mirroring: The following example shows how to set interface g0/2 as the output mirroring of interface g0/1.

```
Switch_config# mirror session 1 destination interface g0/2
Switch_config# mirror session 1 source interface g0/1
```

Remote mirroring: The following example shows how to set interface g0/2 as the local output mirroring of interface g0/1. The VLAN of remote mirroring is 100. TPID is 0x8100.

```
Switch_config# mirror session 1 destination interface g0/2 rspan 100 0x8100
Switch_config# mirror session 1 source interface g0/1
```

9.1.2 show mirror

Syntax

To display the configuration information about port mirroring, run the following command.
show mirror [session *session_number]*

Parameters

Parameters	Description
session_number	Number of port mirroring Value range: 1-4

Default Value

None

Chapter 10 Power Over Ethernet Configuration Commands

10.1 POE Configuration Commands

10.1.1 show poe system

Display POE related system information

show poe system

Parameters

None

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

POE DRIVER

POE CHIP

POE Port Num

PSE Power Management (There are three types: automatic, preemption and non-preemption)

PSE Total Power

PSE Usage Threshold (Set by percentage)

PSE Alarm Power

PSE Lower-Port-Disable Power

PSE Lower-Port-NoConnect Power

PSE Consumed Power

PSE Peak Power

PSE Mib Notification

Temperature PSE

Example

```
Switch#show poe system
POE DRIVER:PETH PD69012 DRV POE CHIP:PD69012
POE Port Num:24
PSE PowerManagement:Preemptive PSE Total Power:80000 mW
PSE Usage Threshold:80% PSE Alarm Power:64000 mW
PSE Lower-Port-Disable Power:62000 mW PSE Lower-Port-NoConnect Power:44000 mW PSE Consumed Power:47500 mW
PSE Peak Power:101300 mW PSE Mib Notification:Disable PSE Temperature:38 degree
```

Related Command

None

10.1.2 show poe all

Display POE port information description table

show poe all

Parameters

None

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

Port enabled/disabled

Port detection Port power status(disabled、searching、delivering-power、fault)

delivering-power Indicates normal power supply

Port pairs Line sequence of port power supply, signal indicates power supply of signal line, spare indicates power supply of idle line

Port priority Priority of port power supply: critical, high, low from high to low

Example

```
Switch#show poe all
Port    Enable   Status    Pair    Priority
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
f0/3    enabled  Disabled  signal  low
```

Related Command

None

10.1.3 show poe power

Display power supply information for all ports

show poe power

Parameters

None

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

Max (Maximum power limit of the port)

Current (Current power of the port)

Average (The average power of the port. The peak power of the port is valid only when the power statistics are enabled. The bottom power of the bottom port is valid only when the power statistics are enabled.)

Example

```
Switch#show poe power
```

Port	Current	Max	Average	Peak	Bottom
f0/3	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/4	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/2	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/1	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/5	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/6	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/7	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/8	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/9	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/10	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/11	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/12	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/13	7600 mW	30000 mW	7620 mW	7800 mW	7600 mW
f0/14	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/15	7600 mW	30000 mW	7600 mW	7800 mW	7600 mW
f0/16	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/17	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/18	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/19	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/20	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/21	0 mW	30000 mW	0 mW	0 mW	0 mW
f0/22	15900 mW	30000 mW	15890 mW	16200 mW	14900 mW
f0/23	7700 mW	30000 mW	7780 mW	7800 mW	7700 mW
f0/24	8400 mW	30000 mW	9850 mW	22500 mW	6500 mW

Related Command

None

10.1.4 show poe interface

Display detailed POE information for the specified port

show poe interface type slot/port

Parameters

parameter	Description
Type	Interface Type
Slot	Slot or card number
Port	Slot or card port number

Default Value

None

Command Mode

Monitoring Mode

Usage Guidelines

PSE Port Number

Port Power Enabled

Port Force Power

Port Detection Status Port power status(disabled, searching, delivering-power, fault)

Port Fault Status

Port Last Disconnection Reason

Port Pairs Line sequence of port power supply, signal indicates power supply of signal line, spare indicates power supply of idle line

Port IEEE Class

Port Priority Port power priority, critical, high, low port from high to low Current

Port Voltage

Port Current Power

Port Average Power The average power of the port. The peak power of the port is valid only when the power statistics are turned on.

Port PD Discription

Example

```
Switch#show poe interface f0/24 PSE Port
Number : 23
Port Power Enabled : enable
Port Force Power : disable
Port Detection Status : delivering-power
Port Fault Status :
Port Last Disconnection Reason :
Port was disabled Port Pairs : signal
Port IEEE Class : 0 Port Priority : critical Port Current : 163 mA
Port Current Power : 8400 mW Port Average Power : 8440 mW
Port Peak Power : 22500 mW Port Bottom Power : 6500 mW Port Max Power : 30000 mW Port PD Discription : AP
```

Related Command

None

10.1.5 poe power-management

Configure switch power management mode

poe power-management {auto | preemptive | non-preemptive | lowDisable | lowNoConnect } value

Parameters

parameter	Description
Auto	Configure the switch power management mode to automatic mode
Preemptive	Configure the switch power management mode to preempt mode
non-preemptive	Configure the switch power management mode to non-preemptive mode
lowDisable	When the total power exceeds lowDisable, the port can no longer supply power, and when it is lower, it can continue to supply power. lowDisable = machine power – value
lowNoConnect	When the total power exceeds lowNoConnect, ports with priority lower than or equal to the lowest priority of the current power supply will be powered off and enabled. lowNoConnect = lowDisable – value

Default Value

Power management is automatic（auto）

Command Mode

Global configuration mode

Usage Guidelines

Automatic mode: The maximum port power limit cannot be set, and the default is the maximum port power supported by the chip.

Preemption mode: Enable the maximum power limit function of the port; enable the power supply priority function of the port;

Non-preemption mode: enable the maximum power limit function of the port; enable the power supply priority function of the port;

Preemption means that under full load conditions, when a high-priority power supply interface accesses a PD device, power is normally supplied to the newly connected PD device, and the port with the lowest power supply priority is powered off;

Non-preemption means that when the device is under full load, a high-priority power supply interface connects to the PD device and generates a prompt message, prompting that the high-priority interface has a PD device access.

Example

The following command sets the power management mode to preemptive mode

```
Switch_config#poe power-management preemptive
Switch_config#poe power-management lowDisable 18000
Switch_config#poe power-management lowNoConnect 18000
```

Related Command

poe max-power

poe priority

10.1.6 poe led-time

Configure the duration when the LED mode is POE

poe led-time time

no poe led-time

Parameters

parameter	Description
Time	Unit is second

Default Value

30 seconds duration when LED mode is POE

Command Mode

Global configuration mode

Usage Guidelines

The prefix no will set the duration back to the default

Example

The following command sets the duration to 10 seconds

```
Switch_config#poe led-time 10
```

Related Command

None

10.1.7 poe mib notification-stop

No trap will be sent to the user when the port power supply changes or a power alarm occurs

poe mib notification-stop

no poe mib notification-stop

Parameters

None

Default Value

By default, when the port power supply changes or a power alarm occurs, a trap will be sent to notify the user

Command Mode

Global configuration mode

Usage Guidelines

The prefix no is restored to the default value

Example

The following command configures not to send a trap to notify the user when the port power supply changes or a power alarm occurs

```
Switch_config#poe mib notification-stop
```

Related Command

None

10.1.8 poe pse-unprotect

Port power protection can prevent problems caused by PSE device docking.

poe pse-unprotect

no poe pse-unprotect

Parameters

None

Default Value

Port protection is enabled by default

Command Mode

Global configuration mode

Usage Guidelines

The prefix no is restored to the default value

Example

The following command turns off port protection

```
Switch_config# poe pse-unprotect
```

Related Command

None

10.1.9 poe counter value

Enable global and port power statistics

poe counter value

no poe counter

Parameters

parameter	Description
value	Sampling interval in seconds

Default Value

Turn off power statistics by default

Command Mode

Global configuration mode

Usage Guidelines

The prefix no is restored to the default value

Example

The following command sets the sampling interval of power statistics to 5 seconds.

```
Switch_config# poe counter 5
```

Related Command

None

10.1.10 poe threshold

Configure the percentage of alarm power to the total power

poe threshold value

no poe threshold

Parameters

parameter	Description
value	Alarm power relative to the total power

Default Value

By default, the percentage of the alarm power to the power of the whole machine is 100%

Command Mode

Global configuration mode

Usage Guidelines

The prefix no will set the percentage back to the default

Example

The following command sets the percentage of alarm power to the power of the whole machine to 50%

```
Switch_config#poe threshold 50
```

Related Command

poe power-management

10.1.11 poe standard

Configure PSE power standards

poe standard {AF| AT| MAX}

Parameters

parameter	Description
AF	Select AF standard, the port can be powered up 15.4W
AT	Select AT standard, the port can be powered up 30W
MAX	Select MAX to take the latest standard supported by this switch. For both AF and AF AT devices take AT, for AF only supported Devices that do not support AT take AF.

Default Value

Take the latest standard (MAX) supported by this switch by default

Command Mode

Global configuration mode

Usage Guidelines

Select AF standard, the port can supply power up to 15.4W; Select AT standard, the port can supply power up to 30W;

Select MAX to take the latest standard supported by this switch. For devices that support both AF and AT, take AT, and for devices that only support AF but not AT.

Example

The following command sets the PSE power standard to AF

```
Switch_config#poe standard AF
```

Related Command

None

10.1.12 poe disable

Configure port power supply

poe disable { time-range name | <cr>} no poe disable {time-range| <cr>}

Parameters

parameter	Description
time-range name	name is the name of the unpowered time period
<cr>	Enter, that is, enter poe disable separately to close the port

Default Value

By default, the port power supply is enabled, and there is no time period power limitation.

Command Mode

Port configuration mode

Usage Guidelines

poe disable

no poe disable

poe disable time-range name

no poe disable time-range

Example

The following command will disable the power supply enable of port f0 / 1

```
Switch_config_f0/1#poe disable
```

The following command enables the closed port power supply when the time of the POE device is within the time period named Sunday_free.

```
Switch_config_f0/1poe disable time-range Sunday_free
```

Related Command

time-range

10.1.13 poe max-power

Configure port maximum power poe

max-power value no poe max-power

Parameters

parameter	Description
value	Maximum port power in mW

Default Value

Maximum port power is 30000mW by default

Command Mode

Port configuration mode

Usage Guidelines

The prefix no will set the port maximum power back to the default value; this command is a command in non-auto mode.

Example

The following command sets the maximum power of port f0 / 1 to 15000mW

```
Switch_config_f0/1#poe max-power 15000
```

Related Command

poe power-management

10.1.14 poe priority

Configure port power priority

poe priority {critical | high | low }

Parameters

parameter	Description
critical	Highest priority
high	Second highest priority
low	Lowest priority

Default Value

Port power priority is low by default

Command Mode

Port configuration mode

Usage Guidelines

This command is a command in non-auto mode.

Example

The following command sets the power priority of port f0 / 1 to critical

```
Switch_config_f0/1#poe priority critical
```

Related Command

poe power-management

10.1.15 poe PD-discription

Configure port descriptions, usually describing PD devices

poe PD-discription string

no poe PD-discription

Parameters

parameter	Description
string	Port description string

Default Value

None

Command Mode

Port configuration mode

Usage Guidelines

The prefix no means to clear the description string

Example

The following command sets the POE port description of port f0 / 1 to "AP-1"

```
Switch_config_f0/1#poe PD-discription AP-1
```

Related Command

None

10.1.16 poe force-power

Configure the port power supply function

poe force-power

no poe force-power

Parameters

None

Default Value

Forced power off by default

Command Mode

Port configuration mode

Usage Guidelines

The prefix no means to turn off the forced power supply

Example

The following command configures the POE port of port f0 / 1 to force power

```
Switch_config_f0/1#poe force-power
```

Related Command

poe power-management

Usage Guidelines

This command can be used to display the information about port mirroring.

Example

The following example shows how to display the information of port mirroring on port 1.

```
Switch_config#show mirror session 1

Session 1
---------
Destination Ports: g0/3
Source Ports:
        RX Only:        None
        TX Only:        None
        Both:           g0/2
```

Chapter 11 MAC Address Configuration Commands

11.1 MAC Address Configuration Commands

11.1.1 mac address-table static

Syntax

To add a static MAC address, run mac address-table static mac-addr vlan vlan-id interface interface-id. To cancel the static MAC address, run no mac address-table static mac-addr vlan vlan-id interface interface-id.

mac address-table static mac-addr vlan vlan-id interface interface-id

[**no**] **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

Parameters

Parameter	Description
mac-addr	MAC address Value range: H.H.H
vlan-id	A VLAN that the MAC address belongs to Value range: 1-4094
interface-id	Physical port that the MAC address belongs to.

Default Value

None

Usage Guidelines

This command is configured in global configuration mode.

Example

The following example shows how to bind MAC address 0004.5600.67ab to port g0/2 of VLAN1.

```
Switch_config# mac address-table static 0004.5600.67ab vlan 1 interface g0/2
```

11.1.2 mac address-table aging-time

Syntax

To configure the aging time of the MAC address table, run the following command.

mac address-table aging-time [**0** | **10-1000000**]

Parameters

Parameters	Description
0	Means that the MAC address never ages.
10-1000000	Aging time of the MAC address whose unit is second

Default Value

300s

Usage Guidelines

This command is configured in global configuration mode.

Example

The following example shows how to set the aging time of the MAC address to 100 seconds.

```
Switch_config# mac address-table aging-time 100
```

11.1.3 mac address-table blackhole

Syntax

To add or delete a black hole MAC address, run the following command.

[**no**] **mac address-table blackhole***mac-addr* **vlan** *vlan-id*

Parameters

Parameters	Description
mac-addr	MAC address Value range: H.H.H
vlan-id	A VLAN that the MAC address belongs to Value range: 1-4094

Default Value

None

Usage Guidelines

This command is configured in global configuration mode.

Example

The following example shows how to configure the address 0004.5600.67ab to the black hole mac on VLAN1.

```
Switch_config# mac address-table blackhole 0004.5600.67ab vlan 1
```

11.1.4 show mac address-table

Syntax

To display the MAC address table of the switch, run the following command.

show mac address-table [dynamic [interface *interface-id* | **vlan** *vlan-id***] | static | brief | multicast | interface** *interface-id* **| vlan** *vlan-id* **| H.H.H | blackhole]**

Parameters

Parameters	Description
dynamic	Dynamically-learned MAC address table
interface-id	Name of an interface
vlan-id	VLAN ID Value range: 1-4094
static	Static MAC address table
brief	Brief information about the MAC address
multicast	Multicast MAC address table

Parameters	Description
Interface	Interface's MAC address table
Vlan	Vlan mac address table
H.H.H	Specific address
Blackhole	Blackhole MAC address;

Default Value

None

Usage Guidelines

This command is used to display the MAC address table.

Example

The following example shows how to display all dynamic MAC address tables.

```
Switch_config#show mac address-table
Mac Address Table (Total 2)
------------------------------------------

Vlan    Mac Address       Type       Ports
----      -----------       ----      -----
1        0026.5a7c.fad3    DYNAMIC    g0/2
1        0000.0000.0004    DYNAMIC    g0/2
```

11.1.5 clear mac address-table

Syntax

To delete the dynamic MAC address, run the following command.

clear mac address-table dynamic [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*]

Parameters

Parameters	Description
mac-addr	MAC address Value range: H.H.H
interface-id	Means a name of a L2 interface.
vlan-id	VLAN ID Value range: 1-4094

Default Value

None

Usage Guidelines

This command is used in EXEC mode.

Example

The following example shows how to clear all dynamically-learned MAC addresses on interface g0/2.

```
Switch# clear mac address-table dynamic interface g0/2
```

Chapter 12 MAC Access List Configuration Commands

12.1 MAC Access List Configuration Commands

The MAC access list configuration commands include:

- mac access-list
- permit
- deny
- mac access-group

12.1.1 mac access-list

Syntax

To add or cancel a MAC access list, run the following command.

[**no**] **mac access-list** *name*

Parameters

Parameters	Description
name	MAC: Name of the MAC access list

Default Value

When there is a rule in the access list, an item- deny any any- will be added to the end by default and the item will not show.

Usage Guidelines

This command is run in global configuration mode.

Example

The following example shows how to configure a mac-acl MAC access list.

```
Switch-config# mac access-list    mac-acl
Switch-config-macl#
```

12.1.2 permit

Syntax

To add or cancel an item to or from the MAC access list, run the following command.

[**no**] **permit** {**any** | **host** *src-mac-addr* | *src-mac-addr src-mac-mask* } {**any** | **host** *dst-mac-addr* | *dst-mac-addr dst-mac-mask*}[**arp** [{*any* | *src-ip-addr*} {*any* | *dst-ip-addr* }] | *ethertype*]

Parameters

Parameters	Description	Value Range
any	Any value	—
host	Chassis	—
src-mac-addr	Stands for source MAC address	H.H.H

Parameters	Description	Value Range
src-mac-mask	Stands for source mac mask	H.H.H
dst-mac-addr	Stands for destination MAC address	H.H.H
dst-mac-mask	Stands for destination mac mask	H.H,H
arp	Stands for matched arp packets	—
src-ip-addr	Stands for source IP address	A.B.C.D
dst-ip-addr	Stands for the destination IP address	A.B.C.D
ethertype	Type of the matched Ethernet packet	0x0600-0xFFFF

Default Value

All items are rejected.

Usage Guidelines

This command is running in MAC access list configuration mode.

Example

The following example shows how to set the MAC address of a host to 1234.5678.abcd.

```
Switch-config-macl#permit host 1234.5678.abcd any
```

12.1.3 deny

Syntax

To add or cancel an item rejected by the MAC access list, run the following command.

[**no**] **deny** {**any** | **host** *src-mac-addr* | *src-mac-addr src-mac-mask* } {**any** | **host** *dst-mac-addr* | *dst-mac-addr dst-mac-mask*}[**arp** [{*any* | *src-ip-addr*} {*any* | *dst-ip-addr* }] | *ethertype*]

Parameters

Parameters	Description	Value Range
any	Any value	—
host	Chassis	—
src-mac-addr	Stands for source MAC address	H.H.H
src-mac-mask	Stands for source mac mask	H.H.H
dst-mac-addr	Stands for destination MAC address	H.H.H
dst-mac-mask	Stands for destination mac mask	H.H,H
arp	Stands for matched arp packets	—
src-ip-addr	Stands for source IP address	A.B.C.D
dst-ip-addr	Stands for the destination IP address	A.B.C.D
ethertype	Type of the matched Ethernet packet	0x0600-0xFFFF

Default Value

All items are rejected.

Usage Guidelines

This command is running in MAC access list configuration mode.

Example

The following example shows how to reject a host whose MAC address is 1234.5678.abcd.

```
Switch-config-macl#deny host 1234.5678.abcd any
```

12.1.4 mac access-group

Syntax

Global：

To apply the established MAC access list to an interface or in the global mode or cancel a MAC access list which is already applied to an interface or in the global mode, run the following command.

mac access-group *name* **[vlan {***word* **| add** *word* **| remove** *word}***]**

[**no**] **mac access-group** *name* **[vlan]**

Port

[**no**] **mac access-group** *name*

Parameters

Parameters	Description
name	MAC: Name of the MAC access list
Vlan	THE ACCESS LIST IS APPLIED IN INGRESS.
Word	VLAN RANGE TABLE
add	ADD VLAN RANGE TABLE
remove	DELETE VLAN RANGE TABLE

Default Value

No MAC access list is applied to an interface.

Usage Guidelines

This command is configured in layer-2 interface configuration mode or the interface configuration mode. If there is no access list, an access list with the empty rule will be created.

Example

The following example shows how to configure the macacl MAC access list on interface g0/1.

```
Switch_config_g0/1#mac access-group macacl
```

Chapter 13 802.1x Configuration Commands

13.1 802.1x Configuration Commands

- 802.1x configuration commands include:
- dot1x enable
- dot1x port-control
- dot1x authentication multiple-hosts
- dot1x authentication multiple-auth
- dot1x default
- dot1x reauth-max
- dot1x re-authentication
- dot1x timeout quiet-period
- dot1x timeout re-authperiod
- dot1x timeout tx-period
- dot1x mab
- dot1x mabformat
- dot1x user-permit
- dot1x authentication method
- dot1x accounting enable
- dot1x accounting method
- dot1x authen-type、dot1x authentication type
- dot1x guest-vlan
- dot1x guest-vlan id
- dot1x forbid multi-network-adapter
- dot1x keepalive
- aaa authentication dot1x
- debug dot1x error
- debug dot1x state
- debug dot1x packet
- show dot1x

13.1.1 dot1x enable

Syntax

dot1x enable

no dot1x enable

Parameters

None

Default Value

None

Usage Guidelines

If the 802.1x function is not enabled, you cannot start it on an interface. If the 802.1x function is forbidden, all interfaces have no the 802.1x function, and at the same time, all 802.1x packets will not be received by CPU but can be forwarded in VLAN like normal multicast packets.

Command Mode

Global configuration mode

Example

The following example shows how to enable dot1x.

```
Switch_config#dot1x enable
Switch_config #
```

13.1.2 dot1x port-control

Syntax

dot1x port-control {**auto**|**force-authorized**|**force-unauthorized**|**misc-mab**}

no dot1x port-control

Parameters

Parameters	Description
auto	Enables the 802.1x authentication mode.
force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.
Misc-mab	The hybrid mode of multi-user and mab authentication

Default Value

force-authorized

Usage Guidelines

The 802.1x protocol is an interface-based two-layer authentication mode. You can run the auto command to enable the authentication mode. This authentication mode can be configured only on the physical interface and the interface's attributes cannot include VLAN backbone, dynamical access, security port or listening port.

Command Mode

Port configuration mode

Example

The following example shows how to enable 802.1x on interface g0/1.

```
Switch_config _g0/1# dot1x port-control auto
Switch_config _g0/1#
The following example shows how to firstly set interface g0/1 to the VLAN backbone and then enable 802.1x.
Switch_config _g0/1#switchport mode trunk
Switch_config _g0/1#dot1x port-control auto
802.1x Control Failed, 802.1x cannot cmd on vlanTrunk port(g0/1)
```

```
Switch_config _g0/1#
```

13.1.3 dot1x authentication multiple-hosts

Syntax

dot1x authentication multiple-hosts

no dot1x authentication multiple-hosts

Parameters

None

Default Value

Disabled

Usage Guidelines

Set one port to the multi-hosts mode of 802.1x, and the switch will authenticate different users. When one user passes the authentication, the port sets to the "up" state. Other users can access the port without authentication.

Note: After modifying the multi-host authentication mode, all users of the port will be authenticated again.

Command Mode

Port configuration mode

Example

The following example shows how to enable multi-hosts authentication on interface g0/1.

```
Switch_config _g0/1# dot1x authentication multiple-hosts
Switch_config _g0/1#
```

13.1.4 dot1x authentication multiple-auth

Syntax

dot1x authentication multiple-auth

no dot1x authentication multiple-auth

Parameters

None

Default Value

Disabled

Usage Guidelines

Set one port to the multi-hosts mode of 802.1x, and the switch will authenticate different users. When only one user passes its authentication, the interface will be up; only when all users fail in their authentication, in another word, only when no successfully authenticated user exist on the interface, the interface will be down. This mechanism gives guarantee to respective authentication for each user and if a user fails in its authentication, other users still have the normal access rights.

NOTE: The multi-auth mode cannot coexist with guest vlan or mab. If an interface is in multi-authen mode, all users on the interface will be authenticated again.

Command Mode

Port configuration mode

Example

The following example shows how to enable multi-auth authentication on interface g0/1.

```
Switch_config _g0/1# dot1x authentication multiple-auth
Switch_config _g0/1#
```

13.1.5 dot1x default

Syntax

dot1x default

Parameters

None

Default Value

None

Usage Guidelines

This command is used to resume all global configurations to the default settings.

Command Mode

Global configuration mode

Example

The following example shows how to resume all dot1x configuration parameters to their default values.

```
Switch_config #dot1x default
Switch_config #
```

13.1.6 dot1x reauth-max

Syntax

dot1x reauth-max *count*

no dot1x reauth-max

Parameters

Parameters	Description
count	Maximum authentication re-try times, ranging between 1 and 10

Default Value

5

Usage Guidelines

This command is used to set the authentication retry times. If the retry times exceeds the maximum retry times and the client has no response, the authentication is mounted.

Command Mode

Global configuration mode

Example

The following example shows how to configure the maximum times of dot1x identity authentication request to 4.

```
Switch_config #dot1x reauth-max 4
Switch_config #
```

13.1.7 dot1x re-authentication

Syntax

dot1x re-authentication

no dot1x re-authentication

Parameters

None

Default Value

None

Usage Guidelines

After an interface passes authentication, the interface will still perform authentication to hosts in a certain period. You can run dot1x timeout re-auth period to configure the period.

Command Mode

Global configuration mode

Example

The following example shows how to enable the re-authentication function.

```
Switch_config #dot1x re-authentication
Switch_config #
```

13.1.8 dot1x timeout quiet-period

Syntax

dot1x timeout quiet-period *time*

no dot1x timeout quiet-period

Parameters

Parameters	Description
time	Period for restarting dot1x authentication, ranging between 0 and 65535 seconds

Default Value

60s

Usage Guidelines

There is a certain period when the switch cannot perform any authentication after the previous authentication fails.

Command Mode

Global configuration mode

Example

The following example shows how to set the value of quiet-period to 40.

```
Switch_config #dot1x timeout quiet-period 40
Switch_config #
```

13.1.9 dot1x timeout re-authperiod

Syntax

dot1x timeout re-authperiod *time*

no dot1x timeout re-authperiod

Parameters

Parameters	Description
time	dot1x re-authentication period, ranging between 1 and 4294967295s

Default Value

3600s

Usage Guidelines

This command validates only when the re-authentication function is enabled.

Command Mode

Global configuration mode

Example

The following example shows how to set the dot1x re-authentication period to 7200 seconds.

```
Switch_config # dot1x timeout re-authperiod 7200
Switch_config #
```

13.1.10 dot1x timeout tx-period

Syntax

dot1x timeout tx-period *time*

no dot1x timeout tx-period

Parameters

Parameters	Description
time	Time which ranges between 1 and 65535 seconds

Default Value

30s

Usage Guidelines

This command is used to set the client's authentication request response interval. If the interval is exceeded, the switch would retransmit the authentication request.

Command Mode

Global configuration mode

Example

The following example shows how to set the transmission frequency to 24.

```
Switch_config # dot1x timeout tx-period 24
Switch_config #
```

13.1.11 dot1x mab

Syntax

dot1x mab

no dot1x mab

Parameters

None

Default Value

The debugging switch is disabled.

Usage Guidelines

When a peer device cannot run the 802.1x client software, the switch will adopt the MAB authentication mode and then the MAC address of the peer device will be sent as both the username and password to the radius server for authentication.

When the MAB authentication is enabled and the peer device, however, neither sends the eapol_start packet nor responds to the request_identity packet and exceeds the timeout threshold, the switch regards this case as the evidence of not support the 802.1x authentication client on the peer device and then turns to the MAB authentication. When the switch sends the gained MAC address as the username and password to the Radius server for authentication, the authentication will still not succeed until the Radius server has authorized this MAC address.

NOTE: The MAB authentication mode cannot coexist with the multi-auth mode.

Command Mode

Port configuration mode

Example

The following example shows how to enable mab authentication on port g0/1.

```
Switch_config _g0/1# dot1x mab
Switch_config _g0/1#
```

13.1.12 dot1x mabformat

Syntax

dot1x mabformat {**1**|**2**|**3**|**4**|**5**|**6**}

no dot1x mabformat

Parameters

Parameters	Description
1	Format of the MAC address: aa:bb:cc:dd:ee:ff
2	Format of the MAC address: aa:bb:cc:dd:ee:ff
3	Format of the MAC address: aabbccddeeff
4	Format of the MAC address: AABBCCDDEEFF
5	Format of the MAC address: aa-bb-cc-dd-ee-ff
6	Format of the MAC address: AA-BB-CC-DD-EE-FF

Default Value

The default is 1.

Usage Guidelines

When the MAB authentication is enabled, you can set the format of the MAC address to the Radius server through this command.

Command Mode

Global configuration mode

Example

The following example shows how to set the format of MAC to 3.

```
Switch_config # dot1x mabformat 3
Switch_config #
```

13.1.13 dot1x user-permit

Syntax

dot1x user-permit xxx yyy zzz

no dot1x user-permit

Parameters

Parameters	Description
xxx	A user name
yyy	A user name
zzz	A user name

Default Value

No user is bound and all users would pass.

Usage Guidelines

This command can be used to bind users on an interface. Each interface can be bound to up to eight users. When the 802.1x authentication is enabled, the authentication is performed only to those bound users. However, to those unbound users, the authentication must fail.

Command Mode

Port configuration mode

Example

The following example shows how to bind users a, b, c and d on interface g0/1.

```
Switch_config _g0/1# dot1x user-permit a b c d
Switch_config _g0/1#
```

13.1.14 dot1x authentication method

Syntax

dot1x authentication method xxx

no dot1x authentication method

Parameters

Parameters	Description
xxx	Method name

Default Value

Default method

Usage Guidelines

This command is used to configure the authentication method which must be one of authentication methods provided by AAA. One interface only uses one authentication method. When AAA performs authentication to the 802.1x user, AAA would select the configured authentication method to perform the authentication.

Command Mode

Port configuration mode

Example

The following example shows how to set the authentication method on interface g0/1 to abcd which applies the local username for authentication and that on interface g0/2 to efgh which applies the remote radius authentication.

```
Switch_config #aaa authentication dot1x abcd local
Switch_config #aaa authentication dot1x efgh group radius
Switch_config #int g0/1
Switch_config _g0/1# dot1x authentication method abcd
Switch_config _g0/1# int g0/2
Switch_config _g0/2# dot1x authentication method efgh
```

13.1.15 dot1x accounting enable

Syntax

dot1x accounting enable

no dot1x accounting enable

Parameters

None

Default Value

The accounting service is disabled by default.

Usage Guidelines

This command is used to enable the accounting function on a port which runs with the authentication function. You'd better enable the dot1x re-authentication function when the accounting function is running.

Command Mode

Port configuration mode

Example

The following example shows how to configure the dot1x authentication function on interface g0/1 and enable the accounting function.

```
Switch_config #dot1x enable
Switch_config #int g0/1
Switch_config _g0/1# dot1x port auto
Switch_config _g0/1# dot1x accounting enable
```

13.1.16 dot1x accounting method

Syntax

dot1x accounting method xxx

no dot1x accounting method

Parameters

Parameters	Description
xxx	Name of the accounting method

Default Value

Default method

Usage Guidelines

This command is used to configure an accounting method on a port. This method must be one of the accounting methods provided by AAA. Each port has only one accounting method. When the dot1x accounting function is enabled, this method will be used for accounting.

Command Mode

Port configuration mode

Example

The following example shows how to set the accounting method on interface g0/1 to abcd, which uses the radius server.

```
Switch_config # aaa accounting network abcd start-stop group radius
Switch_config #radius host 192.168.20.100
Switch_config #int g0/1
Switch_config _g0/1# dot1x accounting method abcd
```

13.1.17 dot1x authen-type, dot1x authentication type

Syntax

To configure the dot1x authentication type in global configuration mode, run dot1x authen-type; to resume the default settings in global configuration mode, run no dot1x authen-type.

dot1x authen-type {**chap**|**eap**}

no dot1x authen-type

To configure the dot1x authentication type on an interface, run dot1x authentication type; to resume the default settings on an interface, run no dot1x authentication type.

dot1x authentication type {**chap**|**eap**}

no dot1x authentication type

Parameters

None

Default Value

The default dot1x authentication type is eap.

The default dot1x authentication type in global configuration mode is also used applied by default in interface configuration mode.

Usage Guidelines

The authentication type decides whether AAA uses the CHAP authentication or the EAP authentication. If the CHAP authentication is used, the challenge required by MD5 is locally generated; if the EAP authentication is used, the challenge is generated on the authentication server. Only one authentication mode can be applied to one interface. By default, the authentication mode is applied in global mode. When an authentication mode is configured for an interface, the authentication mode will be always used on the interface unless the negative form of the command is run to resume the default settings.

Command Mode

Interface or global configuration mode

Example

The following example shows how to set the authentication type on interface g0/1 to chap and the global authentication type to eap.

```
Switch_config #dot1x authen-type eap
Switch_config #int g0/1
Switch_config _g0/1# dot1x authentication type chap
```

13.1.18 dot1x guest-vlan

Syntax

To enable the guest-vlan function of dot1x in global configuration mode, run dot1x guest-vlan. To disable the guest-vlan function of dot1x in global configuration mode, run no dot1x guest-vlan.

dot1x guest-vlan

no dot1x guest-vlan

Parameters

None

Default Value

The debugging switch is disabled.

Usage Guidelines

After the guest-vlan function is enabled, the corresponding port can be grouped into the guest vlan and specific network access rights are attributed to the port if a guest terminal does not respond.

This command is used together with the dot1x guest-vlan id command.

NOTE: This command cannot be set together with the multiple-auth command.

Command Mode

Global configuration mode

Example

The following example shows how to enable the guest-vlan function in global configuration mode.

```
Switch_config #dot1x guest-vlan
```

13.1.19 dot1x guest-vlan id

Syntax

To configure the value of dot1x guest-vlan id on an interface, run dot1x guest-vlan id; to resume the default value 0, run no dot1x guest-vlan.

dot1x guest-vlan id

no dot1x guest-vlan

Parameters

ID: stands for the value of guest vlan,which can be any vlan ID configured in the system.

Default Value

None

Usage Guidelines

After the guest-vlan function is enabled, the corresponding port can be grouped into the guest vlan and specific network access rights are attributed to the port if a guest terminal does not respond.

This command is used together with the dot1x guest-vlan id command.

Note: This command cannot be set together with the multiple-auth command.

Command Mode

Port configuration mode

Example

The following example shows how to configure the guest-vlan id on port g0/1.

```
Switch_config _g0/1#dot1x guest-vlan 2
```

13.1.20 dot1x forbid multi-network-adapter

Syntax

To forbid the supplicant of the multi-network-adapter on an interface, run dot1x forbid multi-network-adapter. To resume the default settings, run no dot1x forbid multi-network-adapter.

dot1x forbid multi-network-adapter

no dot1x forbid multi-network-adapter

Parameters

None

Default Value

None

Usage Guidelines

This command can be used to forbid the supplicant terminal with multiple network adapters, preventing an agent from being occurred.

Command Mode

Port configuration mode

Example

The following example shows how to forbid the supplicant terminal with multiple network adapters on port g0/1.

```
Switch_config _g0/1 # dot1x forbid multi-network-adapter
```

13.1.21 dot1x keepalive

Syntax

The following example shows how to enable or disable the keepalive detection for the authentication user.

dot1x keepalive

no dot1x keepalive

Parameters

None

Default Value

Enabled

Usage Guidelines

The default is enable the keepalive detection.

Command Mode

Global configuration mode

Example

The following example shows how to enable/disable the keepalive detection for the authentication user, run the above commands.

```
Switch_config #no dot1x keepalive
Switch_config #
```

13.1.22 aaa authentication dot1x

Syntax

aaa authentication dot1x {*default* **|** *word* } *method1* [*method2*...]

no aaa authentication dot1x { *default* **|** *word}*

Parameters

Parameters	Description
default	Default method Uses the authentication method when command dot1x authentication method does not run.
word	Designate the name of the authentication method
method1 [method2...]	group radius, local, local-case, none

Default Value

None

Usage Guidelines

The method parameter provides a series of methods to authenticate the password of the client host. You'd better adopt the radius as the AAA authentication mode of 802.1x. You can also use the local configuration data for authentication, such as user password saved in the local configuration.

Command Mode

Global configuration mode

Example

The following example shows how to configure the dot1x authentication method to RADIUS.

```
Switch_config #aaa authentication dot1x default group radius
Switch_config #
```

13.1.23 debug dot1x errors

Syntax

debug dot1x errors

Parameters

None

Default Value

None

Usage Guidelines

This command is used to export all error information occurred during dot1x running. The error information can help locating the errors.

13.1.24 debug dot1x state

Syntax

debug dot1x state

Parameters

None

Default Value

None

Usage Guidelines

The following shows the format of information output:

```
2003-3-18 17:40:09 802.1x:AuthSM(G0/1) state Connecting-> Authenticating, event rxRespId
2003-3-18 17:40:09 802.1x:G0/1 Create user for Enter authentication
2003-3-18 17:40:09 802.1x:BauthSM(G0/1) state Idle-> Response, event authStart
2003-3-18 17:40:09 802.1x:G0/1 user "myname" denied, Authentication Force Failed
2003-3-18 17:40:09 802.1x:G0/1 Authentication Fail
2003-3-18 17:40:09 802.1x:BauthSM(G0/1) state Response-> Fail, event aFail
```

13.1.25 debug dot1x packet

Syntax

debug dot1x packet

Parameters

None

Default Value

None

Usage Guidelines

```
2003-3-18 17:40:09 802.1xG0/1 Tx --> Supplicant(0008.74bb.d21f)
EAPOL   ver:01, type:00, len:5
EAP     code:01, id:03, type:01, len:5
00
2003-3-18 17:40:09 802.1x:G0/1 Rx <-- Supplicant(0008.74bb.d21f)
EAPOL   ver:01, type:00, len:10
EAP     code:02, id:03, type:01, len:10
62 64 63 6f 6d a5
```

13.1.26 show dot1x

Syntax

To display the 802.1x configuration information, run the following command.

show dot1x [*interface intf-id* | *statistics*|*misc-mab-db*]

Parameters

Parameters	Description
interface	Displays dot1x interface information.
Intf-id	Stands for a specific physical interface.
statistics	Displays dot1x statistics information.
misc-mab-db	Displays dot1x hybrid Mab database

Default Value

None

Usage Guidelines

This command is used to display the 802.1x configuration information.

Command Mode

EXEC mode or configuration mode

Example

The following example shows how to display 802.1x configuration information.

```
Switch_config#show dot1x
802.1X Parameters
reAuthen         No
reAuth-Period    3
quiet-Period     10
Tx-Period        30
Supp-timeout     30
Server-timeout   30
reAuth-max       4
max-request      2
authen-type      Eap
IEEE 802.1x on port G0/1 enabled
Authorized                Yes
Authen Type               Eap
Authen Method             default
Permit Users              All Users
Multiple Hosts            Disallowed
Supplicant                aaa(0008.74bb.d21f)
Current Identifier        21
Authenticator State Machine
State                     Authenticated
Reauth Count              0
Backend State Machine
State                     Idle
Request Count             0
Identifier (Server)       20
Port Timer Machine
Auth Tx While Time        16
Backend While Time        16
reAuth Wait Time          3
Hold Wait Time            0
```

Chapter 14 VLAN Configuration Commands

14. 1 VLAN Configuration Commands

The VLAN configuration commands include:

- vlan
- name
- dot1q-tunnel
- switchport pvid
- switchport mode
- switchport trunk
- show vlan
- show interface vlan

14.1.1 vlan

Syntax

[**no**] **vlan** *vlan-id*

To add a VLAN, run vlan vlan-id. To delete a VLAN, run [no] vlan vlan-id.

Parameters

Parameters	Description
vlan-id	Defines the ID of the VLAN. Value range: 1-4094.

Default Value

The default value is 1.

Command Mode

Global configuration mode

Usage Guidelines

After this command is run, the system enters the VLAN configuration mode and then you can modify some VLAN attributes.

Example

The following example shows how to add the VLAN whose ID is 2:

```
Switch_config#
Switch_config#vlan 2
Switch_config_vlan2#exit
```

14.1.2 name

Syntax

To name a VLAN, run name str.

[**no**] **name** *str*

Parameters

Parameters	Description
str	Defines the name of the VLAN. Value range: 1-32 characters.

Default Value

The default VLAN name is 'Default'. Other VLAN's name is VLANxxxx (xxxx is 4-digit stack ID)

Command Mode

VLAN configuration mode

Usage Guidelines

This command can be used to modify the VLAN name to symbolize a specific VLAN.

Example

The following example shows how to set the name of VLAN200 to main405:

```
Switch_config#
Switch_config#
Switch_config#vlan 200
Switch_config_vlan200#name ?
  WORD   The ascii name of VLAN(32bytes)
Switch_config_vlan200#name main405
```

14.1.3 dot1q-tunnel

Syntax

dot1q-tunnel

no dot1q-tunnel

To enable or disable the Dot1q tunnel globally, run the following commands.

Parameters

None

Default Value

Dot1q Tunnel is not enabled globally.

Command Mode

Global configuration mode

Usage Guidelines

After Qot1Q Tunnel is globally enabled, all ports serve as the downlink ports of Qot1Q Tunnel by default and put the SPVLAN tag on the incoming packets.

Example

The following example shows how to enable Dot1q tunnel in the global configuration mode.

```
Switch_config#dot1q-tunnel
```

14.1.4 switchport pvid

Syntax

To configure VLAN of the access-mode port, run switchport pvid vlan-id.

switchport pvid *vlan-id*

no switchport pvid

Parameters

Parameters	Description
vlan-id	VLAN ID which the port belongs to, ranging between 1 and 4049 Value range: 1-4094

Default Value

All ports belong to VLAN 1.

Command Mode

Port configuration mode

Usage Guidelines

If vlan which pvid belongs does not exist before the command, it will be created with the creation of pvid. The port can be configured in the access mode or the relay mode.

Example

The following example shows how to set port GigaEthernet 0/1 to the access port of VLAN10:

```
Switch_config#interface g0/1
Switch_config_g0/1#switchport pvid 10
```

14.1.5 switchport mode

Syntax

switchport mode {access | trunk | dot1q-tunnel-uplink | dot1q-translating-tunnel

no switchport mode

To configure the mode of the port, run the following command.

Parameters

Parameters	Description
access	Access mode

trunk	Relay mode
dot1q-tunnel-uplink	VLAN tunnel uplink mode
dot1q-translating-tunnel	VLAN translating tunnel mode

Default Value

Access mode

Command Mode

Port configuration mode

Usage Guidelines

The switch's port supports the following modes: the access mode, the relay mode, the VLAN tunnel mode, the VLAN translating tunnel mode and the VLAN tunnel uplink mode.

The access mode indicates that the port belongs to just one VLAN; only the untagged Ethernet frame can be transmitted and received.

The relay mode indicates that the port connects other switches and the tagged Ethernet frame can be transmitted and received.

The VLAN translating tunnel mode is a sub mode based on the relay mode. The port looks up the VLAN translation table according to the VLAN tag of received packets to obtain corresponding SPVLAN, and then the switching chip replaces the original tag with SPVLAN or adds the SPVLAN tag to the outside layer of the original tag. When the packets is forwarded out of the port, the SPVLAN will be replaced by the original tag or the SPVLAN tag will be removed mandatorily. Hence, the switch omits different VLAN partitions that access the network, and then passes them without change to the other subnet that connects the other port of the same client, realizing transparent transmission.

The VLAN tunnel uplink mode is a sub mode based on the relay mode. The SPVLAN should be set when packets are forwarded out of the port. When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag. When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag.

The port mode collides with the 802.1X protocol. The 802.1X protocol cannot be configured in relay mode (including the VLAN translating tunnel mode and the VLAN tunnel uplink mode); the port on which the 802.1X protocol is configured cannot be set to the relay mode. That is to say, the 802.1X protocol can be effective only on the access-mode port (including the VLAN tunnel mode).

The 802.1X standard does not support authentication on the trunk port. The reason is that the authentication object regulated in the standard is not the port. As to port multiplexing, if user authentication is approved in one VLAN, all other VLAN users who multiplex this port are also authorized correspondingly, therefore, the trunk port does not support authentication.

Example

The following example shows how to configure the port to VLAN tunnel uplink port mode.

```
Switch_config_g0/1#switchport mode dot1q-tunnel-uplink
```

14.1.6 switchport trunk

Syntax

To configure the attributes of the relay port, run the following command.

[**no**] **switchport trunk** {**vlan-allowed** *vlan-list*} | {**vlan-untagged** *vlan-list*} }

Parameters

Parameters	Description
vlan-allowed	VLAN ID which can be received and transmitted by the port Value Range: 1-4094
vlan-untagged	Frame that will be transmitted without adding the VLAN tag Value

	Range: 1-4094

Default Value

The native VLAN ID of all relay ports is 1. The allowable value for all VLANs ranges between 1 and 4094.

Command Mode

Port configuration mode

Usage Guidelines

No matter the port is in access mode or in relay mode, you can run this command on the port. However, the port is in relay mode when this command functions.

The vlan-allowed parameter is used to control the VLAN range of the port; the vlan-untagged parameter is used to decide which packets need be added with the VLAN tag when a port transmits these packets.

When the vlan list is used, you can add, remove or set (none, all, except) the lists of the existing VLAN. The entered lists are separated by the comma or the hyphen. For example, "1, 3, 5, 7" stands for "vlan 1, vlan 3, vlan 5, vlan 7", while "1, 3-5, 7" stands for "vlan 1, vlan 3, vlan 4, vlan -5, vlan 7".

Example

The following example shows how to set the allowable VLAN range to 1-10, and the untagged VLAN range to 2-1000.

```
Switch_config_g0/1#switchport trunk vlan-allowed 1-10
Switch_config_g0/1#switchport trunk vlan-untagged 2-1000
```

14.1.7 show vlan

Syntax

To display relative information about all VLANs, run the following command.

show vlan [id *vlan-id* **| interface** *intf-id* **| dot1q-tunnel [interface** *intf***] |mac-vlan | subnet | protocol-vlan |dot1q-translating-tunnel|flat-translation-table]**

Parameters

Parameters	Description
Id *vlan-id*	Displays the designated VLAN. Value range: 1-4094
Interface *Intf-id*	Displays the designated port.
dot1q-tunnel [interface *intf*]	Displays the global information and statistics information about Dot1Q tunnel, or displays the detailed information about Dot1Q tunnel of the designated port.
mac-vlan	Displays the configured MAC VLAN entries.
subnet	Displays the configured IP-subnet VLAN entries.
protocol-vlan	Displays the configured protocol VLAN template or entry.
dot1q-translating-tunnel	Displays the port vlan tunnel translation information
flat-translation-table	Checks the configured items of flat translation

Default Value

None

Command Mode

Global configuration mode, port configuration and EXEC configuration mode

Usage Guidelines

None

Example

The following example shows how to display relative information about all VLANs.

```
Switch#show vlan
VLAN Status   Name           Ports
---- -------- ---------------- ------------------------------------------------------
1    Static   Default        g0/1, g0/2, g0/4……
2    Static   VLAN0002       g0/3
3    Static   VLAN0003       g0/3
4    Static   VLAN0004       g0/3
5    Static   VLAN0005       g0/3
```

The status parameter stands for the VLAN generation source; the static parameter means that VLAN is generated through configuration; the dynamic parameter means that VLAN is generated dynamically through the GVRP protocol.

The following example shows the detailed information about a VLAN:

```
Switch#show vlan id 1
VLAN id: 1, Name: default, TotalPorts:11


Ports           Atttributes
------------------------------------------------------------------
g0/1            Trunk,Untagged
g0/2            Access
```

The following example shows relative information about a VLAN on a port:

```
Switch#show vlan int g0/6


Interface          VLAN
Name               Property PVID Vlan-Map        uTagg-VLan-Map
------------------- -------- ---- ---------------- ----------------
GigaEthernet0/2     Trunk    1    3,5,7,9,11,13,15 none
                             17,19
Switch#show vlan int g0/7


Interface          VLAN
Name               Property PVID Vlan-Map        uTagg-VLan-Map
GigaEthernet 0/3      Access   7    7             ----
```

14.1.8 show interface vlan

Syntax

To display relative information about the VLAN interface, run the following command.

show interface vlan *intf-id*

Parameters

Parameters	Notes:	Value Range
Intf-id	Displays the designated port.	1-4094

Default Value

None

Command Mode

Global configuration mode, port configuration and EXEC configuration mode

Usage Guidelines

None

Example

The following example shows how to display the information about interface VLAN 1.

```
Switch#show int vlan 1
VLAN1 is up, line protocol is up
  Hardware is EtherSVI, Address is 00e0.0f42.0071(00e0.0f42.0071)
  MTU 1500 bytes, BW 1000000 kbit, DLY 2000 usec
  Encapsulation ARPA, loopback not set
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 multicasts
     0 input errors,, 0 input discards
     0 packets output, 0 bytes, 0 underruns
     Transmited 0 broadcasts, 0 multicasts
     0 output errors, 0 discards
  ARP type: ARPA, ARP timeout 04:00:00
```

The statistics values are explained as follows:

Packets input means the input of all packets, including broadcast packets, multicast packets and unicast packets.

Bytes means the byte volume of all packets.

Broadcasts means received broadcast packets.

Broadcasts means received broadcast packets.

Input errors means received error packets.

Input discards means that the received packets are dropped, such as the received packets when the interface protocol is down.

Packets output means the output of all packets, including broadcast packets, multicast packets and unicast packets.

Bytes means the byte volume of all transmitted packets.

Broadcasts means transmitted broadcast packets.

Multicasts means transmitted multicast packets.

Output errors means transmitting error packets.

Output discards means that the transmitted packets are dropped, such as the transmitted packets when the interface protocol is down.

Chapter 15 GVRP Configuration Commands

15.1 GVRP Configuration Commands

15.1.1 gvrp

Syntax

To enable or disable GVRP, run gvrp. To resume the default value, run no gvrp.
gvrp
no gvrp

Parameters

None

Default Value

The global GVRP is shut down, while GVRP on ports is enabled.

Usage Guidelines

GVRP can be enabled globally or on a port. Hence, GVRP can be really enabled only after GVRP is enabled both globally and on ports.

Example

The following example shows how to enable GVRP globally.
```
Switch_config#gvrp
Switch_config#
```
The following example shows how to enable GVRP on port 1.
```
Switch_config_g0/1#gvrp
Switch_config_g0/1#
```

15.1.2 gvrp dynamic-vlan-pruning

Syntax

To set the dynamic vlan to be effective on a registered port, run gvrp dynamic-vlan-pruning; to return to the default setting, use the “no” form of this command.
gvrp dynamic-vlan-pruning
no gvrp dynamic-vlan-pruning

Parameters

None

Default Value

dynamic-vlan-pruning is disabled by default, that is, dynamic VLAN can take effect on all ports.

Command Mode

Global configuration mode

Usage Guidelines

After this command is enabled and if a port has not registered a dynamic VLAN, this port will not belong to the dynamic VLAN even though this port is a trunk port and it allows the dynamic VLAN to pass through.

Example

The following example shows how to make dynamic VLAN validate on its registered port.

```
Switch_config#gvrp dynamic-vlan-pruning
Switch_config#
```

15.1.3 show gvrp statistics

Syntax

To display the GVRP statistics information, run this command.

show gvrp statistics [interface *intf-id*]

Parameters

Parameters	Description
Intf-id	Stands for a specific physical interface.

Default Value

None

Usage Guidelines

This command is used to display the GVRP statistics information.

Example

The following example shows how to display the GVRP statistics information about interface g0/1.

```
Switch_config#show gvrp statistics interface g0/1
GVRP statistics on port g0/1
        GVRP Status                 : Enabled
        GVRP Frames Received        : 0
        GVRP Frames Transmitted     : 20
        GVRP Frames Discarded       : 0
        GVRP Last Pdu Origin        : 0000.0000.0000
```

15.1.4 show gvrp status

Syntax

To display the GVRP state information, run this command.
show gvrp status

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the GVRP state information.

Example

The following example shows how to display the GVRP state information about a switch.

```
Switch_config#show gvrp status
 GVRP is enabled
```

15.1.5 debug gvrp event

Syntax

To enable the information output of GVRP debugging, run debug gvrp event. To shut down the information output of GVRP debugging, run no debug GVRP event.
debug gvrp event
no debug gvrp event

Parameters

None

Default Value

None

Usage Guidelines

To enable the information output of GVRP debugging, run debug gvrp event. To shut down the information output of GVRP debugging, run no debug GVRP event.

Example

```
Switch# debug gvrp event
Switch#
```

15.1.6 debug gvrp packet

Syntax

To enable or disable GVRP displaying, run this command.

debug gvrp packet
no debug gvrp packet

Parameters

None

Default Value

None

Usage Guidelines

To enable or disable GVRP displaying, run this command.

Example

```
switch# debug gvrp packet
switch#
```

15.2 GARPC onfiguration Commands

GARP is the basic module of GVRP/CMRP. It schedules GVRP/GMRP running and provides services to GVRP/GMRP.

15.2.1 garp timer leaveall

Syntax

To configure the garp leaveall timer, run garp timer leaveall time_value. To resume the corresponding default value, run no garp timer leaveall.
garp timer leaveall *time_value*
no garp timer leaveall

Parameters

Parameters	Description
timer_value	Stands for the global leave all timer value. Value range: 10~ 32765 centiseconds.

Default Value

1000 centiseconds

Usage Guidelines

After the leave all timer times out, the bridge cancels all registered VLAN information and transmits Leave All Message to the outside.

Example

The following example configures leaveall timer on the switch to 1200 centiseconds.

```
Switch_config# garp timer leaveall 1200
Switch_config#
```

15.2.2 garp timer hold

Syntax

To configure the garp hold timer, run garp timer hold time_value. To return to the default setting, run no garp timer hold.
garp timer hold *time_value*
no garp timer hold

Parameters

Parameters	Description
timer_value	hold timer value of the port Value range: 10~ 32765 centiseconds.

Default Value

10 centiseconds

Command Mode

Port configuration mode

Usage Guidelines

None

Example

The following example shows how to configure garp hold timer on the switch to 15 centiseconds.

```
Switch_config_g0/1#garp timer hold 15
Switch_config_g0/1#
```

15.2.3 garp timer join

Syntax

To configure the garp join timer, run garp timer join time_value. To return to the default setting, run no garp timer join.
garp timer join *time_value*
no garp timer join

Parameters

Parameters	Description
timer_value	join timer value of the port Value range: 10~ 32765 centiseconds.

Default Value

20 centiseconds

Command Mode

Port configuration mode

Usage Guidelines

None

Example

The following example shows how to configure garp join timer of the port g0/1 on the switch to 25 centiseconds.

```
Switch_config_g0/1#garp timer join 25
Switch_config_g0/1#
```

15.2.4 garp timer leave

Syntax

To configure the garp leave timer, run garp timer leave time_value. To return to the default setting, run no garp timer leave.
garp timer leave *time_value*
no garp timer leave

Parameters

Parameters	Description
timer_value	leave timer value of the port Value range: 10~ 32765 centiseconds.

Default Value

60 centiseconds

Command Mode

Port configuration mode

Usage Guidelines

None

Example

The following example shows how to configure garp leave timer of the port g0/1 on the switch to 80 centiseconds.

```
Switch_config_g0/1#garp timer leave 80
Switch_config_g0/1#
```

15.2.5 show garp timers

Syntax

To display theGARP-configured clock information, run the following command.
show garp timers [interface *intf_id*]

Parameters

Parameters	Description
Intf-id	Stands for a specific physical interface.

Default Value

None

Usage Guidelines

This command is used to display theGARP-configured clock information, including the global leaveall timer value, the hold/join/leave timer value on the port.

Example

The following example shows how to display the timer information on interface G0/1.

```
Switch# show garp timers interface g0/1
 GARP   timers on port 1(G0/1)
          Garp Join Time              : 20 centiseconds
          Garp Leave Time             : 60 centiseconds
          Garp LeaveAll Time          : 1000 centiseconds
          Garp Hold Time              : 10 centiseconds
```

15.2.6 show garp status

Syntax

To display the current GARP application instance by default, run the following command.
show garp status

Parameters

None

Default Value

None

Usage Guidelines

To display the current GARP application instance by default, run the following command.

Example

The following example shows the running GARP application instances.

```
Switch_config#show garp status
No   GARP   application is running.
```

15.2.7 debug garp

Syntax

To enable or disable the debug information about the GARP event or timer, run this command.

debug garp { event | timer }
no debug garp { event | timer }

Parameters

Parameters	Description
event	event debug
timer	timer debug

Default Value

None

Usage Guidelines

To enable or disable the debug information about the GARP event or timer, run this command.

Example

The following example shows how to enable GARP event debug information.

```
Switch# debug garp event
Switch#
```

Chapter 16. Private VLAN Configuration Commands

16. 1 Private VLAN configuration commands

The private VLAN configuration commands are:

- private-vlan
- private-vlan association
- switchport mode private-vlan
- switchport private-vlan host-association
- switchport private-vlan mapping
- switchport private-vlan
- show vlan private-vlan
- show vlan private-vlan interface

16.1.1 private-vlan

private-vlan {primary|community|isolated}

Configure VLAN Private VLAN Properties

parameter

parameter	Description
primary	Set VLAN to Primary VLAN
community	Set VLAN as public VLAN
isolated	Set VLAN to isolated VLAN

Default Value

No private VLAN type is configured

Command Mode

VLAN configuration mode

Usage Guidelines

Primary VLAN (Primary VLAN): For a VLAN associated with a promiscuous port, there can be only one Primary VLAN in the Private VLAN, and each port in the Primary VLAN is a member of the Primary VLAN.

Isolated VLAN: Ports in the same isolated VLAN cannot communicate with each other at Layer 2. There is only one isolated VLAN in a private VLAN domain. An isolated vlan must be associated with a primary VLAN. There can be only one isolate VLAN in a private VLAN.

Community VLAN: Ports in the same shared VLAN can communicate with each other at Layer 2 but cannot communicate with ports in other shared VLANs at Layer 2. There can be multiple shared VLANs in a private VLAN domain. A public VLAN must be associated with a primary VLAN.

Example

The following command configures VLAN 2 as the primary VLAN

```
Switch_config#
Switch_config#vlan 2
```

```
Switch_config_vlan2#private-vlan primary
```

16.1.2 private-vlan association

private-vlan association {*svlist* | **add** *svlist* | **remove** *svlist*}

no private-vlan association

Configuring Association for Private VLANs

Parameters

Parameters	Description
svlist	Configure the Secondary VLAN to be associated

Default Value

No secondary VLANs are associated

Command Mode

VLAN configuration mode

Usage Guidelines

This command is used to associate the primary VLAN and the secondary VLAN so that they can implement shared VLAN learning in the entire private VLAN domain. This command can only be performed in the configuration mode of the primary VLAN.

When using svlist, you can add or remove the list of existing auxiliary VLANs (add, remove). The input svlist is separated by ',' and '-'. For example, '1, 3, 5, 7' means vlan 1, vlan 3, vlan 5, vlan7; '1, 3-5, 7' means vlan 1, vlan 3. vlan4, vlan 5, vlan7.

Note that for the entire private VLAN domain to take effect, the attributes of each private VLAN in each domain must be configured correctly and have private VLAN attributes.

Example

The following command will establish an association between Primary VLAN 2 and Community VLAN 3,4

```
Switch_config#
Switch_config#vlan 2
Switch_config_vlan2#private-vlan association 3-4
```

16.1.3 switchport mode private-vlan

switchport mode private-vlan {*host* | *promiscuous*}

Configure the mode of a Layer 2 interface in a private VLAN

Parameters

Parameters	Description
host	Configure the Layer 2 interface to host port mode
promiscuous	Configure a Layer 2 interface in promiscuous port mode

Default Value

Configure a Layer 2 interface in promiscuous port mode

Command Mode

Port configuration mode

Usage Guidelines

This command is mainly used to configure the mode of the Layer 2 interface in the private VLAN, mixed port mode and host port mode. The host port mode is divided into public port and isolated port.

Promiscuous Port: A port that belongs to the primary VLAN. Can communicate with all ports, including isolated and shared ports for secondary VLANs in the same private VLAN domain.

Isolated Port: Host port in an isolated VLAN. In the same private VLAN domain, except for promiscuous ports, isolated ports are completely separated from all other ports at Layer 2. Traffic received from isolated ports can only be forwarded to promiscuous ports.

Community Port: belongs to the host port in the shared VLAN. In a private VLAN domain, shared ports of the same shared VLAN can communicate with each other at Layer 2 or with mixed ports, and cannot communicate with shared ports in other shared VLANs and isolated ports in isolated VLANs communication.

Example

The following command configures interface g0 / 1 in promiscuous port mode.

```
Switch_config#
Switch_config#interface g0/1
Switch_config_g0/1#switchport mode private-vlan promiscuous
```

16.1.4 switchport private-vlan host-association

switchport private-vlan host-association p_vid s_vid

Configure a private VLAN associated with a Layer 2 host port

Parameters

Parameters	Description
p_vid	Configure the VLAN ID of the primary VLAN to be associated, in the range of 1-4094
s_vid	Configure the VLAN_ID of the Secondary VLAN to be associated, in the range of 1-4094

Default Value

No associated private VLANs configured

Command Mode

Port configuration mode

Usage Guidelines

This command is mainly used to configure the Layer 2 host interface to associate the primary VLAN and the secondary VLAN. Note that for this host port to take effect in the associated primary VLAN and secondary VLAN, you need to configure the port as a host port and The private VLAN type of the VLAN is configured correctly, and the association relationship between the two VLANs is configured correctly.

Example

Host association port g0 / 1 with primary VLAN 2 and secondary VLAN 3

```
Switch#config
Switch_config#interface g0/1
Switch_config_g0/1#switchport private-vlan host-association 2 3
```

16.1.5 switchport private-vlan mapping

switchport private-vlan mapping

p_vid{svlist | add svlist | remove svlist}

Configure private VLANs associated with Layer 2 promiscuous ports

Parameters

Parameters	Description
p_vid	Configure the VLAN ID of the primary VLAN to be associated, in the range of 1-4094
svlist	Configure the Secondary VLAN to be associated

Default Value

No associated private VLANs configured

Command Mode

Port configuration mode

Usage Guidelines

This command is mainly used to configure the Layer 2 promiscuous interface to associate the primary VLAN and the auxiliary VLAN. Note that for this promiscuous port to take effect in the associated primary and auxiliary VLANs, you need to configure the port as a promiscuous port and the associated VLAN Private VLAN The private VLAN type of the configuration command is configured correctly, and the association relationship of these private VLANs is configured correctly.

When using svlist, the list of auxiliary VLANs associated with this port can be added and removed (add, remove). The input svlist is separated by ',' and '-'. For example, '1, 3, 5, 7' means vlan 1, vlan 3, vlan 5, vlan7; '1, 3-5, 7' means vlan 1, vlan 3. vlan4, vlan 5, vlan7.

Example

Promiscuously associate port g0 / 1 with primary VLAN 2 and secondary VLANs 3-5

```
Switch#config
Switch_config#interface g0/1
Switch_config_g0/1#switchport private-vlan mapping 2 3-5
```

16.1.6 switchport private-vlan

switchport private-vlan { tag-pvid *p_vid* **| tag-pri** *priority* **| untagged }**

no switchport private-vlan untagged

Configure the tag and related fields in the tag of the outbound packet of the Layer 2 interface in the private VLAN

Parameters

Parameters	Description
p_vid	Configure the VLAN ID in the tag, in the range of 1-4094
priority	Configure the priority field in the tag, ranging from 0-7
untagged	Configure whether outgoing packets are tagged

Default Value

The VLAN ID in the tag defaults to 1.

The priority is 0 by default.

The egress port does not have tags by default.

Command mode

Port configuration mode

Usage Guidelines

This command is mainly used to configure the tag attribute and whether to tag the outbound packet in the private VLAN. The condition for these configuration commands to take effect is that the type of the private VLAN is configured correctly and the association relationship of the private VLANs in the private VLAN domain is configured correctly The mode of the Layer 2 interface in the private VLAN is configured correctly, and the association between the Layer 2 interface and the private VLAN is configured correctly, otherwise it will not take effect.

16.1.7 show vlan private-vlan

show vlan private-vlan

It is mainly used to display the configuration information of VLANs and Layer 2 interfaces in private VLANs.

Parameters

None

Default Value

None

Command Mode

Port configuration mode, VLAN configuration mode, management mode

Usage Guidelines

This command mainly displays the configuration information of the VLAN and the Layer 2 interface in the private VLAN.

Example

Display private VLAN configuration information

```
Switch_config#
Switch_config#show vlan private-vlan
Primary       Secondary        Type             Ports
------------  ---------------  ---------------  ------------------------------------------
2             3                community        G0/1, G0/2, G0/3
2             4                isolated         G0/1, G0/4
2             5                community        G0/1, G0/5
```

16.1.8 show vlan private-vlan interface

show vlan private-vlan interface *interface*

Mainly used to display the configuration information of the Layer 2 interface in the private VLAN

Parameters

Parameters	Description
Interface	The interface to display

Default Value

None

Command Mode

Port configuration mode, VLAN configuration mode, management mode

Usage Guidelines

This command mainly displays the configuration information of the Layer 2 interface in the private VLAN.

Example

Display Layer 2 interface g0 / 1 configuration information in a private VLAN

```
Switch_config#
Switch_config#show vlan private-vlan interface g0/1
port type: promiscuous port
private-vlan host-association: primary vlan 2 secondary vlan 3
private-vlan mapping: primary vlan 2 secondary vlan 3-5
Native VLAN tagging enable: untagged
Native VLAN tagging priority 0
Native VLAN tagging pvid: 1
```

Chapter 17 STP Configuration Commands

17.1 SSTP Configuration Commands

17.1.1 spanning-tree

Syntax

To enable the default STP mode, run spanning-tree; to disable the STP, run no spanning-tree.

Enable or disable STP in interface configuration mode.

spanning-tree

no spanning-tree

Parameters

None

Default Value

RSTP is enabled by default.

Usage Guidelines

None

Command Mode

Global configuration mode

Physical interface configuration mode or aggregation port configuration mode

Example

None

17.1.2 spanning-tree mode sstp

Syntax

To configure the spanning-tree operation mode, run spanning-tree mode sstp. To return to the default setting, use the no form of this command.

spanning-tree mode sstp

no spanning-tree mode

Parameters

None

Default Value

The default STP mode is RSTP.

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to enable the SSTP mode.

```
Switch_config# spanning-tree mode sstp
Switch_config#
```

17.1.3 spanning-tree sstp priority

Syntax

To configure the SSTP priority value, run spanning-tree sstp priority value. To resume the default value of the SSTP priority value, run no spanning-tree sstp priority.

spanning-tree sstp priority *value*

no spanning-tree sstp priority

Parameters

Parameters	Description
value	Priority value Value range: 0-61440

Default Value

32768

Usage Guidelines

When setting the priority value, you can make the switch as the root of the whole network spanning tree. The configuration value takes 4096 as a step and its value is the multiple of 4096. The configurable values are 0, 4096, 8192, 3*4096, 4*4096,…… and 15*4096.

Command Mode

Global configuration mode

Example

The following example shows how to set the priority level of SSTP to 4096.

```
Switch_config# spanning-tree sstp priority 4096
Switch_config#
```

17.1.4 spanning-tree sstp hello-time

Syntax

To configure the transmission interval of SSTP packets, run spanning-tree sstp hello-time time. To resume the default transmission interval, run no spanning-tree sstp hello-time.

spanning-tree sstp hello-time *time*

no spanning-tree sstp hello-time

Parameters

Parameters	Description
time	Updates the interval. Range: 1-10 seconds

Default Value

2s

Usage Guidelines

The Hello-Time configured on the local switch validates only when the local switch runs as a root switch.

Command Mode

Global configuration mode

Example

The following example shows how to configure the transmission interval of BPDU of SSTP to 8 seconds.

```
Switch_config# spanning-tree sstp hello-time 8
Switch_config#
```

17.1.5 spanning-tree sstp max-age

Syntax

To configure the maximum lifespan of the SSTP BPDU, run spanning-tree sstp max-age time. To resume the default interval time, run no spanning-tree sstp max-age.

spanning-tree sstp max-age *time*

no spanning-tree sstp max-age

Parameters

Parameters	Description
seconds	Means the maximum lifespan of BPDU. Range: 6-40 seconds

Default Value

20s

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to configure the maximum lifespan of SSTP to 24 seconds.

```
Switch_config# spanning-tree sstp max-age 24
Switch_config#
```

17.1.6 spanning-tree sstp forward-time

Syntax

To configure the forwarding delay, run spanning-tree sstp forward-time time. To resume the default forwarding delay, run no spanning-tree sstp forward-time.

spanning-tree sstp forward-time *time*

no spanning-tree sstp forward-time

Parameters

Parameters	Description
time	Time of the forwarding delay Value range: 4-30 seconds

Default Value

15 seconds

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to configure the forwarding delay of SSTP to 20 seconds.

```
Switch_config# spanning-tree sstp forward-time 20
Switch_config#
```

17.1.7 spanning-tree sstp cost

Syntax

To configure the path cost of a port in SSTP mode, run spanning-tree sstp cost value. To resume the default path cost, run no spanning-tree sstp cost.

spanning-tree sstp cost *value*

no spanning-tree sstp cost

Parameters

Parameters	Description
value	Value of the path cost Value range: 1-200000000

Default Value

The value of the path cost of the 10M Ethernet is 100.

The value of the path cost of the 100M Ethernet is 19.

The value of the path cost of the 1000M Ethernet is 1.

Usage Guidelines

None

Command Mode

Port configuration mode

Example

The following example shows how to set the path cost of port G0/1 to 100 in SSTP mode.

```
Switch_config_g0/1#spanning-tree sstp cost 100
Switch_config_g0/1#
```

17.1.8 spanning-tree cost

Syntax

To configure the path cost of a port in all STP mode, run spanning-tree cost value. To resume the default path cost, run no spanning-tree cost.

spanning-tree cost *value*

no spanning-tree cost

Parameters

Parameters	Description
value	Value of the path cost of a port Value range: 1-200000000

Default Value

The default value depends on the rate of each port in all STP mode.

Usage Guidelines

The results of this command validates in all STP modes. In VLAN-based STP mode, the path cost of a port will be updated in all VLAN spanning trees; In MSTP mode, the path cost of a port will be updated in all STP cases.

However, the results of this command cannot affect independent configurations in each mode. For example, after you run spanning-tree sstp cost 100 and spanning-tree cost 110, the path cost of the port is still 100 in SSTP mode.

Command Mode

Port configuration mode

Example

The following example shows how to set the path cost of port g0/1 to 24:

```
Switch_config_g0/1# spanning-tree cost 24
Switch_config_g0/1#
```

17.1.9 spanning-tree sstp port-priority

Syntax

To configure the priority value of a port in SSTP mode, run spanning-tree sstp port-priority value. To resume the default value of the priority value, run no spanning-tree sstp port-priority.

spanning-tree sstp port-priority *value*

no spanning-tree sstp port-priority

Parameters

Parameters	Description
value	Means the priority level of a port. Value range: 0-240

Default Value

128 (0x80)

Usage Guidelines

The value of the priority level of a port must be the multiple of 16.

Command Mode

Port configuration mode

Example

The following example shows how to set the priority level of port g0/1 to 32:

```
Switch_config_g0/1# spanning-tree sstp port-priority 32
Switch_config_g0/1#
```

17.1.10 spanning-tree port-priority

Syntax

To configure the priority level of a port in all STP modes, run spanning-tree port-priority value. To resume the default priority level, run spanning-tree port-priority.

spanning-tree port-priority *value*

no spanning-tree port-priority

Parameters

Parameters	Description
value	Means the priority level of a port. Value range: 0-240 Step: 16

Default Value

The default value of the priority level of a port is 128 in all modes.

Usage Guidelines

The results of this command validates in all STP modes. In VLAN-based STP mode, the priority level of a port will be updated in all VLAN spanning trees; In MSTP mode, the priority level of a port will be updated in all STP cases.

However, the results of this command cannot affect independent configurations in each mode. For example, after you run spanning-tree sstp port-priority 128 and spanning-tree port-priority 48, the port-priority of the port is still 128 in SSTP mode.

Command Mode

Port configuration mode

Example

The following example shows how to set the priority level of port g0/1 to 16 in all STP modes.

```
Switch_config_g0/1#spanning-tree port-priority 16
Switch_config_g0/1#
```

17.1.11 show spanning-tree

Syntax

To display the spanning-tree information, run the following command.

show spanning-tree [**detail** | **interface** *intf-i*]

Parameters

Parameters	Description
intf-i	interface name, for instance, G0/1

Default Value

None

Usage Guidelines

This command is used to display the state of the spanning tree.

Command Mode

EXEC mode, Global configuration mode or interface mode

Example

```
Switch_config#show spanning-tree
Spanning tree enabled protocol SSTP
SSTP
  Root ID     Priority    32768
              Address     00E0.0FCC.F775
              This bridge is the root
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     00E0.0FCC.F775
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------------------
G0/1             Desg FWD 19        128.16  P2p
Switch_config#
```

17.1.12 spanning-tree management trap

Syntax

To enable STP Trap, run this command. To return to the default setting, use the no form of this command.

[no] spanning-tree management trap [**newroot** | **topologychange**]

Parameters

Parameters	Description
newroot	Stands for the newRoot trap type.
topologychange	Stands for the topologyChange trap type.

Default Value

STP Trap is disabled.

Usage Guidelines

None

Command Mode

Global configuration mode

Example

None

17.2 VLAN STP Configuration Commands

17.2.1 spanning-tree mode pvst

Syntax

To enable VLAN-based STP mode, run spanning-tree mode pvst. To disable all STP modes, run no spanning-tree mode.

spanning-tree mode pvst

no spanning-tree mode

Parameters

None

Default Value

The default STP mode is RSTP.

Usage Guidelines

None

Example

The following example shows how to enable PVST on the switch.

```
Switch_config# spanning-tree mode pvst
Switch_config#
```

17.2.2 spanning-tree vlan

Syntax

To designate VLAN to distribute the STP case, run spanning-tree vlan vlan-list. To cancel the spanning tree of the designated VLAN, run no spanning-tree vlan vlan-list.

spanning-tree vlan *vlan-list*

no spanning-tree vlan *vlan-list*

Parameters

Parameters	Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15

Default Value

The switch only distributes spanning tree instances for certain VLANs. By default the exceeding VLANs will be added to STP forbidding list automatically.

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to cancel the spanning tree of VLAN 10, 11, 15-19 and then how to distribute the spanning trees to VLAN 40-50.

```
Switch_config#no spanning-tree vlan 10,11,15-19
Switch_config#spanning-tree vlan 40-50
Switch_config#
```

17.2.3 spanning-tree vlan priority

Syntax

To designate the priority level of the bridge of the VLAN STP, run spanning-tree vlan vlan-list priority value.

spanning-tree vlan *vlan-list* **priority** *value*

no spanning-tree vlan *vlan-list* **priority**

Parameters

Parameters	Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15
value	Value of the priority level, ranging between 0 and 61400 (step: 4096)

Default Value

By default, the priority level of the bridge of each VLAN spanning tree is 32768 plus the VLAN number.

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to set the priority levels of the bridges of VLAN1-3, 5-10 to 4096.

```
Switch_config#spanning-tree vlan 1-3,5-10 priority 4096
Switch_config#
```

17.2.4 spanning-tree vlan forward-time

Syntax

To set the Forward Delay parameter of the spanning tree in the designated VLAN, run spanning-tree vlan vlan-list forward-time value.

spanning-tree vlan *vlan-list* **forward-time** *value*

no spanning-tree vlan *vlan-list* **forward-time**

Parameters

Parameters	Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15
value	Value of the forward-delay parameter Value range: 4-30 seconds Default value: 15 seconds

Default Value

The value of the forward-delay parameter of all VLANs is 15 seconds.

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to set the forward delay parameter of VLAN 1-3, 5-10 to 19 seconds.

```
Switch_config#spanning-tree vlan 1-3,5-10 forward-time 19
Switch_config#
```

17.2.5 spanning-tree vlan max-age

Syntax

To set the Max Age parameter of the spanning tree in the designated VLAN, run spanning-tree vlan vlan-list max age value. To resume the default value, run no spanning-tree vlan vlan-list max age.

spanning-tree vlan *vlan-list* **max-age** *value*

no spanning-tree vlan *vlan-list* **max-age**

Parameters

Parameters	Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15
value	Value of the max-age parameter Value range: 6-40 seconds Default value: 20 seconds

Default Value

The default value of the max-age parameter for all VLANs is 20 seconds.

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to set the max age parameter of VLAN 1-3, 5-10 to 19 seconds.

```
Switch_config#spanning-tree vlan 1-3,5-10 max-age 19
Switch_config#
```

17.2.6 spanning-tree vlan hello-time

Syntax

To set the hello time parameter of the spanning tree in the designated VLAN, run spanning-tree vlan vlan-list hello time value. To resume the default value, run no spanning-tree vlan vlan-list hello time.

spanning-tree vlan *vlan-list* **hello-time** *value*

no spanning-tree vlan *vlan-list* **hello-time**

Parameters

Parameters	Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15
value	Value of the hello time parameter Value range: 1-10 seconds Default value: 2 seconds

Default Value

The default value of the Hello-Time parameter for all VLANs is 2 seconds.

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to set the Hello Time parameter of VLAN 1-3, 5-10 to 9 seconds.

```
Switch_config#spanning-tree vlan 1-3,5-10 hello-time 9
Switch_config#
```

17.2.7 spanning-tree vlan cost

Syntax

To set the path cost of the spanning tree in the designated VLAN, run spanning-tree vlan vlan-list cost value. To resume the default value, run no spanning-tree vlan vlan-list cost.

spanning-tree vlan *vlan-list* **cost** *value*

no spanning-tree vlan *vlan-list* **cost**

Parameters

Parameters	Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15
value	Path cost of a port, which ranges between 1 and 200,000,000

Default Value

The path cost of a port depends on the port rate.

The value of the path cost of the 10M Ethernet is 100.

The value of the path cost of the 100M Ethernet is 19.

The value of the path cost of the 1000M Ethernet is 1.

Usage Guidelines

None

Command Mode

Port configuration mode

Example

The following example shows how to set the path cost of port G0/1 VLAN1-3,5-10 to 100.

```
Switch_config_g0/1#spanning-tree vlan 1-3,5-10 cost 100
Switch_config_g0/1#
```

17.2.8 spanning-tree vlan port-priority

Syntax

To set the priority level of the spanning tree in the designated VLAN, run spanning-tree vlan vlan-list port-priority value. To resume the default value, run no spanning-tree vlan vlan-list port-priority.

spanning-tree vlan *vlan-list* **port-priority** *value*

no spanning-tree vlan *vlan-list* **port-priority**

Parameters

Parameters	Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15
value	Priority level of a port, which ranges between 0 and 240 and whose step is 16

Default Value

128

Usage Guidelines

None

Command Mode

Port configuration mode

Example

The following example shows how to set the priority level of port g0/1 VLAN1-3,5-10 to 32.

```
Switch_config_g0/1#spanning-tree vlan 1-3,5-10 port-priority 32
Switch_config_g0/1#
```

17.2.9 show spanning-tree vlan

Syntax

To check the state of the spanning tree in the designated VLAN, run the following command:

show spanning-tree vlan *vlan-list* [**detail**]

Parameters

Parameters	Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15
detail	Displays the detailed information about the state of the spanning tree.

Default Value

None

Usage Guidelines

None

Command Mode

EXEC mode, Global configuration mode or interface mode

Example

The following example shows how to check the spanning tree of VLAN 1-2.

```
Switch_config#show spanning-tree vlan 1-2
Spanning tree enabled protocol PVST
VLAN0001
 Root ID     Priority    32769
             Address     00E0.0FCC.F775
             This bridge is the root
               Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769
             Address     00E0.0FCC.F775
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------------------
G0/1             Desg FWD 19        128.1   P2p
VLAN0002
  Root ID     Priority    32770
              Address     00E0.0FCC.F775
              This bridge is the root
              Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID   Priority      32770
                Address       00E0.0FCC.F775
                Hello Time 2 sec   Max Age 20 sec   Forward Delay 15 sec
Interface          Role Sts Cost      Pri.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
G0/1               Desg FWD 19        128.1    P2p
Switch_config#
```

17.2.10 show spanning-tree pvst instance-list

Syntax

To check the corresponding relation between PVST instances and VLAN, run this command.

show spanning-tree pvst instance-list

Parameters

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC mode, Global configuration mode or interface mode

Example

None

17.3 RSTP Configuration Commands

17.3.1 spanning-tree mode rstp

Syntax

To enable the RSTP function, run spanning-tree mode rstp. To disable the STP, run no spanning-tree mode.

spanning-tree mode rstp

no spanning-tree mode

Parameters

None

Default Value

RSTP is enabled.

Usage Guidelines

None

Example

The following example shows how to enable RSTP on the switch.

```
Switch_config# spanning-tree mode rstp
Switch_config#
```

17.3.2 spanning-tree rstp forward-time

Syntax

To configure the forwarding delay of RSTP, run spanning-tree rstp forward-time time. To resume the default forwarding delay of RSTP, run no spanning-tree rstp forward-time.

spanning-tree rstp forward-time *time*

no spanning-tree rstp forward-time

Parameters

Parameters	Description
time	Time of the forwarding delay Value Range:4-30s.

Default Value

15 seconds

Usage Guidelines

None

Example

The following example shows how to set the forwarding delay of RSTP to 20 seconds.

```
Switch_config# spanning-tree rstp forward-time 20
Switch_config#
```

17.3.3 spanning-tree rstp hello-time

Syntax

To configure the update interval of RSTP, run spanning-tree rstp hello-time time. To resume the default update interval of RSTP, run no spanning-tree rstp hello-time.

spanning-tree rstp hello-time *time*

no spanning-tree rstp hello-time

Parameters

Parameters	Description
time	Updates the interval. Range: 1-10 seconds

Default Value

2 seconds

Usage Guidelines

The Hello-Time configured on the local switch validates only when the local switch runs as a root switch.

Example

The following example shows how to set the update interval of RSTP to 8 seconds.

```
Switch_config# spanning-tree rstp hello-time 8
Switch_config#
```

17.3.4 spanning-tree rstp max-age

Syntax

To configure the maximum lifespan of the SSTP BPDU, run spanning-tree sstp max-age time. To resume the default interval time, run no spanning-tree sstp max-age.

spanning-tree rstp max-age *time*

no spanning-tree rstp max-age

Parameters

Parameters	Description
time	Maximum interval of the lifespan Range: 6-40 seconds

Default Value

20 seconds

Usage Guidelines

None

Example

The following example shows how to set the maximum lifespan of RSTP to 24 seconds.

```
Switch_config# spanning-tree rstp max-age 24
Switch_config#
```

17.3.5 spanning-tree rstp priority

Syntax

To configure the RSTP priority value, run spanning-tree rstp priority value. To resume the default value of the RSTP priority value, run no spanning-tree rstp priority.

spanning-tree rstp priority *value*

no spanning-tree rstp priority

Parameters

Parameters	Description
value	Priority level of the bridge Value range: 0-61440 Step: 4096

Default Value

32768

Usage Guidelines

None

Example

The following example shows how to set the bridge priority of RSTP to 4096.

```
Switch_config# spanning-tree rstp priority 4096
Switch_config#
```

17.3.6 spanning-tree rstp cost

Syntax

To configure the path cost of a port, run spanning-tree rstp cost value. To resume the default value, run no spanning-tree rstp cost.

spanning-tree rstp cost *value*

no spanning-tree rstp cost

Parameters

Parameters	Description
value	Value of the path cost Value range: 1-200000000

Default Value

The path cost depends on the connection rate of the port.

10 Mbps: 2000000

100 Mbps: 200000

1000 Mbps: 20000

Usage Guidelines

None

Example

The following example shows how to set the path cost of port g0/1 to 24:

```
Switch_config_g0/1# spanning-tree rstp cost 24
Switch_config_g0/1#
```

17.3.7 spanning-tree rstp port-priority

Syntax

To configure the priority level of a port, run spanning-tree rstp port-priority value. To resume the default value, run no spanning-tree rstp port-priority.

spanning-tree rstp port-priority *value*

no spanning-tree rstp port-priority

Parameters

Parameters	Description
value	Priority level of a port Value range: 0-240 Step: 16

Default Value

128

Usage Guidelines

None

Example

The following example shows how to set the priority level of port g0/1 to 16:

```
Switch_config_g0/1# spanning-tree rstp port-priority 16
Switch_config_g0/1#
```

17.3.8 spanning-tree rstp edge

Syntax

To set the port to the edge port. To return to the default setting, use the no form of this command.

spanning-tree rstp edge

no spanning-tree rstp edge

Parameters

None

Default Value

Auto-detection

Usage Guidelines

None

Command Mode

Port configuration mode

Example

None

17.3.9 spanning-tree rstp point-to-point

Syntax

To set the point-to-point connection of a port to force-truce, force-false or auto, run this command.

spanning-tree rstp point-to-point [force-true | force-false | auto]

Parameters

Parameters	Description
force-true	Sets the point-to-point connection to be forcedly effective.
force-false	Sets the point-to-point connection to be forcedly ineffective.
auto	Sets the point-to-point connection to be automatic check (default).

Default Value

Auto-detection

Usage Guidelines

None

Command Mode

Port configuration mode

Example

None

17.3.10 spanning-tree rstp migration-check

Syntax

To restart checking protocol transfer of RSTP, run the following command.

spanning-tree rstp migration-check

Parameters

None

Default Value

None

Usage Guidelines

This command is used to restart the protocol transfer check on a port and to change the port in STP-compatible mode to the RSTP mode, enabling RSTP BPDU to be transmitted.

Command Mode

Global or port configuration mode

Example

The following example shows how to check protocol transfer on port G0/1.

```
Switch_config_g0/1#spanning-tree rstp migration-check
Switch_config_g0/1#
```

17.4 MSTP Configuration Commands

17.4.1 spanning-tree mode mstp

Syntax

To set the operation mode of the spanning tree to MSTP, run spanning-tree mode mstp. To return to the default set, run no spanning-tree mode.

spanning-tree mode mstp

no spanning-tree mode

Parameters

None

Default Value

MSTP is disabled, while SSTP is enabled.

Usage Guidelines

None

Example

The following example shows how to enable MSTP on a switch.

```
Switch_config# spanning-tree mode mstp
Switch_config#
```

17.4.2 spanning-tree mstp name

Syntax

To configure the MSTP name, run spanning-tree mstp name string. To resume the default name, run no spanning-tree mstp name.

spanning-tree mstp name *string*

no spanning-tree mstp name

Parameters

Parameters	Description
string	A character string to configure the name, which contains up to 32 characters and is capital sensitive. The default value is the character string of the MAC address.

Default Value

Its default value is the MAC address of a switch.

Usage Guidelines

None

Example

The following example shows how to set the name of MSTP for a switch to reg-01.

```
Switch_config# spanning-tree mstp name reg-01
Switch_config#
```

17.4.3 spanning-tree mstp revision

Syntax

To configure the MSTP revision number, run spanning-tree mstp revision value. To resume the default revision number, run no spanning-tree mstp revision.

spanning-tree mstp revision *value*

no spanning-tree mstp revision

Parameters

Parameters	Description
value	Revision number, which ranges between 0 and 65535 and whose default value is 0

Default Value

The default value of the revision number is 0.

Usage Guidelines

None

Example

The following example shows how to set the revision number of MSTP to 100.

```
Switch_config# spanning-tree mstp revision 100
Switch_config#
```

17.4.4 spanning-tree mstp instance

Syntax

To map VLAN to MSTI, run spanning-tree mstp instance instance-id vlan vlan-list. To remap VLAN to CIST, run no spanning-tree mstp instance instance-id.

spanning-tree mstp instance *instance-id* **vlan** *vlan-list*

no spanning-tree mstp instance *instance-id*

Parameters

Parameters	Description
instance-id	Instance ID of the spanning-tree, which stands for an MSTI Value range: 1-15
vlan-list	A VLAN list which is mapped to a spanning tree It ranges from 1 to 4094.

Default Value

All VLANs are mapped to CIST (MST00).

Usage Guidelines

Instance ID is an independent value which stands for an STP instance.

The vlan-list parameter can stand for a VLAN group, such as VLANs 1,2 and3, VLANs 1-5 or VLANs 1,2,5-10.

Example

The following example shows how to map VLAN2 to STP instance 1, and VLANs 5, 7, 10-20 to STP instance 2 and then remap these VLANs to MST00.

```
Switch_config# spanning-tree mstp instance 1 vlan 2
Switch_config# spanning-tree mstp instance 2 vlan 5,7,10-20
Switch_config# no spanning-tree mstp instance 1
Switch_config# no spanning-tree mstp instance 2
```

17.4.5 spanning-tree mstp root

Syntax

To set a designated STP instance to a primary or secondary root, run spanning-tree mstp instance-id root {primary | secondary}. To resume the default value of the bridge priority of an STP instance, run no spanning-tree mstp root.

spanning-tree mstp *instance-id* **root** {**primary** | **secondary**}

[**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mstp *instance-id* **root**

The diameter command and the hello time command are allowed to modify the network diameter and the hello-time parameter.

Parameters

Parameters	Description
instance-id	Number of the STP instance, which ranges between 0 and 15
primary	Sets an STP instance to a primary root.
secondary	Sets an STP instance to a secondary root.
net-diameter	An optional parameter which presents the network diameter. When instance-id is 0, net-diameter ranges between 2 and 7.
seconds	An optional parameter standing for the value of the Hello Time parameter, which ranges between 1 and 10 seconds

Default Value

The default value of the bridge priority for all STP instances is 32768. The network diameter is 7, while Hello Time is 2 seconds.

Usage Guidelines

The diameter command and the hello-time command validate only when the instance-id parameter is 0.

In general, after the command to set the primary root is executed, the protocol automatically check the bridge ID of the current network's root and then sets the priority of the bridge ID to 24576, which guarantees that the current switch serves as the root of the STP instance. If the priority value of the network root is less than 24576, the protocol will automatically set the STP priority of the current bridge to a value which is 4096 smaller than the priority of the root. It deserves attention that 4096 is the step of the priority value of the bridge.

Different from primary root configuration, after the command to set the secondary root is executed, the protocol directly set the STP priority of the switch to 28672. In case that the priority value of other switches in the network is 32768 by default, the current switch serves as the secondary root.

Example

The following example shows how to set a switch to the primary root in CIST, and how to recalculate the time parameter of STP through diameter 3 and hello-time 3, and then set the switch to the secondary root in MST01.

```
Switch_config# spanning-tree mstp 0 root primary diameter 3 hello-time 3
Switch_config# spanning-tree mstp 1 root secondary
```

17.4.6 spanning-tree mstp priority

Syntax

To configure the value of the bridge priority of a designated STP instance, run spanning-tree mstp instance-id priority value. To resume the default value of the bridge priority, run no spanning-tree mstp priority.

spanning-tree mstp *instance-id* **priority** *value*

no spanning-tree mstp *instance-id* **priority**

Parameters

Parameters	Description
instance-id	Number of the STP instance, which ranges between 0 and 15
value	Value of the bridge priority, which can be one of the following values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440,

Default Value

The default value of the bridge priority for all STP instances is 32768.

Usage Guidelines

The priority values in each STP instance are independent and can be configured independently.

Example

The following example shows how to set the priority values of a switch in CIST and MST01 to 4096 and 8192 respectively.

```
Switch_config# spanning-tree mstp 0 priority 4096
Switch_config# spanning-tree mstp 1 priority 8192
```

17.4.7 spanning-tree mstp hello-time

Syntax

To configure the Hello Time of MSTP, run spanning-tree mstp hello-time seconds. To resume the default value of the Hello Time of MSTP, run no spanning-tree mstp hello-time.

spanning-tree mstp hello-time *seconds*

no spanning-tree mstp hello-time

Parameters

Parameters	Description
seconds	Value range: 1-10 seconds Default value: 2 seconds

Default Value

2 seconds

Usage Guidelines

None

Example

The following example shows how to set the Hello Time parameter of MSTP to 10.

```
Switch_config# spanning-tree mstp hello-time 10
Switch_config# no spanning-tree mstp hello-time
```

17.4.8 spanning-tree mstp forward-time

Syntax

To configure the forward delay parameter of MSTP, run spanning-tree mstp forward-time seconds.To resume the default value of the forward delay parameter of MSTP, run no spanning-tree mstp forward-time.

spanning-tree mstp forward-time *seconds*

no spanning-tree mstp forward-time

Parameters

Parameters	Description
seconds	Value range: 4-30 seconds Default value: 15 seconds

Default Value

15 seconds

Usage Guidelines

None

Example

The following example shows how to set the Forward Delay parameter of MSTP to 10.

```
Switch_config# spanning-tree mstp forward-time 10
Switch_config# no spanning-tree mstp forward-time
```

17.4.9 spanning-tree mstp max-age

Syntax

To configure the max age parameter of MSTP, run spanning-tree mstp max-age seconds.To resume the default value of the forward delay parameter of MSTP, run no spanning-tree mstp max-age.

spanning-tree mstp max-age *seconds*

no spanning-tree mstp max-age

Parameters

Parameters	Description
seconds	Value range: 6-40 seconds Default value: 20 seconds

Default Value

20 seconds

Usage Guidelines

None

Example

The following example shows how to set the max age parameter of MSTP to 10.

```
Switch_config# spanning-tree mstp max-age 10
Switch_config# no spanning-tree mstp max-age
```

17.4.10 spanning-tree mstp diameter

Syntax

To configure the network diameter of MSTP, run spanning-tree mstp diameter net-diameter. To resume the default value of the network diameter, run no spanning-tree mstp diameter.

spanning-tree mstp diameter *net-diameter*

no spanning-tree mstp diameter

Parameters

Parameters	Description
net-diameter	Value range: 2-7 Default value: 7

Default Value

The default value of the network diameter is 7.

Usage Guidelines

The net-diameter parameter is not saved as an independent configuration in the switch. Only the time parameter which is modified through network diameter configuration can be saved. The net-diameter parameter is effective only to CIST. After configuration, the three time parameters of STP are automatically updated to a prior value.

It is recommended to modify the time parameter of STP through setting the root or network diameter, ensuring the rationality of the time parameter.

Example

The following example shows how to set the network diameter of MSTP to 5 and then resume its default value.

```
Switch_config# spanning-tree mstp diameter 5
Switch_config# no spanning-tree mstp diameter
```

17.4.11 spanning-tree mstp max-hops

Syntax

To set the maximum hops of MSTP BPDU, run spanning-tree mstp max-hops hop-count. To resume the default settings, run no spanning-tree mstp max-hops.

spanning-tree mstp max-hops *hop-count*

no spanning-tree mstp max-hops

Parameters

Parameters	Description
hop-count	Value range: 6-40 Default value: 20

Default Value

The default value of the maximum hops is 20.

Usage Guidelines

None

Example

The following example shows how to set the maximum hops of MSTP BPDU to 5 and then resume the default value.

```
Switch_config# spanning-tree mstp max-hops 5
Switch_config# no spanning-tree mstp max-hops
```

17.4.12 spanning-tree mstp port-priority

Syntax

To configure the port priority in the designated spanning-tree instance, run spanning-tree mstp instance-id port-priority value. To resume the port priority to the default settings, run no spanning-tree mstp instance-id port-priority.

spanning-tree mstp *instance-id* **port-priority** *value*

no spanning-tree *instance-id* **port-priority**

Parameters

Parameters	Description
instance-id	Number of the STP instance, which ranges between 0 and 15
value	Value of the port priority, which can be one of the following values 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240,

Default Value

The port priority in all STP instances is 128 by default.

Usage Guidelines

None

Example

The following example shows how to set the priority value of port G0/1 in CIST to 16 and then resume the default value.

```
Switch_config_g0/1# spanning-tree mstp 0 port-priority 16
Switch_config_g0/1# no spanning-tree mstp 0 port-priority
```

17.4.13 spanning-tree mstp cost

Syntax

To set the path cost of the spanning tree in the designated STP instance, run spanning-tree mstp instance-id cost value. To resume the default value, run no spanning-tree mstp instance-id cost.

spanning-tree mstp *instance-id* **cost** value

no spanning-tree mstp *instance-id* **cost**

Parameters

Parameters	Description
instance-id	Number of the STP instance, which ranges between 0 and 15
value	Path cost of a port, which ranges between 1 and 200,000,000

Default Value

The path cost depends on the connection rate of the port.

10 Mbps: 2000000

100 Mbps: 200000

1000 Mbps: 20000

Usage Guidelines

None

Example

The following example shows how to set the path cost of port G0/1 to 200 in CIST.

```
Switch_config_g0/1# spanning-tree mstp 0 cost 200
Switch_config_g0/1#
```

17.4.14 spanning-tree mstp edge

Syntax

To set the port to the edge port. To return to the default setting, use the no form of this command.

spanning-tree mstp edge

no spanning-tree mstp edge

Parameters

None

Default Value

Automatically checks the edge port.

Usage Guidelines

None

Example

None

17.4.15 spanning-tree mstp point-to-point

Syntax

To configure the connection type of a port, run spanning-tree mstp point-to-point { force-true | force-false | auto }. To resume the connection type to auto-check, run no spanning-tree mstp point-to-point.

spanning-tree mstp point-to-point { **force-true** | **force-false** | **auto** }

no spanning-tree mstp point-to-point

Parameters

Parameters	Description
force-true	Sets the port connection mode to point-to-point.
force-false	Sets the port connection mode to sharing.
auto	Sets the port connection mode to auto-check (the default mode).

Default Value

MSTP will automatically check the port connection mode by default.

Usage Guidelines

None

Example

The following example shows how to set the connection mode of port G0/1 to sharing.

```
Switch_config_g0/1# spanning-tree mstp point-to-point force-false
Switch_config_g0/1#
```

17.4.16 spanning-tree mstp mst-compatible

Syntax

To enable or disable multiple spanning tree compatible mode, run this command in global configuration mode.

spanning-tree mstp mst-compatible

no spanning-tree mstp mst-compatible

To enable or disable multiple spanning tree compatible mode, run this command in interface configuration mode.

spanning-tree mstp mst-compatible {enable | disable}

no spanning-tree mstp mst-compatible

Parameters

Parameters	Description
enable	The mst-compatible mode is enabled.
disable	The mst-compatible mode is disabled.

Default Value

The compatible mode is not activated by default and the switch cannot establish an area with other switches which transmit BPDU in compatible mode.

Usage Guidelines

After the compatible mode is enabled, you are recommended to set a connected switch which runs other MSTP to the root of CIST, securing that the switch can enter the compatible mode through receiving packets.

Example

The following example shows how to activate the MST-compatible mode of a switch in global configuration mode.

```
Switch_config#spanning-tree mstp mst-compatible
```

17.4.17 spanning-tree mstp migration-check

Syntax

To remove the STP information which is checked on a port and then restart the protocol transform process, run the following command.

spanning-tree mstp migration-check

Parameters

None

Default Value

None

Usage Guidelines

This command validates both in global configuration mode and in port configuration mode.

Example

The following example shows how to conduct the protocol transfer check on all ports and then conduct the second protocol transfer check on port G0/1.

```
Switch_config# spanning-tree mstp migration-check
Switch_config# interface g0/1
Switch_config_g0/1# spanning-tree mstp migration-check
```

17.4.18 spanning-tree mstp restricted-role

Syntax

To enable role restriction of the port, run the following command. To return to the default setting, use the no form of this command.

[no] spanning-tree mstp restricted-role

Parameters

None

Default Value

The role restriction of the port is disabled by default.

Command Mode

Port configuration mode

Usage Guidelines

The port will not be selected as the root port if the role restriction of the port is enabled.

Example

None

17.4.19 spanning-tree mstp restricted-tcn

Syntax

To enable TCN restriction of the port, run the following command. To return to the default setting, use the no form of this command.

[no] spanning-tree mstp restricted-tcn

Parameters

None

Default Value

TCN restriction of the port is disabled by default.

Command Mode

Port configuration mode

Usage Guidelines

The topology change will not be transferred to other port if TCN restriction of the port is enabled.

Example

None

17.4.20 show spanning-tree mstp

Syntax

To browse the MSTP information, run show spanning-tree mstp [instance instance-id]. If the instance parameter is not in the command syntax, the information about all spanning-tree instances will be displayed.

show spanning-tree mstp [**instance** *instance-id*]

Parameters

Parameters	Description
instance-id	Number of the STP instance, which ranges between 0 and 15

Default Value

None

Usage Guidelines

This command can be used in monitoring mode, global configuration mode or port mode.

Example

The following example shows how to browse all spanning-tree instances. MST00 stands for CIST, while Type stands for the connection type of the corresponding port.

```
Switch#show spanning-tree mstp

MST00            Vlans Mapped:    1,4-4094
Bridge           Address    00E0.0F64.8365    Priority    32768 (32768 mst-id 0)
Root             This bridge is the CIST and regional root
Configured       Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20
Root Times       Hello Time 2, Forward Delay 15, Max Age 20

Interface              Role Sts Cost          Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------------------
G0/1                   Desg FWD 200000        128.1     P2p
G0/2                   Desg FWD 200000        128.2    Edge
MST01            Vlans Mapped:    2
Bridge           Address    00E0.0F64.8365    Priority    32769 (32768 mst-id 1)
Root             This bridge for MST01

Interface              Role Sts Cost          Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------------------
G0/1                   Desg FWD 200000        128.1     P2p

MST02            Vlans Mapped:    3
Bridge           Address    00E0.0F64.8365    Priority    32770 (32768 mst-id 2)
Root             This bridge for MST02

Interface              Role Sts Cost          Pri.Nbr Type
---------------- ---- --- --------- ------- --------------------------------
G0/1                   Desg FWD 200000        128.1     P2p
```

17.4.21 show spanning-tree mstp region

Syntax

To browse the area configuration information about MSTP, run the following command.

show spanning-tree mstp region

Parameters

None

Default Value

None

Usage Guidelines

None

Example

In the following example, MST Config Table is to display the relationship between VLAN and spanning-tree instance.

```
Switch_config# show spanning-tree mstp region

MST Region:
   Name:      [reg01]
   Revision:[0]
Instance         VLAN IDs
----------       ----------
              0        1,4-4094
              1        2
              2        3
```

17.4.22 show spanning-tree mstp detail

Syntax

To browse the detailed information about MSTP, run the following command.

show spanning-tree mstp detail

Parameters

None

Default Value

None

Usage Guidelines

None

Example

The following example shows how to browse the detailed information about MSTP, which includes the port connection types and the configuration of optional attributes.

```
Switch#show spanning-tree mstp detail

MST00            Vlans Mapped:    1,4-4094
Bridge           Address    00E0.0F64.8365    Priority    32768 (32768 mst-id 0)
Root             This bridge is the CIST and regional root
Configured       Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20
Root Times       Hello Time 2, Forward Delay 15, Max Age 20

GigaEthernet0/1 of MST00 is designated forwarding
Port Info                    Port ID 128.1                Priority 128        Cost 200000
Designated Root              Address 00E0.0F64.8365    Priority 32768    Cost 0
CIST Regional Root       Address 00E0.0F64.8365    Priority 32768    Cost 0
Designated Bridge          Address 00E0.0F64.8365    Priority 32768    Port ID 128.1
Edge Port:      disabled                        Link Type:    point-to-point (auto)
Bpdu Guard:    disabled (default)            Root Guard: disabled (default)
Loop Guard:    disabled (default)
Timers:    message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
Bpdu sent 335, received 5
GigaEthernet0/2 of MST00 is designated forwarding
Port Info                    Port ID 128.47               Priority 128        Cost 200000
Designated Root              Address 00E0.0F64.8365    Priority 32768    Cost 0
CIST Regional Root       Address 00E0.0F64.8365    Priority 32768    Cost 0
Designated Bridge          Address 00E0.0F64.8365    Priority 32768    Port ID 128.2
Edge Port:      enabled (auto)                Link Type:    point-to-point (auto)
Bpdu Guard:    disabled (default)            Root Guard: disabled (default)
Loop Guard:    disabled (default)
Timers:    message expires in 0 sec, forward delay 0 sec, up time 1485 sec
Number of transitions to forwarding state: 1
Bpdu sent 744, received 0

MST01            Vlans Mapped:    2
Bridge           Address    00E0.0F64.8365    Priority    32769 (32768 mst-id 1)
Root             This bridge for MST01

GigaEthernet0/1 of MST01 is designated forwarding
```

```
Port Info                Port ID 128.1                Priority 128      Cost 200000
Designated Root          Address 00E0.0F64.8365   Priority 32769    Cost 0
Desingated Bridge        Address 00E0.0F64.8365   Priority 32769    Port ID 128.1
Timers:   message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 335, received 0

MST02          Vlans Mapped:   3
Bridge         Address   00E0.0F64.8365   Priority   32770 (32768 mst-id 2)
Root           This bridge for MST02

GigaEthernet0/1 of MST02 is designated forwarding
Port Info                Port ID 128.1                Priority 128      Cost 200000
Designated Root          Address 00E0.0F64.8365   Priority 32770    Cost 0
Desingated Bridge        Address 00E0.0F64.8365   Priority 32770    Port ID 128.1
Timers:   message expires in 0 sec, forward delay 0 sec, up time 662 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 335, received 0
```

17.4.23 show spanning-tree mstp interface

Syntax

To browse the information about a port under MSTP, run the following command.

show spanning-tree mstp interface *interface-id*

Parameters

Parameters	Description
interface-id	interface name, for instance, "G0/1", "GigaEthernet0/2".

Default Value

None

Usage Guidelines

None

Example

The following example shows how to browse the information about interface G0/1.

```
Switch#show spanning-tree mstp interface g0/1

GigaEthernet0/1 of MST00 is designated forwarding
Port Info                Port ID 128.1                Priority 128      Cost 200000
Designated Root          Address 00E0.0F64.8365   Priority 32768    Cost 0
CIST Regional Root       Address 00E0.0F64.8365   Priority 32768    Cost 0
Designated Bridge        Address 00E0.0F64.8365   Priority 32768    Port ID 128.1
Edge Port:     disabled                    Link Type:    point-to-point (auto)
Bpdu Guard:    disabled (default)          Root Guard: disabled (default)
Loop Guard:    disabled (default)
Timers:   message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
Bpdu sent 430, received 5
```

```
GigaEthernet0/1 of MST01 is designated forwarding
Port Info                   Port ID 128.1                Priority 128       Cost 200000
Designated Root             Address 00E0.0F64.8365   Priority 32769   Cost 0
Desingated Bridge         Address 00E0.0F64.8365   Priority 32769   Port ID 128.1
Timers:   message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 430, received 0

GigaEthernet0/1 of MST02 is designated forwarding
Port Info                   Port ID 128.1                Priority 128       Cost 200000
Designated Root             Address 00E0.0F64.8365   Priority 32770   Cost 0
Desingated Bridge         Address 00E0.0F64.8365   Priority 32770   Port ID 128.1
Timers:   message expires in 0 sec, forward delay 0 sec, up time 851 sec
Number of transitions to forwarding state: 1
MST Config Message transmitted 430, received 0

Instance Role Sts Cost          Pri.Nbr Vlans Mapped
-------- ---- --- --------- ------- --------------------
0            Desg FWD 200000      128.1    1,4-4094
1            Desg FWD 200000      128.1    2
2            Desg FWD 200000      128.1    3
```

17.4.24 show spanning-tree mstp protocol-migration

Syntax

To browse the protocol transfer information on an interface under MSTP, run the following command.

show spanning-tree mstp protocol-migration

Parameters

None

Default Value

None

Usage Guidelines

None

Example

The following example shows how to browse the information about protocol transfer on an interface. In the following example, interface G0/1 is running in 802.1D STP mode.

```
Switch#show spanning-tree mstp protocol-migration
MSTP Port Protocol Migration
Interface              Protocol
---------------- ---------- ------------
G0/1                    802.1D
```

Chapter 18 STP Optional Characteristic Configuration Commands

18.1 STP Optional Characteristic Configuration Commands

18.1.1 spanning-tree portfast

Syntax

To configure the portfast attribute in global configuration mode, run spanning-tree portfast {bpdufilter default | bpduguard default | default}. To cancel this attribute in global configuration mode, run no spanning-tree portfast {bpdufilter default | bpduguard default | default}.

spanning-tree portfast {bpdufilter | bpduguard | default}

no spanning-tree portfast {bpdufilter | bpduguard | default}

To configure the portfast attribute in port configuration mode, run spanning-tree portfast [disable | trunk]. To cancel this attribute in port configuration mode, run no spanning-tree portfast.

spanning-tree portfast [disable]

no spanning-tree portfast

Parameters

Parameters	Description
bpdufilter	Starts the BPDU filtration.
bpduguard	Starts the BPDU protection.
default	Means the default mode.

Default Value

This function is not enabled by default.

Usage Guidelines

The portfast attribute enables a port in SSTP/PVST mode to promptly enter the forwarding state without state change. This configuration invalidates in RSTP/MSTP mode.

After the portfast attribute is configured, it need be protected through BPDU Guard configuration or BPDU Filter configuration.

Command Mode

Global or port configuration mode

Example

The following example shows how to enable the Port Fast attribute in global configuration mode.

```
Switch_config# spanning-tree portfast default
Switch_config#
```

The following example shows how to enable the attributes of port g0/1:

```
Switch_config_g0/1# spanning-tree portfast
Switch_config_g0/1#
```

18.1.2 spanning-tree bpduguard

Syntax

To configure BPDU Guard, run spanning-tree bpduguard {disable | enable}. To cancel BPDU Guard, run no spanning-tree bpduguard.

spanning-tree bpduguard {**disable** | **enable**}

no spanning-tree bpduguard

Parameters

None

Default Value

This function is not enabled by default.

Usage Guidelines

In SSTP/PVST mode, if a port that has the BPDU Guard function and the Portfast function configured receives BPDU, this port will be manadatorily shut down. You have to configure the port manually to resume this port. In RSTP/MSTP mode, if a BPDU-Guard-configured port receives BPDU, the port will be set to the Blocking state in a period of time.

Command Mode

Port configuration mode

Example

The following example shows how to enable BPDU protection on port g0/1.

```
Switch_config_g0/1# spanning-tree bpduguard enable
Switch_config_g0/1#
```

18.1.3 spanning-tree bpdufilter

Syntax

To configure the BPDU filtration, run spanning-tree bpdufilter {disable | enable}. To cancel the BPDU filtration, run no spanning-tree bpdufilter.

spanning-tree bpdufilter {**disable** | **enable**}

no spanning-tree bpdufilter

Parameters

None

Default Value

This function is not enabled by default.

Usage Guidelines

In SSTP/PVST mode, a port which has the BPDU Filter function and the Port Fast function configured receives BPDU, the BPDU Filter attribute and the Port Fast attribute are automatically shut down. In this case, the port resumes to be a normal port which first enters the listening state, the learning state and then the forwarding state.

This function invalidates in RSTP/MSTP mode.

Command Mode

Port configuration mode

Example

The following example shows how to enable BPDU filtration on port g0/1.

```
Switch_config_g0/1# spanning-tree bpdufilter enable
Switch_config_g0/1#
```

18.1.4 spanning-tree uplinkfast

Syntax

To configure the Uplink Fast function, run this command. To return to the default setting, use the no form of this command.

spanning-tree uplinkfast

no spanning-tree uplinkfast

Parameters

None

Default Value

This function is not enabled by default.

Usage Guidelines

The Uplink Fast function validates only in SSTP/PVST mode.

Command Mode

Global configuration mode

Example

The following example shows how to enable the Uplink Fast attribute.

```
Switch_config# spanning-tree uplinkfast
Switch_config#
```

18.1.5 spanning-tree backbonefast

Syntax

To configure the backbonefast function, run spanning-tree backbonefast. To cancel the backbonefast function, run no spanning-tree backbonefast.

spanning-tree backbonefast

no spanning-tree backbonefast

Parameters

None

Default Value

This function is not enabled by default.

Usage Guidelines

The backbonefast function validates only in SSTP/PVST mode.

Command Mode

Global configuration mode

Example

The following example shows how to enable the backbonefast function:

```
Switch_config# spanning-tree backbonefast
Switch_config#
```

18.1.6 spanning-tree guard

Syntax

To configure the Port Guard function, run spanning--tree guard {loop | none | root}. To cancel this function, run no spanning--tree guard.

spanning-tree guard {loop | none | root}

no spanning-tree guard

Parameters

Parameters	Description
loop	Guard loop.
none	Guard none.
root	Guard root

Default Value

This protection function is not enabled.

Usage Guidelines

The Root Guard attribute can prevent a port from serving as a root port after it receives a higher-priority BPDU.

The Loop Guard attribute can protect a port after it changes from a root port or an alternate port to a designated port. This function can prevent a port from generating a loop when the port cannot receive BPDU continuously.

Command Mode

Port configuration mode

Example

The following example shows how to prevent port g0/1 from being the root:

```
Switch_config_g0/1# spanning-tree guard root
Switch_config_g0/1#
```

18.1.7 spanning-tree loopguard

Syntax

To configure the guard loop in global configuration mode, run spanning-tree loopguard default. To cancel the guard loop in global configuration mode, run no spanning-tree loopguard default.

spanning-tree loopguard default

Parameters

None

Default Value

None

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to enable the loopguard function.

```
Switch_config# spanning-tree loopguard default
Switch_config#
```

18.1.8 spanning-tree loopfast

Syntax

To enable Loop Fast in global configuration mode, run spanning-tree loopfast. To return to the default setting, use the no form of this command.

spanning-tree loopfast

To set Loop Fast attribute, run this command.

spanning-tree loopfast

To disable the Loop Fast attribute, use the no form of this command.

spanning-tree loopfast disable

Parameters

None

Default Value

None

Usage Guidelines

Please configure this command under the guide of technical engineers.

Command Mode

Global configuration mode and interface configuration mode

Example

The following example shows how to enable loopfast in global configuration mode and disable the function on port G0/1.

```
Switch_config#spanning-tree loopfast
Switch_config#int g0/1
Switch_config_g0/1#spanning-tree loopfast disable
Switch_config_g0/1#exit
```

```
Switch_config#
```

18.1.9 spanning-tree fast-aging

Syntax

To enable or disable the fast aging mechanism of the address table, run the following commands.

spanning-tree fast-aging

no spanning-tree fast-aging

To enable or disable the protection of fast aging of the address table, run the following commands.

spanning-tree fast-aging protection

no spanning-tree fast-aging protection

To configure the time of aging protection of the address table, run the following commands.

spanning-tree fast-aging protection time *value*

no spanning-tree fast-aging protection time

Parameters

Parameters	Description
value	Stands for the aging protection time. 10-60 seconds (15 seconds by default)

Default Value

Fast aging is enabled by default. However protection is not enabled by default.

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to enable fast aging protection and set the protection time to 30 seconds.

```
Switch_config#spanning-tree fast-aging protection
Switch_config#spanning-tree fast-aging protection time 30
```

18.1.10 spanning-tree fast-aging flush-fdb

Syntax

To enable or disable FDB-Flush, run the following commands.

spanning-tree fast-aging flush-fdb

no spanning-tree fast-aging flush-fdb

Parameters

None

Default Value

FDB-Flush is enabled by default.

Usage Guidelines

Please configure this command under the guide of technical engineers.

FDB-Flush is independent of fast aging.FDB-Flush can be configured while **no spanning-tree fast-aging**is configured. But fast aging protection function has no effect on FDB-Flush.

Command Mode

Global configuration mode

Example

The following example shows how to disable fast aging and enable FDB-Flush.

```
Switch_config#no spanning-tree fast-aging
Switch_config#spanning-tree fast-aging flush-fdb
```

18.1.11 spanning-tree bpdu-terminal

Syntax

To enable or disable BPDU Terminal, run the following commands.

spanning-tree bpdu-terminal

no spanning-tree bpdu-terminal

Parameters

None

Default Value

BPDU Terminal is disabled by default.

Usage Guidelines

BPDU terminal function can forbid forwarding BPDU when there is no STP running.

Command Mode

Global configuration mode

Example

The following example shows how to enable BPDU Terminal:

```
Switch_config#spanning-tree bpdu-terminal
```

Chapter 19 Port Aggregation Commands

19.1 Port Aggregation Commands

19.1.1 aggregator-group

Syntax

To configure port aggregation, run aggregator-group id mode {lacp-negotiation |static }. To resume the default settings, run no aggregator-grou.

aggregator-group *id* mode {lacp |static }

no aggregator-group

Parameters

Parameters	Description
id	Stands for the ID of a logistic port. Value range: 1-32
lacp	Enables LACP negotiation.
static	Disables port negotiation.

Default Value

The port is not aggregated.

Usage Guidelines

Port's link aggregation is to bind several ports of same attributes into a logic port. The binding process is conducted through LACP negotiation or is mandatorily conducted without any negotiation.

If the static aggregation is used, please make sure the attribute of the ports to be binded is the same and vlan attribute is consisted.

When configuring port aggregation, you can select the LACP negotiation mode. In Active mode, the port will transmit the LACP packet actively for LACP negotiation; In passive mode, the port responds to the LACP packets passively and conducts the LACP negotiation passively.

Some models of switches do not support the dynamic negotiation mode, hence, the corresponding configuration command is not provided.

Command Mode

Port configuration mode

Example

The following example shows how to bind port g0/1 and port g0/2 to logic port port-aggregator 3, and then to use LACP negotiation.

```
Switch_config_g0/1# aggregator-group 3 mode lacp

Switch_config_g0/1# interface g0/2

Switch_config_g0/2# aggregator-group 3 mode lacp
```

19.1.2 aggregator-group load-balance

Syntax

aggregator-group load-balance { dst-mac| src-mac| both-mac }

no aggregator-group load-balance

To configure load balance after port aggregation, run aggregator-group load-balance { dst-mac| src-mac| both-mac | src-ip | dst-ip | both-ip }. To resume the default settings, run no aggregator-group load-balance.

Parameters

Parameters	Description
dst-mac	Means taking the destination MAC address as the standard.
src-mac	Means taking the source MAC address as the standard.
both-mac	Means taking the destination/source MAC address as the standard.

Default Value

scr-mac

Usage Guidelines

To ensure each physical port to reach load balance after port aggregation, you need averagely distribute data flow on each physical port. This command can help reaching this function.

When the dst-mac mode is chosen, the distributed data flow takes the destination mac address of the data packet as the standard. Packets with a same MAC address are transmitted from just one physical port. However, the SRC-MAC mode takes the source mac address as the standard.

Switches of different models have different load balance policies. Only the load balance policy is displayed in the command prompt. If no load balance policies is supported or only one load balance policy is supported, the related sub-command will not be displayed.

Command Mode

Port configuration mode

Example

The following example shows how to change the load balance mode of port-aggregator to the src-mac mode.

```
Switch_config# int port-aggregator 1

Switch_config_p1#

Switch_config_p1# aggregator-group load-balance src-mac
```

19.1.3 show aggregator-group

Syntax

show aggregator-group [*id*] {detail|brief|summary}

To display the detailed information about the aggregator-group, run the following command.

Parameters

Parameters	Description
id	IDof a specific logic port

Default Value

None

Usage Guidelines

This command is used to display the information about port aggregation.

Command Mode

EXEC

19.1.4 show interface port-aggregator

Syntax

To display the detailed information about the aggregator-group, run the following command.

show interface port-aggregator *id*

Parameters

Parameters	Description
id	ID of a specific port

Default Value

None

Usage Guidelines

This command is used to display the information about port aggregation.

Command Mode

EXEC

Example

The following example shows how to display the information about aggregated port 1.

```
Switch#show interface port-aggregator 1
Port-aggregator1 is down, line protocol is down
Hardware is Port Aggregator, Address is 0000.0000.0000(0000.0000.0000)
MTU 1500 bytes, BW 1000 kbit, DLY 2000 usec
Encapsulation ARPA, loopback not set
Members in this Aggregator:
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 multicasts
0 input errors, 0 input discards
0 CRC, 0 frame, 0 overrun, 0 ignored
0 packets output, 0 bytes, 0 underruns
Transmited 0 broadcasts, 0 multicasts
0 output errors, 0 discards
0 output buffer failures, 0 output buffers swapped out
```

NOTE: Members in this Aggregator means physical ports which are aggregated to the logical port.

The statistics values are explained as follows:
Packets input means the input of all packets, including broadcast packets, multicast packets and unicast packets.
Bytes means the byte volume of all packets.
Broadcasts means received broadcast packets.
Broadcasts means received broadcast packets.
Input errors means received error packets.
Input discards means that the received packets are dropped, such as the received packets when the interface protocol is down.

Packets output means the output of all packets, including broadcast packets, multicast packets and unicast packets.
Bytes means the byte volume of all transmitted packets.
Broadcasts means transmitted broadcast packets.
Multicasts means transmitted multicast packets.
Output errors means transmitting error packets.
Output discards means that the transmitted packets are dropped, such as the transmitted packets when the interface protocol is down.

19.1.5 debug lacp errors

Syntax

debug lacp errors
no debug lacp errors
To export the LACP debugging error, run debug lacp errors.

Parameters

None

Default Value

None

Usage Guidelines

This command is used to export all error information occurred during LACP running. The error information can help locating the errors.

Command Mode

EXEC

Example

```
Switch# debug lacp errors
Switch#
```

19.1.6 debug lacp state

Syntax

debug lacp state

no debug lacp state

To export the information about the LACP state machine, run debug lacp state.

Parameters

None

Default Value

None

Command Mode

EXEC

Example

```
Switch# debug lacp state
Switch#
```

19.1.7 debug lacp packet

Syntax

debug lacp packet

no debug lacp packet

To export the information about LACP receiving or transmitting packets, run debug lacp packet.

Parameters

None

Default Value

None

Command Mode

EXEC

Example

```
Switch# debug lacp packet

Switch#
```

Chapter 20 Port Aggregation Commands

20.1 Port Aggregation Commands

20.1.1 aggregator-group

Syntax

To configure port aggregation, run aggregator-group id mode {lacp-negotiation |static }. To resume the default settings, run no aggregator-grou.

aggregator-group *id* mode {lacp |static }

no aggregator-group

Parameters

Parameters	Description
id	Stands for the ID of a logistic port. Value range: 1-32
lacp	Enables LACP negotiation.
static	Disables port negotiation.

Default Value

The port is not aggregated.

Usage Guidelines

Port's link aggregation is to bind several ports of same attributes into a logic port. The binding process is conducted through LACP negotiation or is mandatorily conducted without any negotiation.

If the static aggregation is used, please make sure the attribute of the ports to be binded is the same and vlan attribute is consisted.

When configuring port aggregation, you can select the LACP negotiation mode. In Active mode, the port will transmit the LACP packet actively for LACP negotiation; In passive mode, the port responds to the LACP packets passively and conducts the LACP negotiation passively.

Some models of switches do not support the dynamic negotiation mode, hence, the corresponding configuration command is not provided.

Command Mode

Port configuration mode

Example

The following example shows how to bind port g0/1 and port g0/2 to logic port port-aggregator 3, and then to use LACP negotiation.

```
Switch_config_g0/1# aggregator-group 3 mode lacp

Switch_config_g0/1# interface g0/2

Switch_config_g0/2# aggregator-group 3 mode lacp
```

20.1.2 aggregator-group load-balance

Syntax

aggregator-group load-balance { dst-mac| src-mac| both-mac }

no aggregator-group load-balance

To configure load balance after port aggregation, run aggregator-group load-balance { dst-mac| src-mac| both-mac | src-ip | dst-ip | both-ip }. To resume the default settings, run no aggregator-group load-balance.

Parameters

Parameters	Description
dst-mac	Means taking the destination MAC address as the standard.
src-mac	Means taking the source MAC address as the standard.
both-mac	Means taking the destination/source MAC address as the standard.

Default Value

scr-mac

Usage Guidelines

To ensure each physical port to reach load balance after port aggregation, you need averagely distribute data flow on each physical port. This command can help reaching this function.

When the dst-mac mode is chosen, the distributed data flow takes the destination mac address of the data packet as the standard. Packets with a same MAC address are transmitted from just one physical port. However, the SRC-MAC mode takes the source mac address as the standard.

Switches of different models have different load balance policies. Only the load balance policy is displayed in the command prompt. If no load balance policies is supported or only one load balance policy is supported, the related sub-command will not be displayed.

Command Mode

Port configuration mode

Example

The following example shows how to change the load balance mode of port-aggregator to the src-mac mode.

```
Switch_config# int port-aggregator 1

Switch_config_p1#

Switch_config_p1# aggregator-group load-balance src-mac
```

20.1.3 show aggregator-group

Syntax

show aggregator-group [*id*] {detail|brief|summary}

To display the detailed information about the aggregator-group, run the following command.

Parameters

Parameters	Description
id	IDof a specific logic port

Default Value

None

Usage Guidelines

This command is used to display the information about port aggregation.

Command Mode

EXEC

20.1.4 show interface port-aggregator

Syntax

To display the detailed information about the aggregator-group, run the following command.

show interface port-aggregator *id*

Parameters

Parameters	Description
id	ID of a specific port

Default Value

None

Usage Guidelines

This command is used to display the information about port aggregation.

Command Mode

EXEC

Example

The following example shows how to display the information about aggregated port 1.

```
Switch#show interface port-aggregator 1
Port-aggregator1 is down, line protocol is down
 Hardware is PortAggregator, Address is 0000.0000.0000(0000.0000.0000)
 MTU 1500 bytes, BW 1000 kbit, DLY 2000 usec
 Encapsulation ARPA, loopback not set
```

```
Members in this Aggregator:
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 multicasts
0 input errors, 0 input discards
0 CRC, 0 frame, 0 overrun, 0 ignored
0 packets output, 0 bytes, 0 underruns
Transmited 0 broadcasts, 0 multicasts
0 output errors, 0 discards
0 output buffer failures, 0 output buffers swapped out
```

NOTE: Members in this Aggregator means physical ports which are aggregated to the logical port.

The statistics values are explained as follows:
Packets input means the input of all packets, including broadcast packets, multicast packets and unicast packets.
Bytes means the byte volume of all packets.
Broadcasts means received broadcast packets.
Broadcasts means received broadcast packets.
Input errors means received error packets.
Input discards means that the received packets are dropped, such as the received packets when the interface protocol is down.

Packets output means the output of all packets, including broadcast packets, multicast packets and unicast packets.
Bytes means the byte volume of all transmitted packets.
Broadcasts means transmitted broadcast packets.
Multicasts means transmitted multicast packets.
Output errors means transmitting error packets.
Output discards means that the transmitted packets are dropped, such as the transmitted packets when the interface protocol is down.

20.1.5 debug lacp errors

Syntax

debug lacp errors
no debug lacp errors
To export the LACP debugging error, run debug lacp errors.

Parameters

None

Default Value

None

Usage Guidelines

This command is used to export all error information occurred during LACP running. The error information can help locating the errors.

Command Mode

EXEC

Example

```
Switch# debug lacp errors
Switch#
```

20.1.6 debug lacp state

Syntax

debug lacp state

no debug lacp state

To export the information about the LACP state machine, run debug lacp state.

Parameters

None

Default Value

None

Command Mode

EXEC

Example

```
Switch# debug lacp state
Switch#
```

20.1.7 debug lacp packet

Syntax

debug lacp packet

no debug lacp packet

To export the information about LACP receiving or transmitting packets , run debug lacp packet.

Parameters

None

Default Value

None

Command Mode

EXEC

Example

```
Switch# debug lacp packet

Switch#
```

Chapter 21 LLDP Configuration Commands

21.1 LLDP Commands

21.1.1 lldp run

Syntax

To enable LLDP, run lldp run; to disable LLDP, run no lldp run.

lldp run

no lldp run

Parameters

None

Default Value

The debugging switch is disabled.

Usage Guidelines

The port will send lldp packets after the lldp function is enabled.

Command Mode

Global configuration mode

Example

The following command is used to enable LLDP.

```
switch_config# lldp run
```

21.1.2 lldp holdtime

Syntax

To configure the ttl value of LLDP, run lldp holdtime time. To resume the default transmission delay, run no lldp holdtime.

Lldp holdtime time

no lldp holdtime

Parameters

Parameters	Description
time	Holdtime of the to-be-transmitted packet Range: 0-65535 seconds

Default Value

120s

Usage Guidelines

In normal condition, the remote information stored in MIB will update before aging. But the frame may loss in sending and causes the information ages. For avoiding this, you need to set the value of TTL and ensure the update LLDP frame is forwarded time after time.

Command Mode

Global configuration mode

Example

The following example shows how to set the ttl value of LLDP to 100 seconds.

```
switch_config# lldp  holdtime 100
switch_config#
```

21.1.3 lldp timer

Syntax

To configure the transmission delay of LLDP, run lldp timer time. To resume the default transmission delay, run no lldptimer.

lldp timer *time*

no lldp timer

Parameters

Parameters	Description
time	Interval for LLDP to transmit the packets Range: 5-65534 seconds

Default Value

30s

Usage Guidelines

The transmission interval of the LLDP message must be shorter than its storage time, ensuring multiple updates in the storage time and preventing error which is led by packet loss.

Command Mode

Global configuration mode

Example

The following example shows how to configure the transmission interval of LLDP to 24 seconds.

```
switch_config# lldp  timer  24
switch_config#
```

21.1.4 lldp reinit

Syntax

To configure the transmission delay of LLDP, run lldp reinit time. To resume the default transmission delay, run no lldp reinit.

lldp reinit *time*

no lldp reinit

Parameters

Parameters	Description
time	Transmission delay of LLDP, whose values range from two to five seconds Range: 2-5 seconds

Default Value

2s

Usage Guidelines

LLDP information will be forwarded automatically in two conditions: first, the status or value of one or more information elements (management objects) change; second, the sending timer timeouts. A single information change cause the LLDP packet is forwarded and a series of information change may cause many LLDP frames forwarded, but a frame can only report one change. For avoiding this, the web management defines the interval of two continuous LLDP frames.

Command Mode

Global configuration mode

Example

The following example shows how to set the transmission delay of LLDP to five seconds.

```
switch_config# lldp reinit 5
switch_config#
```

21.1.5 lldp tlv-select

Syntax

To add TLV which is transmitted by the LLDP message, run lldp med-tlv-select tlv-type. To delete TLV which is transmitted by the LLDP message, run no lldp med-tlv-select tlv-type.

lldp tlv-select *tlv-type*

no lldp tlv-select *tlv-type*

Parameters

Parameters	Description	
tlv-type	Stands for TLV that are available for selective transmission. Its values are:	
	management-address	management address TLV
	port-description	port description TLV
	system-capabilities	system-capabilities TLV
	system-description	system description TLV
	system-name	system name TLV

Default Value

All TLVs are sent.

Usage Guidelines

Three mandatory TLVs must be sent.

Command Mode

Global configuration mode

Example

The following example shows how to enable the port description not to be transmitted in the message.

```
switch_config#no lldp tlv-select port-description
switch_config#
```

21.1.6 lldp dot1-tlv-select

Syntax

To add TLV which is transmitted by the LLDP message, run lldp med-tlv-select tlv-type. To delete TLV which is transmitted by the LLDP message, run no lldp med-tlv-select tlv-type.

lldp dot1-tlv-select *tlv-type*

no lldp dot1-tlv-select *tlv-type*

Parameters

Parameters	Description	
tlv-type	Stands for TLV that are available for selective transmission. Its values are:	
	port-vlan-id	port vlan address TLV
	protocol-vlan-id	port and protocol VLAN ID TLV
	vlan-name	vlan name TLV

Default Value

All TLVs are sent.

Usage Guidelines

The TLV of the protocol identity does not support transmission but supports reception.

Command Mode

Port configuration mode

Example

The following example shows how to enable the TLV not to be transmitted by deletion of the VLAN address of a port in the transmitted packet.

```
switch_config#int g0/1
switch_config_g0/1#no lldp dot1-tlv-select port-vlan-id
switch_config_g0/1#
```

21.1.7 lldp dot3-tlv-select

Syntax

To add TLV which is transmitted by the LLDP message, run lldp med-tlv-select tlv-type. To delete TLV which is transmitted by the LLDP message, run no lldp med-tlv-select tlv-type.

lldp dot3-tlv-select *tlv-type*

no lldp dot3-tlv-select *tlv-type*

Parameters

Parameters	Description	
tlv-type	Stands for TLV that are available for selective transmission. Its values are:	
	link-aggregation	link aggregation TLV
	macphy-confg	MAC/Phy configuration/status TLV
	max-frame-size	max frame size TLV
	power	Power Via MDI TLV

Default Value

All TLVs are sent.

Usage Guidelines

None

Command Mode

Port configuration mode

Example

The following example shows how to enable the TLV not to be transmitted by deletion of the MAC/Phy configuration/status of a port in the transmitted packet.

```
switch_config#int g0/1
switch_config_g0/1#no  lldp  dot3-tlv-select  macphy-confg
switch_config_g0/1#
```

21.1.8 lldp med-tlv-select

Syntax

To add TLV which is transmitted by the LLDP message, run lldp med-tlv-select tlv-type. To delete TLV which is transmitted by the LLDP message, run no lldp med-tlv-select tlv-type.

lldp med-tlv-select *tlv-type*

no lldp med-tlv-select *tlv-type*

Parameters

Parameters	Description	
tlv-type	Stands for TLV that are available for selective transmission. Its values are:	
	network-policy	network policy TLV
	inventory	inventory management TLV
	location	location identification TLV
	power-management	expand Power Via MDI TLV

Default Value

All TLVs are sent.

Usage Guidelines

By default, the TLV of MED cannot be transmitted. When the TLV of MED need be transmitted, the MED capability TLV must be transmitted. Hence it does not fall into the choice.

Command Mode

Port configuration mode

Example

The following example shows how to enable the TLV not to be transmitted by deletion of the detailed list management in a transmitted packet.

```
switch_config#int g0/1
switch_config_g0/1#no  lldp  med-tlv-select  inventory
switch_config_g0/1#
```

21.1.9 lldp transmit

Syntax

lldp transmit

no lldp transmit

To set the port to send the LLDP message, run lldp transmit. To forbid receiving the LLDP message, run no lldp transmit.

Parameters

None

Default Value

Transmittable LLDP message mode

Usage Guidelines

Only after the LLDP module is enabled can the command be valid.

Command Mode

Port configuration mode

Example

The following example shows how to set port g0/1 not to send the LLDP message.

```
switch_config_g0/1# no lldp transmit
switch_config_g0/1#
```

21.1.10 lldp receive

Syntax

lldp receive

no lldp receive

To set the port to the receivable LLDP message mode, run lldp receive. To forbid receiving the LLDP message, run no lldp receive.

Parameters

None

Default Value

Receivable LLDP message mode

Usage Guidelines

Only after the LLDP module is enabled can the configuration be valid.

Command Mode

Port configuration mode

Example

The following example shows how to set port g0/1 not to receive the LLDP message.

```
switch_config_g0/1# no lldp receive
switch_config_g0/1#
```

21.1.11 lldp management-ip

Syntax

lldp management-ip *A.B.C.D*

no lldp management-ip

To configure the management address of the LLDP port, run lldp management-ip A.B.C.D. To resume the default transmission delay, run no lldp management-ip.

Parameters

Parameters	Description
A.B.C.D	Stands for the management IP address that will be specified.

Default Value

The default management address is the IP address of the VLAN interface that pvid corresponds to; if this IP address does not exist, the default management address is 0.0.0.0.

Usage Guidelines

The configured management IP address should be the IP address related with a port.

Command Mode

Port configuration mode

Example

The following example shows how to set the management IP address of port g0/1 to 90.0.0.99.

```
switch_config_g0/1# lldp  management-ip 90.0.0.99
switch_config_g0/1#
```

21.1.12 lldp trap-send

Syntax

lldp tranp-sendlldp-mib

To forward trap notification to lldp mib, run this command.

lldp tranp-sendptopo-mib

To forward trap notification to ptopo mib, run this command.

Parameters

None

Default Value

None

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to send trap notification to lldp mib.

```
switch_config#lldp trap-send lldp-mib
switch_config#
```

The following example shows how to send trap notification to ptopo mib.

```
switch_config#lldp trap-send ptopo-mib
switch_config#
```

21.1.13 location elin identifier id WORD

Syntax

location elin identifier *id WORD*

no location elin identifier *id*

To add the elin information, run location elin identifier id WORD; to delete the elin information, run no location elin identifier id.

Parameters

Parameters	Description
id	Stands for the ID of the to-be-set elin, which ranges from 1 to 65535.
WORD	Stands for the content of the configured elin, which ranges from 10 to 25 bytes.

Default Value

None

Usage Guidelines

None

Command Mode

Global configuration mode

Example

The following example shows how to set the identifier to 1 and the content of elin to 1234567890.

```
switch_config# location elin identifier 1 1234567890
switch_config#
```

21.1.14 location civic identifier id

Syntax

location civic identifier *id*

no location civic identifier *id*

To enter the location configuration mode and set the civic information, run location civic identifier id. To delete the civic information, run no location civic identifier id.

Parameters

Parameters	Description
id	Stands for the ID of the to-be-set civic, which ranges from 1 to 65535.

Default Value

None

Usage Guidelines

After the system enters the location configuration mode, you can run the following commands to conduct the corresponding configuration to the civic of the ID.

Command	Purpose
(no) language WORD	Sets the language.
(no) state WORD	Sets the state's (provincial) name, such as shanghai.
(no) county WORD	Sets the name of a county.
(no) city WORD	Sets the name of a city.
(no) division WORD	Sets the name of a division.
(no) neighborhood WORD	Sets the name of neighborhood.
(no) street WORD	Sets the name of a street.
(no) leading-street-dir WORD	Sets the direction of a main street, such as N (north).
(no) trailing-street-suffix WORD	Sets the suffix of a small street, such as SW.
(no) street-suffix WORD	Sets the suffix of a street, such as platz.
(no) number WORD	Sets the street number, such as number 123.
(no) street-number-suffix WORD	Sets the suffix of the street number, such as number 1/2 of A road.
(no) landmark WORD	Sets the landmark, such as Colombia University.
(no) additional-location WORD	Sets the additional location.
(no) name WORD	Sets the information about a resident, such as Joe's haircut shop.
(no) postal-code WORD	Sets the postal code.
(no) building WORD	Sets the information about a building.
(no) unit WORD	Sets the information about a unit.
(no) floor WORD	Sets the information about a floor.
(no) room WORD	Sets the information about a room.
(no) type-of-place WORD	Sets the type of a place, such as office.
(no) postal-community WORD	Sets the name of a postal office.
(no) post-office-box WORD	Sets the name of a postal box, such as 12345.
(no) additional-code WORD	Sets the additional code.
(no) country WORD	Sets the name of a country.
(no) script WORD	Sets the script.

Command Mode

Global configuration mode

Example

The following example shows how to set the civic information of identifier 1.

```
Switch_config#location civic identifier 1
Switch_config_civic#language English
Switch_config_civic#city Shanghai
Switch_config_civic#street Curie
Switch_config_civic#script EN
Switch_config_civic#quit
Switch_config#
```

21.1.15 location elin/civic id

Syntax

location elin/civic *id*

no location elin/civic

To set the location for a port, run location elin/civic id. To delete the location of a port, run no location elin/civic id.

Parameters

Parameters	Description
id	Stands for the ID of the to-be-set elin/civic, which ranges from 1 to 65535.

Default Value

None

Usage Guidelines

None

Command Mode

Port configuration mode

Example

The following example shows how to set the elin and the civic for a port.

```
Switch_config#int g0/8
Switch_config_g0/8#location elin 1
Switch_config_g0/8#location civic 1
```

21.1.16 show lldp errors

Syntax

show lldp errors

To display the error information about the LLDP module, run this command.

Parameters

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC/global configuration mode

Example

The following example shows how to check the error information of lldp module.

```
switch_config#show lldp errors
LLDP errors/overflows:
        Total memory allocation failures: 0
        Total encapsulation failures: 0
        Total table overflows: 0
switch_config#
```

21.1.17 show lldp interface

Syntax

show lldp interface *interface-name*

To check the transmission and reception mode, run show lldp interface interface name.

Parameters

Parameters	Description
interface-name	The interrface name, for instance, "G0/1", "GigaEthernet0/1".

Default Value

None

Usage Guidelines

Only when lldp is enabled can the state of the port, the transmission and reception mode of lldp packets can be checked.

Command Mode

EXEC/global configuration mode

Example

The following example shows how to check the transmission and reception mode of port g0/1.

```
switch_config#show lldp interface g0/1
GigaEthernet0/1:
Rx: enabled
Tx: enabled
switch_config#
```

21.1.18 show lldp neighbors

Syntax

show lldp neighbors

To display the simple information about neighbors, run this command.

Parameters

None

Default Value

None

Usage Guidelines

The command is used to display the simple information about neighbor list, including Device-ID, Local-Intf, Hldtme, Port-ID and Capability.

Command Mode

EXEC/global configuration mode

Example

```
switch_config#show lldp neighbors
Capability Codes:
        (R)Router,(B)Bridge,(C)DOCsIs Cable Device,(T)Telephone
        (W)WLAN Access Point, (P)Repeater,(s)station,(O)Other

Device-ID       Local-Intf      Hldtme      Port-ID      Capability
switch          Gig0/2          115         Gig0/32      B
switch          Gig0/32         114         Gig0/2       B

Total entries dispalyed: 2
switch_config#
```

21.1.19 show lldp neighbors detail

Syntax

show lldp neighbors detail

It is used to display the detailed information about the neighbor.

Parameters

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC/global configuration mode

Example

```
switch_config#show lldp neighbors detail

chassis id: 00e0.0f61.ca53
port id: Gig0/32
port description: GigaEthernet0/32
system name: switch

system description: s3448 software, Version 2.0.1K
serial: s35000456
Compiled: 2008-11-13 13:33:36 by 16170F032B9F

Time remaining: 98
system capabilities: R B
enabled capabilities: B
Managment Address:
    IP: 192.168.213.62

Auto Negotiation -- supported,enabled
Physical media capabilitise:
    100baseTX(FD)
    100baseTX(HD)
    10baseT(FD)
    10baseT(HD)
Media Attachment Unit type: 16

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

chassis id: 00e0.0f61.ca35
port id: Gig0/2
port description: GigaEthernet0/2
system name: switch

system description: s3448 software, Version 2.0.1K
serial: s35000456
Compiled: 2008-11-13 13:33:36 by 16170F032B9F

Time remaining: 95
system capabilities: R B
enabled capabilities: B
Managment Address:
    IP: 90.0.0.66

Auto Negotiation -- supported,enabled
Physical media capabilitise:
    100baseTX(FD)
    100baseTX(HD)
    10baseT(FD)
    10baseT(HD)
Media Attachment Unit type: 16

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


Total entries dispalyed: 2
switch#
```

21.1.20 show lldp traffic

Syntax

show lldp traffic

To display all statistics information about LLDP, run show lldp traffic.

Parameters

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC/global configuration mode

Example

```
switch_config#show lldp traffic
LLDP traffic statistics:
    Total frames out: 1599
    Total entries aged: 0
    Total frames in: 624
    Total frames received in error: 0
    Total frames discarded: 0
    Total TLVs unrecognized: 0
switch_config#
```

21.1.21 show location elin

Syntax

show location elin

To display the elin configuration of the location, run the previous command.

Parameters

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC/global configuration mode

Example

```
Switch_config#show location elin
elin information:
```

```
   elin 2: 0987654321
   elin 1: 1234567890
total: 2
Switch_config#
```

21.1.22 show location civic [identifier *id*]

Syntax

show location civic [identifier *id*]

To display the civic information of the location, run the previous command.

Parameters

Parameters	Description
id	Stands for the ID of the to-be-set civic, which ranges from 1 to 65535.

Default Value

None

Usage Guidelines

None

Command Mode

EXEC/global configuration mode

Example

```
Switch_config#show location civic
civic address information:
   identifier: 2
   Language: Chinese
   Script: CN
-------------------------------------
   identifier: 1
   City: Shanghai
   Language: English
   Script: EN
-------------------------------------
total: 2
Switch_config#
```

21.1.23 clear lldp counters

Syntax

clear lldp counters

To clear the statistics information, run clear lldp counters.

Parameters

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC

Example

```
switch#clear lldp counters
switch#
switch#show lldp traffic
LLDP traffic statistics:
        Total frames out: 0
        Total entries aged: 0
        Total frames in: 0
        Total frames received in error: 0
        Total frames discarded: 0
        Total TLVs unrecognized: 0
switch#
switch#show lldp errors
LLDP errors/overflows:
        Total memory allocation failures: 0
        Total encapsulation failures: 0
        Total table overflows: 0
switch#
```

21.1.24 clear lldp table

Syntax

clear lldp table

To remove the neighbor list, run cleas lldp table.

Parameters

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC

Example

```
switch#clear lldp table
switch#
switch#show lldp neighbors
Capability Codes:
        (R)Router,(B)Bridge,(C)DOCsIs Cable Device,(T)Telephone
        (W)WLAN Access Point, (P)Repeater,(s)station, (O)Other
Device-ID       Local-Intf      Hldtme      Port-ID      Capability
Total entries displayed: 0
```

Chapter 22 Backuplink Configuration Commands

22.1 Global Commands

22.1.1 backup-link-group id

Syntax

To set the BackupLink group, run this command.

backup-link-group id

To delete the BackupLink group, use the no form of this command.

no backup-link-group id

Parameters

Parameters	Description
Id	Stands for the instance ID of the backuplink group.

Default Value

The backuplink group is not configured by default.

Command Mode

Global configuration mode

Usage Guidelines

None

Example

```
Switch_config#backup-link-group 1
Switch_config#
```

Related Command

None

22.1.2 backup-link-group id preemption-mode forced {delay value}

Syntax

To set the port-based preemption mode for the backuplink group, run this command.

backup-link-group id preemption-mode forced {delay value}

To delete the port-based preemption mode for the backuplink group, run the following command:

no backup-link-group id

Parameters

Parameters	Description
Id	Stands for the instance ID of the backuplink group.
value	Stands for the delay time.

Default Value

The backuplink group has not been set with the trait of port-based preemption by default.

Command Mode

Global configuration mode

Usage Guidelines

The command **backup-link-group** *id* **preemption-mode forced {delay** *value***}** can be used to create BackupLink group directly.

Example

```
Switch_config#backup-link-group 1 preemption-mode forced delay 5
Switch_config#
```

Related Command

```
backup-link-group id
backup-link-group id preemption-mode bandwidth {delay value}
```

22.1.3 backup-link-group id preemption-mode bandwidth {delay value}

Syntax

To set port bandwidth preemption mode for the backuplink group, run the following command:

backup-link-group id preemption-mode bandwidth **{**delay value**}**

To delete port bandwidth preemption mode for the backuplink group, run the following command:

no backup-link-group id

Parameters

Parameters	Description
Id	Stands for the instance ID of the backuplink group.
value	Stands for the delay time.

Default Value

The backuplink group has not been set with the trait of port bandwidth preemption by default.

Command Mode

Global configuration mode

Usage Guidelines

None

Example

```
Switch_config#backup-link-group 1 preemption-mode bandwidth delay 5
Switch_config#
```

Related Command

```
backup-link-group id
backup-link-group id preemption-mode forced {delay value}
```

22.1.4 monitor-link-group id

Syntax

To set the MonitorLink group, run the following command:

```
monitor-link-group id
```

To delete the MonitorLink group, run the following command:

```
no monitor-link-group id
```

Parameters

Parameters	Description
Id	Stands for the instance ID of the monitorlink group.

Default Value

The MonitorLink group is not configured by default.

Command Mode

This command is run in global configuration mode.

Usage Guidelines

None

Example

```
Switch _config# monitor-link-group 1
Switch_config#
```

Related Command

None

22.2 Port Configuration Commands

22.2.1 backup-link-group id active

Syntax

To set a port to be an active port, run the following command:

backup-link-group id active

To cancel the primary port configuration of a port, run the following command:

no backup-link-group id

Parameters

Parameters	Description
Id	Stands for the instance ID of the backuplink group.

Default Value

The primary port is not configured by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

If the backuplink group is not established, it will be automatically created when you configure the backuplink group on a port directly.

Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#backup-link-group 1 active
Switch_config_g0/1#exit
```

Related Command

```
backup-link-group id
backup-link-group id backup
```

22.2.2 backup-link-group id backup

Syntax

To set a port to be a backup port, run the following command:

backup-link-group id backup

To cancel the edge port configuration of a port, run the following command:

no backup-link-group id

Parameters

Parameters	Description
Id	Stands for the instance ID of the backuplink group.

Default Value

The backup port is not configured by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

If the backuplink group is not established, it will be automatically created when you configure the backuplink group on a port directly.

Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#backup-link-group 1 backup
Switch_config_g0/1#exit
```

Related Command

```
backup-link-group id
backup-link-group id active
```

22.2.3 share-load vlan vlanmap

Syntax

To set VLAN load balance for the backup port, run the following command:

```
share-load vlan vlanmap
```

To delete VLAN load balance for the backup port, run the following command:

```
no share-load vlan
```

Parameters

Parameters	Description
vlanmap	Stands for the VLAN value.

Default Value

VLAN load balance is not set for the backup port by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

This command can be set only on the backup port, that is, a port must be set to be a backup port before VLAN load balance is set on the port.

For different BackupLink groups, the same group VLAN can be configured, or they have overlapping VLAN segments. If there are overlapped VLAN segments, the system will classify these VLANs into different MSTs (STGs) and conduct operations toward a group of ports, the statuses of these ports in different MSTs vary. So, typically, when the load balancing VLAN group is configured, it is better to select the VLAN group without overlapping.

Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1# share-load vlan 100-200
Switch_config_g0/1#exit
```

Related Command

```
backup-link-group id
backup-link-group id backup
```

22.2.4 backup-link-group mmu transmit

Syntax

To set MMU transmission for the ports of the backuplink group, run the following command:

```
backup-link-group mmu transmit
```

To delete MMU transmission for the ports of the backuplink group, run the following command:

```
no backup-link-group mmu
```

Parameters

None

Default Value

The MMU transmission function for the ports of the backuplink group is not set by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

Only the ports of the backuplink group can be set to transmit, that is, the ports must be set to active or backup.

Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#backup-link-group mmu transmit
Switch_config_g0/1#exit
```

Related Command

```
backup-link-group id
```

22.2.5 backup-link-group mmu receive

Syntax

To set MMU reception for ports, run the following command:

```
backup-link-group mmu receive
```

To delete MMU reception for ports, run the following command:

```
no backup-link-group mmu
```

Parameters

None

Default Value

The MMU reception function for the ports is not set by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

The ports that are set to receive are not necessarily the ports of the backuplink group.

Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#backup-link-group mmu receive
Switch_config_g0/1#exit
```

Related Command

None

22.2.6 monitor-link-group id uplink

Syntax

To set a port to be an uplink port, run the following command:

monitor-link-group id uplink

To cancel the uplink port configuration, run the following command:

no monitor-link-group id

Parameters

Parameters	Description
Id	Stands for the instance ID of the monitorlink group.

Default Value

The uplink port is not configured by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

If the MonitorLink group port role is directly configured for the port in the case that the MonitorLink group is not established, the system will automatically create the MonitorLink group .

Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1# monitor-link-group 1 uplink
Switch_config_g0/1#exit
```

Related Command

```
monitor-link-group id
monitor-link-group id downlink
```

22.2.7 monitor-link-group id downlink

Syntax

To set a port to be a downlink port, run the following command:

```
monitor-link-group id downlink
```

To cancel the downlink port configuration, run the following command:

```
no monitor-link-group id
```

Parameters

Parameters	Description
Id	Stands for the instance ID of the monitorlink group.

Default Value

The downlink port is not configured by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

If the MonitorLink group port role is directly configured for the port in the case that the MonitorLink group is not established, the system will automatically create the MonitorLink group .

Example

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1# monitor-link-group 1 downlink
Switch_config_g0/1#exit
```

Related Command

```
monitor-link-group id
monitor-link-group id uplink
```

22.3 Show

22.3.1 show backup-link-group id

Syntax

To display the information about the backuplink group, run the following command:

show backup-link-group id

Parameters

Parameters	Description
Id	Stands for the instance ID of the backuplink group.

Default Value

None

Command Mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Usage Guidelines

None

Example

```
Switch_config# show backup-link-group 1
  Active Interface       Backup Interface       State                    Vlan State

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

  GigaEthernet0/2        GigaEthernet0/4        Forward/Block            Block/Block

  Share load vlan: 100-200,port[GigaEthernet0/4] vlan state: Forwarding
Preemption Mode: No Preempt
  Preemption Delay: 0 seconds
```

Related Command

None

22.3.2 show monitor-link-group id

Syntax

To configure the instance ID of the monitorlink group, run the following command.

show monitor-link-group id

Parameters

Parameters	Description
Id	Stands for the instance ID of the monitorlink group.

Default Value

None

Command Mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Usage Guidelines

None

Example

```
Switch_config#show monitor-link-group 1
uplink interface: GigaEthernet0/2       Forwarding
downlink interface:
GigaEthernet0/1       Forwarding
GigaEthernet0/3       Forwarding
```

Related Command

None

Chapter 23 EAPS Configuration Commands

23.1 Global Commands

23.1.1 ether-ring

To set an instance of ring and enter the node mode, run the following command:

ether-ring *id*

To cancel an instance of ring, run the following command:

no ether-ring *id*

Parameters

Parameters	Description
id	ID of the node

Default Value

By default, the ring node is not configured.

Command Mode

Global configuration mode

Usage Guidelines

STP should not be disabled before the configuration of node instance.

Example

```
S1_config#ether-ring 1
S1_config_ring1#
```

Related Command

None

23.1.2 control-vlan

To set the control VLAN of the ring node, run the following command:

control-vlan *vlan-id*

Parameters

Parameters	Description
vlan-id	ID of the control VLAN Value range: 1-4094

Default Value

By default, the control VLAN of a node is not configured.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. Any VLAN can be configured as the control VLAN of the node. If you specify the control VLAN, the system VLAN will be created consequently. The user doesn't need to create the system VLAN manually.

2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the Ethernet ring has already been started.

Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
```

Related Command

ether-ring

master-node

transit-node

23.1.3 master-node

To configure an Ethernet ring as a master node, run the following command:

master-node

Parameters

None

Default Value

By default, the node type is not configured.

Command Mode

Node configuration mode

Usage Guidelines

1. A node can be set to be a master node or a transit node.

2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the node of the Ethernet ring has already been started.

Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#master-node
```

Related Command

control-vlan

transit-node

23.1.4 transit-node

To configure the node type to be a transit node, run the following command.

transit-node

Parameters

None

Default Value

By default, the node type is not configured.

Command Mode

Node configuration mode

Usage Guidelines

1. A node can be set to be a master node or a transit node.

2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the node of the Ethernet ring has already been started.

Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#transit-node
```

Related Command

control-vlan

master-node

23.1.5 hello-time

To configure the cycle for the master node to transmit the HEALTH packets of the Ethernet ring, run the following command:

hello-time *value*

To resume the default value of the cycle, run the following command:

no hello-time

Parameters

Parameters	Description
value	Stands for a time value, whose unit is second. The default value is one second. The value ranges between 1 and 10 seconds.

Default Value

By default, the hello-time is one second.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The hello-time configuration validates only on the master node.

2. By default, the value of the hello-time is smaller than that of the fail-time, which avoids the Ethernet ring protocol from being shocked. The hello-time needs to modify after modifying fail-time.

Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#master-node
S1_config_ring1#hello-time 2
```

Related Command

fail-time

23.1.6 fail-time

To configure the time cap of waiting for the HEALTH packets for the secondary port of the master node, run the following command:

fail-time *value*

To resume the default value of the fail-time, run the following command:

no fail-time

Parameters

Parameters	Description
value	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 3 and 30 seconds.

Default Value

By default, the fail-time is 3 seconds.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The fail-time configuration validates only on the master node.

2. By default, the value of the fail-time is triple of the hello-time, which avoids the Ethernet ring protocol from being shocked. The hello-time needs to modify after modifying fail-time.

Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#master-node
S1_config_ring1#hello-time 2
S1_config_ring1#fail-time 6
```

Related Command

hello-time

23.1.7 pre-forward-time

To configure the time of maintaining the pre-forward state on the transit port, run the following command.

pre-forward-time *value*

To resume the default value of the pre-forward-time, run this command.

no pre-forward-time

Parameters

Parameters	Description
value	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 3 and 30 seconds.

Default Value

By default, the pre-forward-time is 3 seconds.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The pre-forward-time configuration validates only on the transit node.

2. By default, the pre-forward-time on the transit node is triple the value of the hello-time on the master node, which avoids the network loop from being occurred after the transmission link recovers from disconnection. After the hello-time of the master node is modified, the corresponding pre-forward-time on the transit node need be adjusted.

Example

```
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
S1_config_ring1#transit-node
S1_config_ring1#pre-forward-time 8
```

Related Command

None

23.2 Port Configuration Commands

23.2.1 ether-ring primary-port

To set a port to be the primary port of a master node, run the following command:

ether-ring *id* **primary-port**

To cancel the primary port configuration of a port, run the following command:

no ether-ring *id* **primary-port**

Parameters

Parameters	Description
id	ID of the node

Default Value

The primary port is not configured by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

Usage Guidelines

The primary port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type is the master node.

Example

```
S1_config#interface GigaEthernet 0/1
S1_config_g0/1#ether-ring 1 primary-port
S1_config_g0/1#exit
```

Related Command

master-node

ether-ring secondary-port

23.2.2 ether-ring secondary-port

To set a port to be the secondary port of a master node, run the following command:

ether-ring *id* **secondary-port**

To cancel the secondary port configuration, run the following command:

no ether-ring *id* **secondary-port**

Parameters

Parameters	Description
id	ID of the node

Default Value

The secondary port on the master node is not configured by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

Usage Guidelines

The primary port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type is the master node.

Example

```
S1_config#interface GigaEthernet 0/3
S1_config_g0/3#ether-ring 1 secondary-port
S1_config_g0/3#exit
```

Related Command

master-node

ether-ring primary-port

23.2.3 ether-ring transit-port

To set a port to be the transit port of a transit node, run the following command:

ether-ring *id* **transit-port**

To cancel the transit port, run the following command:

no ether-ring *id* **transit-port**

Parameters

Parameters	Description
id	ID of the node

Default Value

The transit port on the transit node is not configured by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Note: The versions of switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

Usage Guidelines

The transit port can be configured only after the control VLAN and node type of the Ethernet ring are configured, and when the node type must be the transit node. Two transit ports can be configured on one transit node.

Example

```
S1_config_ring1#exit
S1_config#interface GigaEthernet 0/1
S1_config_g0/1#ether-ring 1 transit-port
S1_config_g0/1#exit
S1_config#interface GigaEthernet 0/3
S1_config_g0/3#ether-ring 1 transit-port
S1_config_g0/3#exit
```

Related Command

transit-node

23.3 Show

23.3.1 show ether-ring

To display the summary information about the Ethernet-ring node, run the following command:

show ether-ring *id*

To display the detailed information about the Ethernet-ring node, run the following command:

show ether-ring *id* **detail**

To display the information about the Ethernet-ring port, run the following command:

show ether-ring *id* **interface** *intf-name*

To display all summary information about the Ethernet-ring node, run the following command:

show ether-ring <cr>

Parameters

Parameters	Description
id	ID of the node
intf-name	Name of an interface

Default Value

None

Command Mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Usage Guidelines

None

Example

None

Related Command

None

Chapter 24 MEAPS Configuration Commands

24.1 Global Commands

24.1.1 mether-ring *id1* domain *id2*

To set an instance of ring and enter the node mode, run the following command:

mether-ring *id1* **domain** *id2*

To cancel an instance of ring, run the following command:

no mether-ring *id1* **domain** *id2*

Parameters

Parameters	Description
Id1	Stands for the node instance ID, which ranges from 0 to 7.
Id2	Stands for the domain instance ID, which ranges from 0 to 3.

Default Value

By default, the ring node is not configured.

Command Mode

Global configuration mode

Usage Guidelines

If the configured domain is 0, that is **id2 is o,** *domain id2*can be omitted.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#
```

Related Command

None

24.1.2 master-node

To configure an Ethernet ring as a master node, run the following command:

master-node

Parameters

None

Default Value

By default, the node type is not configured.

Command Mode

Node configuration mode

Usage Guidelines

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.

2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#
```

Related Command

transit-node

edge-node

assistant-node

major-ring

sub-ring

control-vlan

24.1.3 transit-node

To configure the node type to be a transit node, run the following command.

transit-node

Parameters

None

Default Value

By default, the node type is not configured.

Command Mode

Node configuration mode

Usage Guidelines

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.

2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1# transit-node
S1_config_ring1#
```

Related Command

master-node

edge-node

assistant-node

major-ring

sub-ring

control-vlan

24.1.4 edge-node

To set the node type to be an edge node, run the following command:

edge-node

Parameters

None

Default Value

By default, the node type is not configured.

Command Mode

Node configuration mode

Usage Guidelines

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.

2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1# edge-node
S1_config_ring1#
```

Related Command

master-node

transit-node

assistant-node

major-ring

sub-ring

control-vlan

24.1.5 assistant-node

To set the node type to be an assistant edge node, run the following command:

assistant-node

Parameters

None

Default Value

By default, the node type is not configured.

Command Mode

Node configuration mode

Usage Guidelines

1. A node can be set to be a master node, a transit node, an edge node or an assistant node.

2. After the node type, the node ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node type can never be modified.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1# assistant-node
S1_config_ring1#
```

Related Command

master-node

transit-node

edge-node

major-ring

sub-ring

control-vlan

24.1.6 major-ring

To set the node ring's level to be the major ring node, run the following command:

major-ring

Parameters

None

Default Value

By default, the node ring's level is not configured.

Command Mode

Node configuration mode

Usage Guidelines

1. The node ring's level can only be set to one of the two levels: major-ring or sub-ring.

2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node ring's level can never be modified.

3. The edge node and the assistant node cannot be set to major ring.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1# transit-node
S1_config_ring1#major-ring
S1_config_ring1#
```

Related Command

master-node

transit-node

edge-node

assistant-node

sub-ring

control-vlan

24.1.7 sub-ring

To set the node ring's level to be the sub-ring node, run the following command:

sub-ring

Parameters

None

Default Value

By default, the node type is not configured.

Command Mode

Node configuration mode

Usage Guidelines

1. The node ring's level can only be set to one of the two levels: major-ring or sub-ring.

2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the node ring's level can never be modified.

3. If the edge node or the assistant node is set, they are regarded as sub-rings by default. Of course, you can set them not to be sub-rings.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#sub-ring
S1_config_ring1#
```

Related Command

master-node

transit-node

edge-node

assistant-node

major-ring

control-vlan

24.1.8 control-vlan

To set the control VLAN of the ring node, run the following command:

control-vlan *vlan-id*

Parameters

Parameters	Description
vlan-id	ID of the control VLAN Value range: 1-4094

Default Value

By default, the control VLAN of a node is not configured.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. You can set any VLAN to be the control VLAN of a node and at the same time the system will create the corresponding system VLAN and another control VLAN according to the ring level.

2. After the node type, the ring's level and ring control VLAN are set, you need to decide whether to exist from the ring configuration mode and enable the ring's node, for if you conduct the two actions, the ring control VLAN can never be modified.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#sub-ring
S1_config_ring1#control-vlan 2
S1_config_ring1#
```

Related Command

master-node

transit-node

edge-node

assistant-node

major-ring

sub-ring

24.1.9 single-subring-mode

To configure the edge node or assistant edge node and enter the single subring mode, run the following command.

single-subring-mode

Parameters

None

Default Value

Don't enter the single subring mode by default.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. Configuration of single-subring-node can only be effective in the edge node and the assistant edge node.

2. As in the single ring mode the subring protocol packet channel status detection on the main ring is not run, the dual-homing networking can't appear in the Ethernet ring.

Example

```
S1_config#mether-ring 1 domain 2
```

```
S1_config_ring1#edge-node
S1_config_ring1#control-vlan 2
S1_config_ring1#single-subring-mode
```

Related Command

None

24.1.10 hello-time

To configure the cycle for the master node to transmit the HEALTH packets of the Ethernet ring, run the following command:

hello-time *value*

To resume the default value of the cycle, run the following command:

no hello-time

Parameters

Parameters	Description
value	Stands for a time value, whose unit is second. The default value is one second. The value ranges between 3 and 10 seconds.

Default Value

By default, the hello-time is three seconds.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The hello-time configuration validates only on the master node.

2. By default, the value of the hello-time is smaller than that of the fail-time, which avoids the Ethernet ring protocol from being shocked. The hello-time needs to modify after modifying fail-time.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#sub-ring
S1_config_ring1#control-vlan 2
S1_config_ring1#hello-time 4
```

Related Command

fail-time

24.1.11 fail-time

To configure the time cap of waiting for the HEALTH packets for the secondary port of the master node, run the following command:

fail-time *value*

To resume the default value of the fail-time, run the following command:

no fail-time

Parameters

Parameters	Description
value	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 9 and 30 seconds.

Default Value

By default, the fail-time is 9 seconds.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The fail-time configuration validates only on the master node.

2. By default, the value of the fail-time is triple of the hello-time, which avoids the Ethernet ring protocol from being shocked. The hello-time needs to modify after modifying fail-time.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#master-node
S1_config_ring1#sub-ring
S1_config_ring1#control-vlan 2
S1_config_ring1#hello-time 4
S1_config_ring1#fail-time 12
```

Related Command

hello-time

24.1.12 pre-forward-time

To configure the time of maintaining the pre-forward state on the transit port, run the following command.

pre-forward-time *value*

To resume the default value of the pre-forward-time, run this command.

no pre-forward-time

Parameters

Parameters	Description
value	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 9 and 30 seconds.

Default Value

By default, the pre-forward-time is 9 seconds.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The pre-forward-time configuration validates only on the transit node.

2. By default, the pre-forward-time on the transit node is triple the value of the hello-time on the master node, which avoids the network loop from being occurred after the transmission link recovers from disconnection. After the hello-time of the master node is modified, the corresponding pre-forward-time on the transit node need be adjusted.

Example

```
S1_config#mether-ring 1 domain 2
S1_config_ring1#transit-node
S1_config_ring1#sub-ring
S1_config_ring1#control-vlan 2
S1_config_ring1#pre-forward-time 12
```

Related Command

None

24.2 Port Configuration Commands

24.2.1 mether-ring *id1* domain *id2* primary-port

To set a port to be the primary port of a master node, run the following command:

mether-ring *id1* **domain** *id2* **primary-port**

To cancel the primary port configuration of a port, run the following command:

no mether-ring *id1* **domain** *id2* **primary-port**

Parameters

Parameters	Description
Id1	ID of the node
Id2	ID of the domain

Default Value

The primary port is not configured by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

The primary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the master node.

If the configured domain is 0, that is**id2 is o,** *domain id2*can be omitted.

Example

```
S1_config#interface GigaEthernet 0/1
S1_config_g0/1# mether-ring 1 domain 2 primary-port
S1_config_g0/1#exit
```

Related Command

master-node

mether-ring id1 domain id2 secondary-port

24.2.2 mether-ring *id1* domain *id2* secondary-port

To set a port to be the secondary port of a master node, run the following command:

mether-ring *id1* **domain** *id2* **secondary-port**

To cancel the secondary port configuration, run the following command:

no mether-ring *id1* **domain** *id2* **secondary-port**

Parameters

Parameters	Description
Id1	ID of the node
Id2	ID of the domain

Default Value

The secondary port on the master node is not configured by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

The primary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the master node.

If the configured domain is 0, that is**id2 is o,** *domain id2*can be omitted.

Example

```
S1_config#interface GigaEthernet 0/3
S1_config_g0/3# mether-ring 1 domain 2 secondary-port
S1_config_g0/3#exit
```

Related Command

master-node

mether-ring id1 domain id2 primary-port

24.2.3 mether-ring *id1* domain *id2* transit-port

To set a port to be the transit port of a transit node, run the following command:

mether-ring *id1* **domain** *id2* **transit-port**

To cancel the transit port, run the following command:

no mether-ring *id1* **domain** *id2* **transit-port**

Parameters

Parameters	Description
Id1	ID of the node
Id2	ID of the domain

Default Value

The transit port on the transit node is not configured by default.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

The primary port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the transit node. Two transit ports can be configured on one transit node.

If the configured domain is 0, that is**id2 is o,** *domain id2*can be omitted.

Example

```
S1_config_ring1#exit
S1_config#interface GigaEthernet 0/1
S1_config_g0/1# mether-ring 1 domain 2 transit-port
S1_config_g0/1#exit
S1_config#interface GigaEthernet 0/3
S1_config_g0/3# mether-ring 1 domain 2 transit-port
S1_config_g0/3#exit
```

Related Command

transit-node

24.2.4 mether-ring *id1* domain *id2* common-port

To set a port to be a public port of an edge node (assistant edge node), run the following command:

mether-ring *id1* **domain** *id2* **common-port**

To cancel the public port, run the following command:

no mether-ring *id1* **domain** *id2* **common-port**

Parameters

Parameters	Description
Id1	ID of the node
Id2	ID of the domain

Default Value

By default, there is no configuration of the public port of an edge node.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

The public port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the edge node.

If the configured domain is 0, that is**id2 is o,** *domain id2*can be omitted.

Example

```
S1_config_ring1#exit
S1_config#interface GigaEthernet 0/1
S1_config_g0/1# mether-ring 2 domain 2 common-port
S1_config_g0/1#exit
```

Related Command

edge-node

assistant-node

mether-ring id1 domain id2 edge-port

24.2.5 mether-ring *id1* domain *id2* edge-port

To set a port to be an edge port of an edge node (assistant edge node), run the following command:

mether-ring *id1* **domain** *id2* **edge-port**

To cancel the edge port configuration of a port, run the following command:

no mether-ring *id1* **domain** *id2* **edge-port**

Parameters

Parameters	Description
Id1	ID of the node
Id2	ID of the domain

Default Value

By default, there is no configuration of the edge port of an edge node.

Command Mode

The physical port configuration mode and the converged port configuration mode

Usage Guidelines

The edge port can be configured only when the ring control VLAN, the ring's node type and the ring level are configured, and when the node type is the edge node.

If the configured domain is 0, that is**id2 is o,** *domain id2*can be omitted.

Example

```
S1_config_ring1#exit
S1_config#interface GigaEthernet 0/3
S1_config_g0/3# mether-ring 2 domain 2 edge-port
S1_config_g0/3#exit
```

Related Command

edge-node

assistant-node

mether-ring id1 domain id2 common-port

24.3 Show

24.3.1 show mether-ring

To display the summary information about the Ethernet-ring node, run the following command:

show mether-ring *id1* **domain** *id2*

To display the detailed information about the Ethernet-ring node, run the following command:

show mether-ring *id1* **domain** *id2* **detail**

To display the information about the Ethernet-ring port, run the following command:

show mether-ring *id1* **domain** *id2* **interface** *intf-name*

To display all summary information about the Ethernet-ring node, run the following command:

show mether-ring

Parameters

Parameters	Description
Id1	ID of the node
Id2	ID of the domain
intf-name	Name of an interface

Default Value

None

Command Mode

Monitoring mode, global configuration mode, node configuration mode or port configuration mode

Usage Guidelines

If the configured domain is 0, that is**id2 is o,** *domain id2*can be omitted.

Example

None

Related Command

None

Chapter 25 IP ACL Application Configuration Commands

25.1 IP ACL Application Configuration Commands

IP ACL Application Configuration Commands include:

- ip access-group
- ipv6 access-group

25.1.1 ip access-group

To control and access an interface, run ip access-group. To cancel the designated access group, run no ipv6 access-group.

Use it on the interface

[no] ip access-group name

To apply the established IP access list to an interface or in the global mode or cancel a IP access list which is already applied to an interface or in the global mode, run the following command.

Use it in the global mode

[no] ip access-group name [vlan {word | add word | remove word}]

Parameters

Parameters	Description
Name	Name of the IP access control list
Vlan	THE ACCESS LIST IS APPLIED IN INGRESS.
Word	VLAN RANGE TABLE
Add	ADD VLAN RANGE TABLE
Remove	DELETE VLAN RANGE TABLE

Command Mode

Global configuration mode or interface configuration mode

Usage Guidelines

Most rules in the ACL take effect through hardware; those that hardware does not support give no errors but they have no actual effects; a few rules such as time-range take effect through software.

Note:

The IPv4 standard ACL supports the following rules:

any: means any source IP address.

source-addr source-mask: means matching up the source address.

reverse-mask source-addr source-mask: means to use the reverse source address for match-up.

The IPv4 extended ACL supports the following rules:

any: means any IP address.

ip-protocol: means the IP protocol ID.

ip –IP protocol

reverse-mask: means the reverse configuration of varied protocols

eq/gt/lt/src-portrange/ dst-portrange: means TCP/UDP port ID match-up.

gre: GRE protocol ID match-up

icmp: ICMP protocol ID match-up

icmp: IGMP protocol ID match-up

ospf: OSPF routing protocol ID match-up

Though tcp/udp port ID can enable the source port ID match-up and the destination port ID simultaneously, only the destination port ID match-up takes effect. Here is an exception when the match-up is configured to eq. In such case, the source port ID match-up and the destination port ID match-up takes effect simultaneously.

Example

The following **Example** shows how to apply the ACL filter at the ingress direction of interface g0/1.

```
Switch_config#inter g0/1
Switch_config_g0/1# ip access-group filter
```

25.1.2 ipv6 access-group

To designate an access group, run the ipv6 access-group. To cancel the designated access group, run no ipv6 access-group.

Use it on the interface

[no] ipv6 access-group *name*

Use it in the global mode

To apply or delete a created IPv6 ACL on a port or in global mode, run this command.

[no] ipv6 access-group *name* **[vlan** {*word* **| add** *word* **| remove** *word*}**]**

Parameters

Parameters	Description
name	Name of the ip access control list
vlan	The access list is applied in ingress.
word	vlan range table
add	Add vlan range table
remove	Delete vlan range table

Command Mode

Global configuration mode or interface configuration mode

Usage Guidelines

Most rules in the ACL take effect through hardware; those that hardware does not support give no errors but they have no actual effects; a few rules such as time-range take effect through software.

Note:

The IPv6 ACL supports the following rules:

any: means any IP address.

Ipv6-addr/ **host** *Ipv6-addr*： **means IPv6 address match-up.**

ip-protocol: means the IPv6 protocol ID.

eq/gt/lt/src-portrange/ dst-portrange: means TCP/UDP port ID match-up.

dscp/flow-label: means field match-up.

Though tcp/udp port ID can enable the source port ID match-up and the destination port ID simultaneously, only the destination port ID match-up takes effect. Here is an exception when the match-up is configured to eq. In such case,the source port ID match-up and the destination port ID match-up takes effect simultaneously.

Example

The following **Example** shows how to apply the ACL filter at the ingress direction of interface g0/1.

```
Switch_config#inter g0/1
Switch_config_g0/1# ipv6 access-group filter
```

Chapter 26 UDLD Configuration Commands

26.1 UDLD Configuration Commands

UDLD Configuration Commands:

- udld enable
- udld aggressive
- udld port
- udld port aggressive
- udld message
- udld reset
- show udld
- udld enable

26.1.1 udld enable

udld enable Enable UDLD function in global mode in normal mode

no udld enable Turn off UDLD function for global state in normal mode

parameter

none

default

none

Instructions

Start the UDLD function of all interfaces in normal mode. In Normal mode, if UDLD determines that the connection is lost, UDLD will not set the protocol state of the port to down, it will only put the port in the undetermined state. If UDLD considers the link to be bidirectional, the port is in Bidirectional.

Command mode

Global configuration mode

Example

The following command will start UDLD in normal mode.

```
Switch_config#udld enable
```

26.1.2 udld aggressive

Command description

udld aggressive Enable UDLD in global mode in aggressive mode
no udld aggressive Turn off UDLD for global state in aggressive mode

parameter
none

default
none

Instructions

Start the UDLD function of all interfaces in aggressive mode. In the Aggressive mode, if UDLD determines that the connection is lost and is unable to re-establish the connection, the mode considers that the communication interruption is a serious network problem. UDLD will set the port protocol state to down and the port will be in the errdisable state. If UDLD considers the link to be bidirectional, the port is in Bidirectional.

Command mode

Global configuration mode

Example

The following command will start UDLD in aggressive mode.

```
Switch_confi1g#udld agg
```

26.1.3 udld port

Command description

udld port Start the UDLD function of the interface in normal mode
no udld port Disable the UDLD function of the interface in normal mode

parameter
none

default
none

Instructions

Start the UDLD function of the interface in normal mode. In Normal mode, if UDLD determines that the connection is lost, UDLD will not set the protocol state of the port to down, it will only put the port in the undetermined state. If UDLD considers the link to be bidirectional, the port is in Bidirectional.

Command mode

Interface configuration mode

Example

The following command will start UDLD in normal mode.

```
Switch_config_g0/1#udld port
```

26.1.4 udld port aggressive

Command description

udld port aggressive Start UDLD function of the interface in aggressive mode

no udld port aggressive Disabling UDLD on the interface in aggressive mode

parameter

none

default

none

Instructions

Start the UDLD function of the interface in aggressive mode. In the Aggressive mode, if UDLD determines that the connection is lost and is unable to re-establish the connection, the mode considers that the communication interruption is a serious network problem. UDLD will set the port protocol state to down and the port will be in the errdisable state. If UDLD considers the link to be bidirectional, the port is in Bidirectional.

Command mode

Interface configuration mode

Example

The following command will start UDLD in aggressive mode.

```
Switch_config_g0/1#udld port aggressive
```

26.1.5 udld message

Command description

udld message time sets the message interval for aggressive mode

no udld message Restore default aggressive mode message interval

parameter

Parameter	Parameter Description
time	Message interval in Aggressive mode. Value range: 7-90s

default

15s

Instructions

Set the message interval in aggressive mode. After setting the message interval, restart the aggressive mode before the new message interval becomes effective.

Command mode

Global configuration mode

Example

The following command will set the aggressive mode message interval to 7s. It will take effect after restarting aggressive mode.

```
Switch_config#udld message 7
```

26.1.6 udld reset

Command description

udld reset Reset the interface that was down by the UDLD module protocol to up.

parameter

none

default

none

Instructions

Reset the interface that was down by the UDLD module protocol to up.

Command mode

Management model

Example

The following command will restart the interface closed by the UDLD module

```
Switch#udld reset
1 ports shutdown by UDLD were reset.
%%UDLD-2-UDLD_PORT_RESET: UDLD reset interface GigaEthernet0/1.
%%PM-4-ERR_RECOVER: Attempting to recover from udld err-disable state on GigaEthernet0/1.
```

26.1.7 show udld

Command description

show udld interface [*interface*]

Display running connection information of UDLD

parameter

Parameter	Parameter Description
interface	Display UDLD module operation information for a specific interface

default

none

Instructions

Displays the operation information of the UDLD module. When the interface parameter is not entered, the running information of UDLD on all interfaces is displayed; when the interface parameter is entered, only the UDLD operating information of the interface is displayed.

Command mode

Management / Global Configuration Mode

Example

he following command will display the running status information of the UDLD module on all interfaces

```
Switch_config#show udld

Interface GigaEthernet0/1
---
Port enable administrative configuration setting: Enabled Port enable operational state: Enabled
Current bidirectional state: Unknown Current operational state: Link down Message interval: 15
Time out interval: 1
No neighbor cache information stored
```

```
Interface GigaEthernet0/2
---
Port enable administrative configuration setting: Enabled
```

Chapter 27 IGMP-Snooping Configuration Commands

The IGMP-Snooping configuration commands include:

(1) ip igmp-snooping

(2) ip igmp-snooping static

(3) ip igmp-snooping immediate-leave

(4) ip igmp-snooping mrouter

(5) ip igmp-snooping policy

(6) ip igmp-snooping dlf-drop

(7) ip igmp-snooping router age

(8) ip igmp-snooping response time

(9) ip igmp-snooping querier

(10) ip igmp-snooping forward-l3-to-mrouter

(11) ip igmp-snooping sensitive

(12) ip igmp-snooping v3-leave-check

(13) ip igmp-snooping forward-wrongiif-within-vlan

(14) ip igmp-snooping policy

(15) ip igmp-snooping limit

(16) show ip igmp-snooping

(17) show ip igmp-snooping timer

(18) show ip igmp-snooping groups

(19) show ip igmp-snooping statistics

(20) debug ip igmp-snooping packet

(21) debug ip igmp-snooping timer

(22) debug ip igmp-snooping event

(23) debug ip igmp-snooping error

27.1.1 igmp-snooping

Syntax

ip igmp-snooping [vlan *vlan_id* **]**

no ip igmp-snooping [vlan *vlan_id* **]**

To enable or disable the IGMP-snooping function, run ip igmp-snooping [vlan vlan_id]. To resume the corresponding default settings, run no ip igmp-snooping [vlan vlan_id].

Parameters

Parameters	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094

Default Value

The IGMP-Snooping function of the designated VLAN is shut down by default.

Usage Guidelines

If the vlan parameter is not designated, all VLANs in the system will be enabled or disabled after you run this command (IGMP-snooping supports at most 16 VLANs simultaneously).

Example

The following example shows how to enable the IGMP snooping function of VLAN1.

```
switch_config# ip igmp-snooping vlan 1
switch_config#
```

27.1.2 igmp-snooping static

Syntax

ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*

no ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*

Parameters

Parameters	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094
A.B.C.D	IP address of the multicast
intf	Port

Default Value

None

Usage Guidelines

This command is used to configure the static multicast address of VLAN. Its negative form is used to cancel the static multicast address.

Example

The following example shows how to add static multicast address 234.5.6.7 to interface FastEthernet0/5 of VLAN 2.

```
switch_config# ip igmp-snooping vlan 2 static 234.5.6.7 interface GigaEthernet0/5
switch_config#
```

NOTE: 224.0.0.0-224.0.0.255 stands for irroutable multicast addresses which cannot be registered on each port.

27.1.3 igmp-snooping immediate-leave

Syntax

To configure the immediate-leave attribute of VLAN, run ip igmp-snooping vlan vlan id immediate-leave. To resume the default value, run no ip igmp-snooping vlan vlan_id immediate-leave.

ip igmp-snooping vlan *vlan_id* **immediate-leave**

no ip igmp-snooping vlan *vlan_id* **immediate-leave**

Parameters

Parameters	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094

Default Value

The immediate-leave attribute is shut down by default.

Usage Guidelines

None

Example

The following example shows how to enable the immediate-leave attribute of VLAN1.

```
switch_config# ip igmp-snooping vlan 1 immediate-leave
switch_config#
```

27.1.4 igmp-snooping mrouter

Syntax

ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*

no ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*

Parameters

Parameters	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094
intf	Port

Default Value

None

Usage Guidelines

The command is used to set the static routing port of VLAN. Use the no form of this command to delete the routing port.

Example

The following example shows how to add gigabit Ethernet port 0/5 to the static routing port of VLAN 2.

```
switch_config# ip igmp-snooping vlan 2 mrouter interface GigaEthernet0/5
switch_config#
```

27.1.5 igmp-snooping policy

Syntax

ip igmp-snooping policy *word*

no ip igmp-snooping policy

Parameters

Parameters	Description
Word	IP ACL name

Default Value

None

Usage Guidelines

The command is used to set the to be detected IP ACL list of igmp-snooping when adding multicast forwarding table. Use the no form of this command to cancel the detection of the list.

Example

The following example is to detect the IP ACL whose name is 123 when adding multicast forwarding table.

```
switch_config# ip igmp-snooping policy 123
switch_config#
```

27.1.6 igmp-snooping dlf-drop

Syntax

ip igmp-snooping dlf-drop

no ip igmp-snooping dlf-drop

Default Value

None

Usage Guidelines

This command is used to set the multicast packets whose destination multicast addresses are not registered to the filtration mode. The negative form of this command is used to resume the default settings.

Example

The following example shows how to drop the multicast packets with unregistered destination addresses in all VLANs.

```
switch_config# ip igmp-snooping dlf-drop
switch_config#
```

27.1.7 igmp-snooping router age

Syntax

ip igmp-snooping timer router-age *time_value*

no ip igmp-snooping timer router-age

Parameters

Parameters	Description
time value	Queries the time of the timer. Value range: 10-2147483647

Default Value

260 seconds

Usage Guidelines

This command is used to query the time of the timer of IGMP-Snooping. The negative form of this command is used to resume the default value.

Example

The following example shows how to set the query time of the router to 300 seconds.

```
switch_config# ip igmp-snooping timer router-age 300
switch_config#
```

27.1.8 igmp-snooping response time

Syntax

To configure the maximum response time of IGMP snooping, run ip igmp-snooping timer response-time timer value. To resume the default value of IGMP snooping, run no ip igmp-snooping timer response-time timer value.

ip igmp-snooping timer response-time *time_value*

no ip igmp-snooping timer response-time

Parameters

Parameters	Description
time value	Queries the time of the timer. Value range: 1-2147483647

Default Value

15 seconds

Usage Guidelines

None

Example

The following example shows how to set the query response time of IGMP snooping to 20 seconds.

```
switch_config# ip igmp-snooping timer response-time 20
switch_config#
```

27.1.9 igmp-snooping querier

Syntax

To activate the IGMP-snooping querier mechanism, or set the source IP address of the automatic query packet, run ip igmp-snooping querier [address <ip_addr>]. To resume the default value, run no ip igmp-snooping querier [address <ip_addr>].

ip igmp-snooping querier [address <*ip_addr*>**]**

no ip igmp-snooping querier [address]

Parameters

Parameters	Description
ip_addr	IP address of a normal unicast

Default Value

By default, the querier function is not enabled and the source IP address is 10.0.0.200.

Usage Guidelines

None

Example

The following example shows how to activate IGMP Querier to serve as a multicast router if no multicast router is working.

```
switch_config# ip igmp-snooping querier
switch_config#
```

27.1.10 igmp-snooping querier querier-timer

Syntax

To configure the forward interval of forwarding query packets by the local querier, run the first one of the above commands. To return to the default setting, use the no form of this command.

ip igmp-snooping querier querier-timer *time_value*

no ip igmp-snooping querier querier-timer

Parameters

Parameters	Description
time_value	local querier interval

Default Value

The default interval is 200 seconds in enabling Querier.

Usage Guidelines

None

Example

The following command shows how to configure the query period of the local querier to 140s.

```
switch_config# ip igmp-snooping querier querier-timer 140
switch_config#
```

27.1.11 igmp-snooping forward-l3-to-mrouter

Syntax

To send the data packets to the multicast routing port, run ip igmp-snooping forward-l3-to-mrouter. To resume the default settings, use the "no" form of this command.

ip igmp-snooping forward-l3-to-mrouter

no ip igmp-snooping forward-l3-to-mrouter

Parameters

None

Default Value

If the forward-l3-to-mrouter command is not enabled, the data packets will not be sent to the related multicast routing port.

Usage Guidelines

This command is mainly to send the data packets to the IGMP JOIN port and meanwhile to the multicast routing port. Especially in case of L3 multicast cascading, the upstream L3 switches cannot receive the IGMP JOIN packets from a relative group and hence cannot learn the

information about the relative group, and then the data packets will be sent to all physical ports in the L3 egress VLAN. After this command is run, the data packets will only be sent to the multicast routing port, which is registered on PIM-SM.

Example

The following example shows how to activate IGMP forward-l3-to-mrouter and make the upstream multicast data packets be sent to the multicast routing port:

```
switch_config# ip igmp-snooping forward-l3-to-mrouter
switch_config#
```

27.1.12 igmp-snooping sensitive

Syntax

To activate the IGMP-snooping sensitive mechanism or set the value of the sensitive parameter, run ip igmp-snooping sensitive [value int<3-30>]. To resume the default value, use the "no" form of this command.

ip igmp-snooping sensitive [value *int<3-30>***]**

no ip igmp-snooping sensitive [value]

Parameters

Parameters	Description
int	3-30

Default Value

The sensitive function is disabled by default.

Usage Guidelines

This command is mainly used to modify the router-age of the mrouter port in active state and deliver the new query packets rapidly when a port in trunk mode is shut down.

Example

The following example shows how to activate IGMP sensitive and set the route-age of mrouter to be a converged one.

```
switch_config# ip igmp-snooping sensitive
switch_config# ip igmp-snooping sensitive value 10
```

27.1.13 igmp-snooping v3-leave-check

Syntax

To send the special query packets after the v3-leave packet is received, run ip igmp-snooping v3-leave-check; to resume the default settings, run the "no" form of this command.

ip igmp-snooping v3-leave-check

no ip igmp-snooping v3-leave-check

Default Value

v3-leave-check is disabled and the special query packet will not be sent after v3-leave packet is received.

Usage Guidelines

None

Example

The following example shows how to activate IGMP v3-leave-check and send the special query packet after the v3-leave packet is received.

```
switch_config# ip igmp-snooping v3-leave-check
switch_config#
```

27.1.14 igmp-snooping forward-wrongiif-within-vlan

Syntax

To send the multicast data packets, received from the wrongiif port, to the relative physical ports in the local vlan, run ip igmp-snooping forward-wrongiif-within-vlan; to resume the default value, run the "no" form of this command.

ip igmp-snooping forward-wrongiif-within-vlan

no ip igmp-snooping forward-wrongiif-within-vlan

Default Value

This command is enabled by default and the multicast packets from the wrongiif port will be sent to the relative physical ports.

Usage Guidelines

The command takes its importance only when the L3 multicast is enabled. After this command is enabled, the multicast packets, entering from the wrongiif port, will be sent to the physical ports that are added into the group of vlan; otherwise, the multicast packets will be dropped.

Example

The following example shows how to activate IGMP forward-wrongiif-within-vlan, and how to send the multicast packets from the wrongiif port to the relative physical ports in the local VLAN:

```
switch_config# ip igmp-snooping forward-wrongiif-within-vlan
switch_config#
```

27.1.15 igmp-snooping policy

Syntax

ip igmp-snooping policy *word*

no ip igmp-snooping policy

Parameters

Parameters	Description
Word	IP ACL name

Default Value

None

Usage Guidelines

Enable IPACL function of IGMP-snooping and determine the packets of some multicast IP address are to be deleted or ignored.

Configuration Mode

Port Configuration

Example

The following example is to detect the IP ACL whose name is 123 when dealing with the packets.

```
switch_config_G0/1# ip igmp-snooping policy 123
switch_config_G0/1#
```

27.1.16 igmp-snooping limit

Syntax

ip igmp-snooping limit *value*

no ip igmp-snooping limit

Parameters

Parameters	Description
value	1-2048

Default Value

2048

Usage Guidelines

The command configures the max multicast IP address number in the port of IGMP-snooping. The command will estimate whether the applied groups have reached the configuration number when IGMP-snooping generating the forward table. Otherwise, the table of the port is no longer generated.

Configuration Mode

Port Configuration

Example

The following example shows how to set the max number of the joining group as 1000.

```
switch_config_G0/1# ip igmp-snooping limit 1000
switch_config_G0/1#
```

27.1.17 show ip igmp-snooping

Syntax

show ip igmp-snooping

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the information about IGMP-snooping configuration.

Example

The following example shows how to display each VLAN where IGMP-snooping is running.

```
switch_config# show ip igmp-snooping
Global IGMP snooping configuration:
-----------------------------------
Globally enable          : Enabled
VLAN nodes               : 1,50,100,200,400,500
Dlf-frames filtering : Disabled
Sensitive                : Disabled
Querier                  : Enabled
Querier address          : 10.0.0.200
Querier interval         : 140 s
Router age               : 260 s
Response time            : 15 s

  vlan_id    Immediate-leave    Ports    Router Ports
-------------------------------------------------------------------
     1            Disabled          5-10       SWITCH(querier);
    50            Disabled          1-4        SWITCH(querier);
   100            Disabled          NULL       SWITCH(querier);G0/1(static);
   200            Disabled          NULL       SWITCH(querier);
   400            Disabled          NULL       SWITCH(querier);
   500            Disabled          NULL       SWITCH(querier);
switch_config#
```

27.1.18 show ip igmp-snooping timer

Syntax

show ip igmp-snooping timer

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the information about the IGMP-snooping clock.

Example

The following example shows how to display the information about the IGMP-snooping clock.

```
switch_config# show ip igmp-snooping timer
vlan 1 mrouter on port 3 : 251
switch_config#
```

27.1.19 show ip igmp-snooping groups

Syntax

show ip igmp-snooping groups

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the information about the multicast group of IGMP-snooping.

Example

The following example shows how to display the information about the multicast group of IGMP-snooping.

```
switch_config# show ip igmp-snooping groups
                The total number of groups              2

Vlan Group                  Type Port(s)
---- --------------- ---- -----------------------------------------------------
   1 226.1.1.1           IGMP G0/1                       G0/3
   1 225.1.1.16          IGMP G0/1                       G0/3
switch_config#
```

27.1.20 show ip igmp-snooping statistics

Syntax

show ip igmp-snooping statistics

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the information about IGMP-snooping statistics.

Example

The following example shows how to display the information about IGMP-snooping statistics.

```
switch_config# show ip igmp-snooping statistics
   vlan 1
------------
      v1_packets:1
      v2_packets:2
      v3_packets:0
      general_query_packets:1
      special_query_packets:2
      join_packets:0
      leave_packets:0
      send_query_packets:0
      err_packets:0
switch_config#
```

27.1.21 debug ip igmp-snooping packet

Syntax

debug ip igmp-snooping packet

no debug ip igmp-snooping packet

Parameters

None

Default Value

None

Usage Guidelines

This command is used to enable or disable the igmp-snooping packet.

Example

The following example shows how to enable the packet debugging switch of IGMP-snooping.

```
switch # debug ip igmp-snooping packet
switch #
```

27.1.22 debug ip igmp-snooping timer

Syntax

debug ip igmp-snooping timer

no debug ip igmp-snooping timer

Parameters

None

Default Value

None

Usage Guidelines

This command is used to enable or disable the timer debugging switch of IGMP-snooping.

Example

The following example shows how to enable the timer debugging switch of IGMP-snooping.

```
switch # debug ip igmp-snooping timer
switch #
```

27.1.23 debug ip igmp-snooping event

Syntax

debug ip igmp-snooping event

no debug ip igmp-snooping event

Parameters

None

Default Value

None

Usage Guidelines

This command is used to enable or disable the event debugging switch of IGMP-snooping.

Example

The following example shows how to enable the event debugging switch of IGMP-snooping.

```
switch # debug ip igmp-snooping event
switch #
```

27.1.24 debug ip igmp-snooping error

Syntax

debug ip igmp-snooping error

no debug ip igmp-snooping error

Parameters

None

Default Value

None

Usage Guidelines

This command is used to enable or disable the error debugging switch of IGMP-snooping.

Example

The following example shows how to enable the error debugging switch of IGMP-snooping.

```
switch # debug ip igmp-snooping error
switch #
```

Chapter 28 NTP Configuration Commands

28.1.1 ntp master

Syntax

To set the device as the original NTP server (stratum=1), run the following command.

ntp master primary

To set the device as the secondary NTP server, run the following command.

ntp master secondary

To disable NTP server, run the following command.

no ntp master

Parameters

None

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

If the device is not configured with NTP server (ntp server command is not configured), ntp master primary command must be configured. Or the switch cannot provide time synchronization service. ntp master secondary command must be run when the switch configures NTP server. Moreover, the switch can provide time synchronization service to the NTP client in condition its own time synchronization is realized.

Example

```
Switch_config#ntp master primary
Switch_config#ntp master secondary
Switch_config#no ntp master
```

Related command

ntp server

ntp peer

28.1.2 ntp authentication enable

Syntax

To enable NTP identity authentication, run the following command.

ntp authentication enable

To return to the **Default** setting, use the no form of this command.

no ntp authentication enable

Parameters

None

Default Value

Disabled

Command Mode

Global configuration mode

Usage Guidelines

For a secure network, NTP identity authentication must be enabled when operating NTP protocol. The identity authentication ensures that the client only realize time synchronization with the server which passes the identity authentication. Thus, the client will not obtain error time information from the illegal server.

Example

```
Switch_config#ntp authentication enable
```

Related command

ntp authentication key

ntp authentication trusted-key

28.1.3 ntp authentication key

To set NTP identity authentication key, run the first one of the following commands.

ntp authentication key *keyid* **md5** *password*

To return to the **Default** setting, use the no form of this command.

no ntp authentication key *keyid*

Parameters

Parameters	Description
keyid	The serial number of the authentication key. The value ranges from 1 to 4294967295.
password	The key of keyed. The length ranges from 1 to 50.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command is used to set identity authentication key. The client and the server must set the same key serial number and key value, or they cannot realize time synchronization.

After set NTP authentication key, Set the key as the trusted key by command ntp authentication trusted-key. The trusted key will automatically disappear from the trusted key list when it is deleted. There is no need to run command "no ntp authentication trusted-key".

The command can set multiple ntp authentication key commands.

Example

```
Switch_config#ntp authentication key 5 md5 abc123
Switch_config#no ntp authentication key 5
```

Related command

ntp authentication enable

ntp authentication trusted-key

28.1.4 ntp authentication trusted-key

To set the created key as the trusted key, run the first one of the following commands.

ntp authentication trusted-key *keyid*

To return to the **Default** setting, use the no form of this command.

no ntp authentication trusted-key *keyid*

Parameters

Parameters	Description
keyid	The serial number of the authentication key. The value ranges from 1 to 4294967295.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

Enable the identity authentication function, the client can only time synchronize with the server providing the trusted key. If the key provided by the server is not trusted, the client cannot synchronize to the NTP server.

The command must be configured after the key is set. The trusted key will automatically disappear from the trusted key list when it is deleted. There is no need to run command "no ntp authentication trusted-key".

Example

```
Switch_config#ntp authentication trusted-key 5
Switch_config#no ntp authentication trusted-key 5
```

Related command

ntp authentication enable

ntp authentication key

28.1.5 ntp server

To set NTP server, run the following command.

ntp server *ip-address* **[version** *number* **| key** *keyid***]***

To return to the **Default** setting, use the no form of this command.

no ntp server *ip-address*

Parameters

Parameters	Description
ip-address	NTP Server IP address
number	NTP version number, the value ranges from: <1-4>, the **Default** value is 4.
keyid	When sending NTP packets to the NTP server, calculate the packet information abstract with the key corresponds to the keyid. The value ranges from 1 to 4294967295. If the **Parameter** is not set, the device will not authenticate the identity of the server, or vice verse.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

After a NTP server is set, the device can time synchronize with the server, but the server time will not synchronize to the device.

Multiple ntp server commands can be configured. If using the NTP server on the public network, you have to configured at least 4 different NTP severs, so that the error clock source can be expelled.

Example

```
Switch_config#ntp server 1.1.1.1 version 4 key 5
```

Related command

ntp authentication enable

ntp authentication key

ntp authentication trusted-key

28.1.6 ntp peer

To set a NTP peer for the device, run the following command.

ntp peer *ip-address* **[version** *number* **| key** *keyid***]***

To return to the **Default** setting, use the no form of this command.

no ntp peer *ip-address*

Parameters

Parameters	Description
ip-address	NTP peer IP address
number	NTP version number, the value ranges from: <1-4>, the **Default** value is 4.
keyid	When sending NTP packets to the NTP peer, calculate the packet information abstract with the key corresponds to the keyid. The value ranges from 1 to 4294967295. If the **Parameter** is not set, the device will not authenticate the identity of the peer, or vice verse.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command is used to set the NTP peer and synchronize the time of the peer to the device provided that the peer time is synchronized. The command is often used as backup between the NTP servers. The device as the client is usually not configure the command. The command ntp server is used to set the NTP server.

Example

Switch_config#ntp peer 1.1.1.2 version 3 key 5

Related command

ntp authentication enable

ntp authentication key

ntp authentication trusted-key

28.1.7 show ntp

To show NTP current status, run the following command.

show ntp [status]

To show NTP association status, run the following command.

show ntp associations [detail]

To show NTP timer status, run the following command.

show ntp timers

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

Show NTP relevant information

Example

```
Switch#show ntp

Time-zone: GMT+8:00, Shanghai
Current time: 2014-05-21 10:45:26
```

Clock Status: synchronized
Clock Stratum: 3
Leap Indicator: 0
Reference ID: 211.233.84.186
Clock Jitter: 0.004149
Clock Precision: -18
Clock Offset: 6.561 ms
Root Delay: 172.153 ms
Root Dispersion: 587.873 ms
Packets Sent: 30788
Packets Received: 27969 (bad version: 0)
Reference Time: 2014-05-21 10:41:37
Last Update Time: 2014-05-21 10:37:08

Switch#show ntp associations

ip address	reference clock	st	poll	reach	delay	offset	dispersion
61.110.197.50	204.123.2.5	2	64	377	59.99	0.96	2.7
27.114.150.12	193.190.230.65	2	64	377	489.97	-34.56	3.1
*211.233.84.186	204.123.2.5	2	64	377	19.99	9.15	3.0
198.55.111.50	216.229.0.50	3	64	377	229.98	-40.09	3.4
199.241.31.224	132.163.4.103	2	64	377	198.04	2.51	3.6
204.2.134.163	241.199.164.101	2	64	360	169.97	-17.16	942.8

Note: * system peer(master), poll(s), delay(ms), offset(ms), dispersion(ms)

Total Associations: 6

Related command

None

28.1.8 debug ntp

To enable NTP packet debug switch, run the following command.
debug ntp packet
To enable NTP event debug switch, run the following command.
debug ntp event
To enable NTP error debug switch, run the following command.
debug ntp error
To enable NTP all debug switches, run the following command.
debug ntp all
To disable all debug switches, run the following command.
no debug ntp

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

Check NTP running process by debug information.

Example

None

Related command

None

28.1.9 time-zone

To enable time zone function, run the following command.

time-zone *name offset-hour* **[***offset-minute***]**

To return to the **Default** setting, use the no form of this command.

no time-zone

Parameters

Parameters	Description
name	Stands for the name of a time zone.
offset-hour	Hour off-set of local time to UTC time (-12~12)
offset-minute	Minute offset of local time to UTC time (0~59); the **Default** value is 0.

Default Value

None

Command Mode

Global configuration mode

Usage Guidelines

The command is used to transfer UTC to the local time.

Example

Switch_config#time-zone Beijing 8

Related command

None

Chapter 29 MLD Multicast Configuration Commands

The MLD multicast configuration commands include:

- ipv6 mld-snooping
- ipv6 mld-snooping solicitation
- ipv6 mld-snooping vlan vlan_id static X:X:X:X::X interface intf
- ipv6 mld-snooping timer router-age timer_value
- ipv6 mld-snooping timer response-time timer_value
- ipv6 mld-snooping vlan vlan_id mrouter interface inft_name
- ipv6 mld-snooping vlan vlan_id immediate-leave
- show ipv6 mld-snooping
- show ipv6 mld-snooping timer
- show ipv6 mld-snooping groups
- show ipv6 mld-snooping statistics
- show ipv6 mld-snooping mac

29.1 ipv6 mld-snooping

Syntax

To enable MLD snooping, run ipv6 mld-snooping.

ipv6 mld-snooping

ipv6 mld-snooping

Parameters

None

Default Value

Enables MLD snooping multicast.

Usage Guidelines

After MLD snooping is enabled, when DLF occurs on multicast packets (that is, the destination address is not registered in the swap chip through the MLD-snooping), all multicast packets whose destination addresses are not registered on any port will be dropped.

Example

The following example shows how to enable the MLD snooping function:

```
switch_config# ipv6 mld-snooping
```

29.2 ipv6 mld-snooping solicitation

Syntax

ipv6 mld-snooping solicitation

no ipv6 mld-snooping solicitation

To enable or disable the hardware forwarding of the multicast group, run ip mld-snooping solicitation. To resume the default value, run no ip mld-snooping solicitation.

Parameters

None

Default Value

This function is shut down.

Usage Guidelines

None

Example

The following example shows how to enable the hardware forward of the multicast group.

```
switch_config#ipv6 mld-snooping solicitation
```

29.3 ipv6 mld-snooping vlan vlan_id static X:X:X:X::X interface intf_name

Syntax

ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf_name*

no ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf_name*

Parameters

Parameters	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094
X:X:X:X::X	IP address of the multicast
Inft_name	An interface

Default Value

None

Usage Guidelines

This command is used to configure the static multicast address of VLAN. Its negative form is used to cancel the static multicast address.

Example

The following example shows how to add the static multicast address ff12::5 to port G0/1.

```
switch_config# ipv6 mld-snooping vlan 1 static ff12::5 interface g0/1
switch_config#
```

29.4 ipv6 mld-snooping timer router-age timer_value

Syntax

ipv6 mld-snooping timer router-age timer_value

no ipv6 mld-snooping timer router-age

Parameters

Parameters	Description
time value	Queries the time of the timer. Value range: 10-2147483647

Default Value

260 seconds

Usage Guidelines

This command is used to query the time of the timer of MLD-Snooping. The negative form of this command is used to resume the default value.

Example

The following example shows how to set the query time of the router to 300 seconds.

```
switch_config# ipv6 mld-snooping timer router-age 300
switch_config#
```

29.5 ipv6 mld-snooping timer response-time timer_value

Syntax

ipv6 mld-snooping timer response-time timer_value

no ipv6 mld-snooping timer response-time

To configure the maximum response time of IGMP snooping, run ip mld-snooping timer response-time timer_value. To resume the default value of IGMP snooping, run no ip mld-snooping timer response-time timer_value.

Parameters

Parameters	Description
time value	Queries the time of the timer. Value range: 10-2147483647

Default Value

10 seconds

Usage Guidelines

None

Example

The following example shows how to set the query response time of IGMP snooping to 20 seconds.

```
switch_config# ipv6 mld-snooping timer response-time 20
```

29.6 ipv6 mld-snooping querier

Syntax

Ipv6 mld-snooping querier [address <*ip_addr*>**]**

no ipv6 mld-snooping querier [address]

To activate the mld-snooping querier mechanism, or set the source IP address of the automatic query packet, run ip igmp-snooping querier [address <ip_addr>]. To resume the default value, run no ip igmp-snooping querier [address].

Parameters

Parameters	Description
ip_addr	IPv6 address of a normal unicast

Default Value

By default, the querier function is not enabled and the source IP address is FE80::3FF:FEFE:FD00:1.

Usage Guidelines

None

Example

The following example shows how to activate IGMP Querier to serve as a multicast router if no multicast router is working.

```
switch_config# ipv6 mld-snooping querier
switch_config#
```

29.7 ipv6 mld-snooping vlan vlan_id mrouter interface inft_name

Syntax

ipv6 mld-snooping vlan *vlan_id* **mrouter** interface *inft_name*

no ipv6 mld-snooping vlan *vlan_id* **mrouter** interface *inft_name*

To configure the port of the static multicast router of MLD snooping, run ipv6 mld-snooping vlan vlan_id mrouter interface inft_name.

Parameters

Parameters	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094
inft_name	Shows the port type, the slot and the port ID.

Default Value

None

Usage Guidelines

None

Example

The following example shows how to set port G0/4 to the port of the static multicast router of MLD Snooping.

```
switch_config# ipv6 mld-snooping vlan 1 mrouter interface g0/4
```

29.8 ipv6 mld-snooping vlan vlan_id immediate-leave

Syntax

ipv6 mld-snooping vlan *vlan_id* **immediate-leave**

no ipv6 mld-snooping vlan *vlan_id* **immediate-leave**

Parameters

Parameters	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094

Default Value

The immediate-leave function is disabled.

Usage Guidelines

This command is used to set the immediate-leave function.

Example

The following example shows how to enable the immediate-leave functionality on VLAN 1:

```
switch_config# ipv6 mld-snooping vlan 1 immediate-leave
switch_config#
```

29.9 show ipv6 mld-snooping

Syntax

show ipv6 mld-snooping

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the information about MLD-snooping configuration.

Example

The following example shows how to display the information about MLD snooping.

```
switch#show ipv6 mld-snooping

Global MLD snooping configuration:
-----------------------------------
Globally enable          : Enabled
Querier                  : Enabled
Querier address          : FE80::3FF:FEFE:FD00:1
Router age               : 260 s
Response time            : 10 s
Handle Solicitation    : Enabled

Vlan 1:
----------
      Running
      Routers: SWITCH(querier);
Vlan 2:
----------
      Running
      Routers: SWITCH(querier);
```

```
Switch_config#show ipv6 mld-s g
Vlan Group                   Type Port(s)
---- --------------- ---- ---------------------------------------
   1 FF02::1:FF13:647D MLD    G0/2
   1 FF02::1:FF13:394 MLD    G0/2
   2 FF02::1:FF00:2    MLD    G0/1
   1 FF02::1:FF00:12 MLD    G0/1
   1 FF02::1:FF00:2    MLD    G0/1
   2 FF02::1:FF61:9901 MLD    G0/2
switch#
```

29.10 show ipv6 mld-snooping timer

Syntax

show ipv6 mld-snooping timer

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the information about the MLD-snooping clock.

Example

The following example shows how to display the information about the MLD-snooping clock.

```
switch#show ipv6 mld-snooping timers

  vlan 1 Querier on port 0 : 251
  vlan 2 Querier on port 0 : 251
vlan 2 multicast address 3333.0000.0005 response time : 13

switch#
```

Querier on port 0: 251 means the timeout time of the ageing timer of the router.

vlan 2 multicast address 3333.0000.0005 response time : this shows the time period from receiving a multicast query packet to the present; if there is no host to respond when the timer times out, the port will be canceled.

29.11 show ipv6 mld-snooping groups

Syntax

show ipv6 mld-snooping groups

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the information about the multicast group of MLD-snooping.

Example

The following example shows how to display the information about the multicast group of MLD-snooping.

```
switch# show ipv6 mld-snooping timer

Vlan Group                    Type Port(s)
---- --------------- ---- ----------------------------------------
     2 FF02::1:FF00:2    MLD    G0/2
     2 FF02::1:FF61:9901 MLD    G0/2
     1 FF02::1:FF13:394 MLD    G0/1
     1 FF02::1:FF00:2    MLD    G0/1
     1 FF02::1:FF00:12 MLD    G0/1
     1 FF02::1:FF13:647D MLD    G0/2
switch#
```

29.12 show ipv6 mld-snooping statistics

Syntax

show ipv6 mld-snooping statistics

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the information about MLD-snooping statistics.

Example

The following example shows how to display the information about MLD-snooping statistics.

```
switch#show ipv6 mld-snooping statistics
                v1_packets:0              Quantity of MLD v1 packets
                v2_packets:6              Quantity of MLD v2 packets
                general_query_packets:5       Quantity of general query packets
                special_query_packets:0       Quantity of special query packets
                listener_packets:6        Quantity of Report packets
                done_packets:0        Quantity of Leave packets
send_query_packets:0            Quantity of sending packets
err_packets:0          Quantity of error packets
```

29.13 show ipv6 mld-snooping mac

Syntax

show ipv6 mld-snooping mac

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the multicast MAC of MLD snooping.

Example

The following example shows how to display the information about MLD snooping.

```
switch#show ipv6 mld-snooping mac
Vlan Mac                          Ref Flags
---- ---------------- ---- ------
    1 3333:0000:0001       1     2
    2 3333:ff61:9901       1     0
            FF02::1:FF61:9901
    1 3333:0000:0002       1     2
    1 3333:ff00:0002       1     0
            FF02::1:FF00:2
    1 3333:ff00:0012       1     0
            FF02::1:FF00:12
    1 3333:ff13:647d       1     0
            FF02::1:FF13:647D
    2 3333:ff00:0002       1     0
            FF02::1:FF00:2
    1 3333:ff13:0394       1     0
            FF02::1:FF13:394
    1 3333:ff00:0001       1     2
    1 3333:ff8e:7000       1     2
switch#
```

Ref means the quantity of referred IPv6 addresses of MAC.

Flags means the debug output information, and 2 means the information need be sent to CPU.

Chapter 30 OAM Configuration Commands

30.1 OAM Configuration Commands

OAM configuration commands include:

- ethernet oam
- ethernet oam {max-rate | min-rate | mode | timeout }
- ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action
- ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high
- ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low
- ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window
- ethernet oam link-monitor high-threshold action
- ethernet oam link-monitor negotiation-supported

30.1.1 ethernet oam

Syntax

To enable or disable the OAM function, run [no] ethernet oam.

[no] ethernet oam

Parameters

None

Default Value

Ethernet OAM is disabled by default.

Command Mode

Port configuration mode

Usage Guidelines

None

Example

The following commands are used to enable the OAM function on GigaEthernet 0/2 interface.

```
Switch#
Switch#config
Switch_config#interface g0/2
Switch_config_g0/2#ethernet oam
```

30.1.2 ethernet oam {max-rate | min-rate | mode | timeout }

Syntax

[no] ethernet oam {max-rate value1 | min-rate value2 | mode {active | passive} | timeout value3}

ethernet oam max-rate value1 is used to set the fastest transmission rate of the OAM packet.

ethernet oam max-rate value2 is used to set the slowest transmission rate of the OAM packet.

ethernet oam mode {active | passive} is used to set the OAM mode.

ethernet oam timeout value3 is used to set the timeout time of the OAM connection.

Parameters

Parameters	Description
value1	Fastest transmission rate, which ranges between 1 and 10. Its unit is packet/second.
value2	Slowest transmission rate, which ranges between 1 and 10. Its unit is second.
value3	Timeout time of the OAM connection, which ranges between 2 and 30 and whose unit is second

Default Value

The value of max-rate is 10.

The value of min-rate is 1.

The value of timeout is 5.

The value of mode is active.

Command Mode

Port configuration mode

Usage Guidelines

This command can be used to configure some optional parameters for establishing the OAM connection.

Example

The following example shows how to set the fastest and slowest connection rates of the OAM on the GigaEthernet 0/2 interface to 5 packets/second, the connection timeout time to 10 seconds and the OAM mode to passive.

```
Switch #config
Switch_config#
Switch_config#interface g0/2
Switch_config_g0/2# ethernet oam max-rate 5
Switch_config_g0/2#ethernet oam min-rate 5
Switch_config_g0/2#ethernet oam timeout 10
Switch_config_g0/2#ethernet oam mode passive
```

30.1.3 ethernet oam remote-failure {critical-event | dying-gasp | link-fault } action

Syntax

To configure the trigger action after the remote fault instruction is received, run the following command. To return to the default setting, use the no form of this command.

ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action error-disable-interface

no ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action

Parameters

None

Default Value

No trigger action is conducted after the remote fault instruction is received.

Command Mode

Port configuration mode

Usage Guidelines

The switch cannot generate the LINK FAULT packets and the Critical Event packets. However, these packets will be handled if they are received from the remote terminal. router can transmit and receive the Dying Gasp packet. When the local port enters the err disabled state or is closed by the administrator or the OAM function of the local port is closed by the manager, the Dying Gasp packet will be transmitted to the remote terminal that connects the local port.

Example

The following example shows how to enable error-disable-interface after receiving remote link fault on GigaEthernet 0/1.

```
Switch_config#interface g0/1
Switch_config_g0/1#ethernet oam remote-failure link-fault action error-disable-interface
```

30.1.4 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high

Syntax

To configure the high threshold for link monitoring, run the following command.

[**no**] **ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold high {none |** *value***}**

Parameters

Parameters	Description
Value	Error-signal period events ranges between 1 and 65535, whose unit is signal number. Error-frame event ranges between 1 and 65535, whose unit is frame number. Error-frame event ranges between 1 and 65535, whose unit is frame number. Error-frame second event ranges between 1 and 900, whose unit is second. Error-CRC event ranges between 1 and 65535, whose unit is frame number.

Default Value

The default value of each general link event is none.

Command Mode

Port configuration mode

Usage Guidelines

After the high threshold of an event and ethernet oam link-monitor high-threshold action error-disable-interface are configured, the local port enters the errdisabled state when the local port receives the high threshold of the event.

Example

The following example shows how to configure the high threshold of the error-frame event to 10 on interface GigaEthernet0/2.

```
Switch_config_g0/2#ethernet oam link-monitor symbol-period threshold high 10
```

30.1.5 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low

Syntax

To configure the high threshold for link monitoring, run the following command.

[no] ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} threshold low {none | value}

Parameters

Parameters	Description
Value	Error-signal period events ranges between 0 and 65535, whose unit is signal number. Error-frame event ranges between 0 and 65535, whose unit is frame number. Error-frame event ranges between 0 and 65535, whose unit is frame number. Error-frame second event ranges between 0 and 900, whose unit is second. Error-CRC event ranges between 0 and 65535, whose unit is frame number.

Default Value

The default value of the error-signal period event is 1.

The default value of the error-frame event is 1.

The default value of the error-frame period event is 1.

The default value of the error-frame second event is 1.

The default value of the error-CRC event is 10.

Command Mode

Port configuration mode

Usage Guidelines

After the low threshold of an event is configured and the locally-received event exceeds the low threshold, the Event Notification OAM packet will be transmitted to notify the peer terminal.

Example

The following example shows how to set the low threshold of the error-frame event to 10 on interface GigaEthernet0/2.

```
Switch_config_g0/2#ethernet oam link-monitor symbol-period threshold low 10
```

30.1.6 ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window

Syntax

To configure the size of the round-query window for link monitoring, run the following command.

ethernet oam link-monitor {symbol-period | frame | frame-period | frame-seconds | receive-crc} window value

Parameters

Parameters	Description
Value	The error-signal period event ranges between 10 and 600 on GigaEthernet and ranges between 1 and 60 on Fast Ethernet. The unit is 100M signals. The error-frame event ranges between 1 and 60, whose unit is second. The error-frame period event ranges between 100 and 6000 on GigaEthernet and ranges between 10 and 600 on Fast Ethernet. The unit is 14881 frames. Error-frame second event ranges between 10 and 900, whose unit is second. The error-CRC event ranges between 1 and 180, whose unit is second.

Default Value

The default value of the error-signal period event is 10 on GigaEthernet and is 1 on Fast Ethernet.

The default value of the error-frame event is 1.

The default value of the error-frame period event is 100 on GigaEthernet and is 10 on Fast Ethernet.

The default value of the error-frame second event is 60.

The default value of the error-CRC event is 1.

Command Mode

Port configuration mode

Usage Guidelines

None

Example

The following example shows how to set the window of the error-frame period event to 50 on interface GigaEthernet0/2.

```
Switch_config_g0/2#ethernet oam link-monitor symbol-period window 50
```

30.1.7 ethernet oam link-monitor high-threshold action

Syntax

To configure the link-monitor trigger event with the high threshold, run ethernet oam link-monitor high-threshold action error-disable-interface. To return to the default setting, use the no form of this command.

ethernet oam link-monitor high-threshold action error-disable-interface

[no] ethernet oam link-monitor high-threshold action

Parameters

None

Default Value

The high-threshold trigger event does not exist by default.

Command Mode

Port configuration mode

Usage Guidelines

After the high threshold of an event and ethernet oam link-monitor high-threshold action error-disable-interface are configured, the local port enters the err disabled state when the local port receives the high threshold of the event.

Example

The following example shows how to set the high-threshold trigger event on interface GigaEthernet 0/2 to error-disable-interface.

```
Switch_config_g0/2#ethernet oam link-monitor high-threshold action error-disable-interface
```

30.1.8 ethernet oam link-monitor negotiation-supported

Syntax

To configure the link-monitor negotiation, run ethernet oam link-monitor negotiation-supported. To return to the default setting, use the no form of this command.

ethernet oam link-monitor negotiation-supported

[no] ethernet oam link-monitor negotiation-supported

Parameters

None

Default Value

Link-monitor negotiation is supported.

Command Mode

Port configuration mode

Usage Guidelines

Devices support link monitoring. However, if the third-party devices do not support link monitoring, devices automatically do not support link monitoring during OAM Discovery and the OAM connection can be established through the third-party devices in this case. Otherwise, when the link-monitor negotiation is not configured, devices mandatorily support the link-monitor function, but the OAM connection cannot be created if the third-party devices do not support the link-monitor function.

Example

The following example shows that the link-monitor function is not supported on interface GigaEthernet 0/2.

```
Switch_config_g0/2#no ethernet oam link-monitor negotiation-supported
```

30.1.9 clear ethernet oam statistics

Syntax

To clear the OAM statistics information, run the following command.

clear ethernet oam statistics [interface intf-type intf-id]

Parameters

Parameters	Description
Intf-id	Designates a designated interface. If an interface is not designated, the OAM statistics information on all interfaces will be deleted.

Default Value

None

Command Mode

Privileged mode

Usage Guidelines

After this command is run, the following statistics information (type-classified packet numbering information, link-event statistics information and remote trouble statistics information) is deleted meanwhile.

Example

The following example shows how to clear the OAM statistics information on interface GigaEthernet 0/2.

```
Switch#clear ethernet oam statistics interface g0/2
```

30.1.10 show ethernet oam discovery

Syntax

To display the OAM discovery information on all interfaces or a designated interface, including local DTE port loopback state, information about Local information TLV and Remote information TLV of OAM Information packet, run the following command.

show ethernet oam discovery interface [intf-type intf-id**]**

Parameters

Parameters	Description
Intf-id	Displays the Discovery information on the designated interface or on all protocol-up ports and enables the Discovery information on the OAM interface.

Default Value

None

Usage Guidelines

None

Example

The following example shows how to display OAM discovery information on port GigaEthernet 0/2.

```
Switch_config_g0/2#show ethernet oam discovery interface g0/2
GigaEthernet0/2
Local Info TLV
--------------
PDU revision:          1

Loopback status:     LB_DISABLED

OAM configurations field:
Mode                        : active
Unidirection           : not supported
Remote loopback     : supported
Link Events             : supported
Variable retrieval: not supported

Mtu size:                 1500

OUI:                         00e00f

Remote Info TLV
---------------
MAC address:               001b.0d9c.e703

PDU revision:          0

OAM configurations field:
Mode                        : active
Unidirection           : not supported
Remote loopback     : not supported
Link Events             : supported
Variable retrieval: not supported

Mtu size:                 1500

OUI:                         00000c
```

30.1.11 show ethernet oam statistics {pdu | link-monitor | remote-failure}

Syntax

To display the OAM statistics information on a designated interface or all interfaces, run the following command. The OAM statistics information includes packet type statistics information, general link event statistics information and remote fault statistics information

show ethernet oam statistics {pdu | link-monitor | remote-failure} interface [intf-type intf-id**]**

Parameters

Parameters	Description
Intf-id	Displays the statistics information on the designated interface or on all protocol-up ports and enables the statistics information on the OAM interface.

Default Value

None

Usage Guidelines

None

Example

The following example shows how to display the packet statistics information on interface GigaEthernet 0/2.

```
Switch#show ethernet oam statistics pdu interface g0/2
GigaEthernet0/2
Counters:
---------
Information OAMPDU Tx                 : 59
Information OAMPDU Rx                 : 56
Unique Event Notification OAMPDU Tx   : 0
Unique Event Notification OAMPDU Rx   : 0
Duplicate Event Notification OAMPDU TX: 0
Duplicate Event Notification OAMPDU RX: 0
Loopback Control OAMPDU Tx            : 0
Loopback Control OAMPDU Rx            : 0
Variable Request OAMPDU Tx            : 0
Variable Request OAMPDU Rx            : 0
Variable Response OAMPDU Tx           : 0
Variable Response OAMPDU Rx           : 0
Organization Specific OAMPDU Tx       : 0
Organization Specific OAMPDU Rx       : 0
Unsupported OAMPDU Tx                 : 0
Unsupported OAMPDU Rx                 : 0
Frames Lost due to OAM                : 0
```

30.1.12 show ethernet oam configuration

Syntax

To display the OAM configuration information on all interfaces or a designated interface, run the following command.

show ethernet oam configuration interface [intf-type intf-id**]**

Parameters

Parameters	Description
Intf-id	Displays the OAM configuration information on the designated interface or on all protocol-up ports and enables the configuration information on the OAM interface.

Default Value

None

Usage Guidelines

None

Example

The following example shows how to display the OAM configuration information on interface GigaEthernet 0/2.

```
Switch#show ethernet oam configuration interface g0/2
GigaEthernet0/2
General
-------
Admin state                : enabled
Mode                       : active
PDU max rate               : 10 packets/second
PDU min rate               : 1 seconds/packet
Link timeout               : 1 seconds
High threshold action: no action

Remote Failure
--------------
Link fault action      : no action
Dying gasp action      : no action
Critical event action: no action

Remote Loopback
---------------
Is supported               : supported
Loopback timeout           : 2

Link Monitoring
---------------
Negotiation                : supported
Status                     : on

Errored Symbol Period Event
Window                     : 10 * 100M symbols
Low threshold              : 1 error symbol(s)
High threshold             : none

Errored Frame Event
Window                     : 1 seconds
Low threshold              : 1 error frame(s)
High threshold             : none

Errored Frame Period Event
Window                     : 100 * 14881 frames
Low threshold              : 1 error frame(s)
```

```
High threshold          : none

Errored Frame Seconds Summary Event
Window                  : 60 seconds
Low threshold           : 1 error second(s)
High threshold          : none

Errored CRC Frames Event
Window                  : 1 seconds
Low threshold           : 10 error frame(s)
High threshold          : none
```

30.1.13 show ethernet oam runtime

Syntax

To display the OAM running information on all interfaces or a designated interface, run the following command. The OAM running information includes the control variables in some protocols and the latest 10 times status changing records.

show ethernet oam runtime interface [intf-type intf-id]

Parameters

Parameters	Description
Intf-id	Displays the Runtime information on the designated interface or on all protocol-up ports and enables the Runtime information on the OAM interface.

Default Value

None

Usage Guidelines

None

Example

The following example shows how to display the OAM Runtime information on interface GigaEthernet 0/2.

```
Switch#show ethernet oam runtime interface g0/2
GigaEthernet0/2
Runtime Settings:
-----------------
local_pdu               : NOT_WORKING
local_mux               : FWD
local_par               : FWD
local_link_status : OK
local_satisfied     : FALSE
local_stable          : FALSE
pdu_cnt                 : 10
pdu_timer               : stopped
lost_link_timer     : stopped
remote_state_valid: FALSE
remote_stable         : FALSE
remote_evaluating : FALSE

Discovery State Machine:
------------------------
Last 10 state transition recorded: INACTIVE -> FAULT -> ACTIVE_SEND_LOCAL -> SEN
D_LOCAL_REMOTE -> SEND_LOCAL_REMOTE_OK -> SEND_ANY -> INACTIVE
```

Chapter 31 Overview

Stipulation

Format Stipulation in the Command Line

Syntax	Meaning
Bold	Stands for the keyword in the command line, which stays unchanged and must be entered without any modification. It is presented as a bold in the command line.
{italic}	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the brace.
<italic>	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the point bracket.
[ ]	Stands for the optional parameter, which is in the square bracket.
{ x | y | ...}	Means that you can choose one option from two or more options.
[x | y | ...]	Means that you can choose one option or none from two or more options.
{ x | y | ...} *	Means that you has to choose at least one option from two or more options, or even choose all options.
[x | y | ...] *	Means that you can choose multiple options or none from two or more options.
&<1-n>	Means that the parameter before the "&" symbol can be entered 1～n times.
#	Means that the line starting with the "#" symbol is an explanation line.

CFM and Y1731 Configuration Commands

31.1 CFM Configuration Commands

31.1.1 Adding the Maintenance Domain and Entering the Maintenance Domain Mode

Syntax

To add a maintenance domain or enter the already existent maintenance domain, run the following command.

ethernet cfm md mdnf *{string}* **mdn** <*char_string*> [**level** <*0-7*> | **creation** <*MHF_creation_type*> | **sit** <*sender_id_type*> | **ip** <*IP_address*>]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
level	(optional parameter) Stands for the level of a maintenance domain. It is 0 by default.
creation	MIP It is none by default.
sit	Stands for the identifier type of the sender. It is none by default.
ip	(optional parameter) Stands for the IP address reported by the trouble alarm. It is 0.0.0.0 by default.

Command Mode

Global configuration mode

Example

```
Switch_config#ethernet cfm md mdnf string mdn customer level 5
```

Related Command

None

31.1.2 Deleting the Maintenance Domain

Syntax

To delete a designated maintenance domain, run the following command.

no ethernet cfm md mdnf *{string}* **mdn** <*char_string*>

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.

Command Mode

Global configuration mode

Example

```
Switch_config#no ethernet cfm md mdnf string mdn customer
```

Related Command

None

31.1.3 Browsing the Maintenance Domain

Syntax

To browse all the maintenance domains or the designated maintenance domains of the local device, run the following command.

show ethernet cfm md [mdnf *{string}* **mdn** <*char_string*>**]**

Parameters

Parameters	Description
mdnf	Stands for the format of the name of a to-be-browsed designated maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of a to-be-browsed designated maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.

Command Mode

EXEC, global, interface, maintenance domain

Example

```
Switch_config#show ethernet cfm md mdnf string mdn customer
```

Related Command

None

31.1.4 Adding a maintenance association

Syntax

To add a maintenance association, run the following command.

ma manf *{string}* **man** <*char_string*> **ci** *{100ms | 1s | 10s | 1min | 10min}* **meps** <*mepids*> [**vlan** <*1-4094*> | **creation** <*MHF_creation_type*> | **sit** <*sender_id_type*> | **ip** <*IP_address*>]

Parameters

Parameters	Description
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string mode.
ci	Stands for the transmission interval of CCM. The shortest transmission interval which is supported presently is 100ms.
meps	Stands for the MEPID of all MEPs in the local maintenance domain.
vlan	Stands for the identifier of the VLAN where the maintenance association is located. It is 1 by default.

Parameters	Description
creation	MIP It is none by default.
sit	Stands for the identifier type of the sender. It is none by default.
ip	(optional parameter) Stands for the IP address reported by the trouble alarm. It is 0.0.0.0 by default.

Command Mode

Maintenance domain mode

Example

```
Switch_config_cfm#ma manf string man customer1 ci 1s meps 1-2,2009 vlan 10
```

Related Command

None

31.1.5 Deleting the Maintenance Association

Syntax

To delete a designated maintenance association, run the following command.

no ma manf *{string}* man <*char_string*>

Parameters

Parameters	Description
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string mode.

Command Mode

Maintenance domain mode

Example

```
Switch_config_cfm#no ma manf string man customer
```

Related Command

None

31.1.6 Browsing the Maintenance Association

Syntax

To browse all or designated maintenance associations in a designated maintenance domain on the local device, run the following command.

show ethernet cfm ma mdnf *{string}* **mdn** <*char_string*> [**manf** {string} **man** <char_string>]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain where the to-be-browsed maintenance association is located. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain where the to-be-browsed maintenance association is located. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
manf	Stands for the format of the name of a to-be-browsed maintenance association. At present only the char-string format is supported.
man	Stands for the name of a to-be-browsed maintenance association. It is in character string mode.

Command Mode

EXEC, global, interface, maintenance domain

Example

```
Switch_config#show ethernet cfm ma mdnf string mdn customer manf string man customer1
```

Related Command

None

31.1.7 Adding MIP

Syntax

To add an MIP of a specific level, which belongs to a designated VLAN, on a specific interface, run the following command.

ethernet cfm mip add level *<0-7>* [**vlan** *<1-4094>*]

Parameters

Parameters	Description
level	Stands for the level of a maintenance domain.
vlan	Stands for the identifier of the VLAN where the maintenance association is located. It is 1 by default.

Command Mode

Physical interface configuration mode

Example

```
Switch_config_g0/1#ethernet cfm mip add level 1 vlan 10
```

Related Command

None

31.1.8 Deleting MIP

Syntax

To delete a designated MIP, run the following command.

ethernet cfm mip del vlan *<1-4094>*

Parameters

Parameters	Description
vlan	Stands for the identifier of the VLAN where MIP is located.

Command Mode

Interface configuration mode

Example

```
Switch_config_g0/1#ethernet cfm mip del vlan 10
```

Related Command

None

31.1.9 Browsing MIP

【Method 1】

Syntax

To browse all MIPs of a designated interface in the local device or MIPs in a specific VLAN, run the following command.

show ethernet cfm mip vlan *<1-4094>* **interface** *<interface_name>*

show ethernet cfm mip interface *<interface_name>*

Parameters

Parameters	Description
interface	Stands for a to-be-browsed interface.
vlan	Stands for the identifier of a to-be-browsed VLAN.

Command Mode

EXEC, global, interface, maintenance domain

Example

```
Switch_config#show ethernet cfm mip vlan 1 interface g0/1
```

Related Command

None

【Method 2】

Syntax

To browse all MIPs on the current interface of the local device, run the following command.

ethernet cfm mip display

Parameters

None

Command Mode

Physical interface mode

Example

```
Switch_config_g0/1#ethernet cfm mip display
```

Related Command

None

31.1.10 Adding MEP

Syntax

To add an MEP, which belongs to a designated maintenance association, on a specific interface, run the following command.

ethernet cfm mep add mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*> [**direction** *{up | down}* **| ip** <*ip_address*> **| lap** *{all | mac | rCCM | eCCM | xcon | none}*]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
mepid	Stands for the MEPID of the to-be-added MEP.
direction	(optional parameter) Stands for the direction of the to-be-added MEP. It is down by default.
ip	(optional parameter) Stands for the IP address reported by the trouble alarm. It is 0.0.0.0 by default.
lap	Stands for the lowest priority of trouble report. It is all by default.

Command Mode

Physical interface configuration mode

Example

```
Switch_config_g0/1#ethernet cfm mep add mdnf string mdn customer manf string man customer1 mepid 2009 direction up lap all
```

Related Command
None

31.1.11 Deleting MEP

Syntax

To delete a designated MEP, run the following command.

ethernet cfm mep del mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*>

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
mepid	Stands for the MEPID of the to-be-added MEP.

Command Mode

Physical interface configuration mode

Example

```
Switch_config_g0/1#ethernet cfm mep del mdnf string mdn customer manf string man customer1 mepid 2009
```

Related Command

None

31.1.12 Browsing MEP

【Method 1】

Syntax

To browse the detailed or brief information about all MEPs in the designated maintenance domain of the local device, or that about a specific MEP, run the following command.

show ethernet cfm mep mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> [**mepid** <*1-8191*>] [**view** *{detail | brief}*]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
mepid	Stands for the MEPID of the to-be-browsed MEP.
view	Means to browse the detailed information or the brief information. It is the detailed information that will be browsed by default.

Command Mode

EXEC, global, interface, maintenance domain

Example

```
Switch_config#show ethernet cfm mep mdnf string mdn x manf string man x view brief
```

Related Command

None

【Method 2】

Syntax

To browse all MEPs on the current interface of the local device, run the following command.

ethernet cfm mep display

Parameters

None

Command Mode

Physical interface mode

Example

```
Switch_config_g0/1#ethernet cfm mep display
```

Related Command

None

31.2 Y1731 Configuration Commands

31.2.1 Modifying the transmission interval of the AIS frame

Syntax

To modify the transmission interval of AIS frame, run the following command.

ethernet y1731 ais-mep timer *time*

To set the default transmission interval, run the following command.

[**no**] **ethernet y1731 ais-mep timer**

Parameters

Parameters	Description
time	Stands for the transmission interval of the AIS frame. The value ranges: <1> -- 1 frame per second <2> -- 1 frame per minute. The default transmission value is 1 second.

Default Value

The default transmission interval is one frame every second.

Command Mode

Global configuration mode

Usage Guidelines

If a current device supports Eth-AIS and have to go through 4094 VLANs, the AIS frames it sends every second may cause tension. Therefore, the current device has to support another AIS transmission period based on one minute. The AIS frame exchanges the AIS transmission interval through its period field.

Example

The following example shows how to modify the transmission interval of the AIS frame to 1 minute.

```
Switch#
Switch#config
Switch_config#ethernet y1731 ais-mep timer 2
Switch_config#
```

31.2.2 Enabling the bidirectional delay measurement

Syntax

To enable the bidirectional delay measurement, run the following command.

ethernet y1731 delay-measurement [-n *number***]*** *MEGID* { **aimmep** *MEPID* | *macaddr* }

Parameters

Parameters	Description
-n *number*	(optional parameter) means the number of the to-be-transmitted LBM packets. Value range: 1-65534 (transmit 5 packets by default)
MEGID	Stands for the name of MEG, which is a character string with a length of 1 to 13.
MEPID	Stands for the identifier of the destination MEP.
macaddr	Stands for the MAC address of the destination of MEP/MIP.

Default Value

Five LBM packets are transmitted by default.

Command Mode

EXEC mode

Usage Guidelines

The frame delay measurement can only be conducted between two peer MEPs. The bidirectional frame delay measurement can be used to measure the bidirectional frame delay and the delay variable.

Example

The following example shows how to create a point-to-point MEG whose local MEP is MEP 111 and whose remote MEP is MEP 222. In this example, MEG first gets its CC function to run, then learns the MAC address of the peer MEP and finally the local MEP executes the bidirectional DM operation towards the remote MEP.

```
Switch_config#ethernet  cfm  enable
Switch_config# ethernet cfm md mdnf STRING mdn t level 1
Switch_config_cfm# ma manf STRING man t meps 1-3 ci 10s vlan 1
Switch_config#interface  g0/2
Switch_config_g0/2# ethernet cfm ENABLE
Switch_config_g0/2# ethernet cfm mep add mdnf STRING mdn t manf STRING man t mepid 1
Switch_config_g0/2#ethernet cfm mep ENABLE mdnf STRING mdn t manf STRING man t mepid 1
Switch_config_g0/2#ethernet cfm mep cci-ENABLE mdnf STRING mdn t manf STRING man t mepid 1
Switch_config_g0/2#exit
Switch_config#exit
  Switch#ethernet y1731 delay-measurement aaa aimmep 2 mac 00E0.0F5F.7459
  Two-way delay measurement MEG: aaa Local MEP: 1 Aimaddress: 00E0.0F5F.7459
  Switch_config#
  -- delay measurement statistics--
    Packets: send = 5, Received = 5, Lost = 0(0/5 loss)
  -- Approximate round trip times in milli-seconds:
    MINFD = 0ms, MAXFD = 0ms, Average = 0ms
    MINFDV = 0ms, MAXFDV = 0ms
```

31.2.3 Enabling the Ethernet loopback function of the unicast

Syntax

To enable the Ethernet loopback function of the unicast (an operation conducted towards the MAC address of the peer MEP/MIP), run the following command.

ethernet y1731 delay-measurement [-n *number***]*** *MEGID* {**aimmep** *MEPID*| *macaddr*} **one-way**

Parameters

Parameters	Description
-n *number*	(optional parameter) means the number of the to-be-transmitted LBM packets. Value range: 1-65534 (transmit 5 packets by default)
MEGID	Stands for the name of MEG, which is a character string with a length of 1 to 13.
MEPID	Stands for the identifier of the destination MEP.
macaddr	Stands for the MAC address of the destination of MEP/MIP.

Default Value

Five 1DM packets are transmitted by default.

Command Mode

EXEC mode

Usage Guidelines

The frame delay measurement can only be conducted between two peer MEPs. After the one-way delay measurement is enabled, the local MEP will transmit the 1DM packets to the peer MEP continuously. The one-way frame delay measurement can be used to measure the one-way frame delay variable only when the clock systems at two terminals synchronize.

Example

The following example shows how to create a point-to-point MEG whose local MEP is MEP 111 and whose remote MEP is MEP 222. In this example, the MAC address of MEP 222 is 00E0.0F5F.7459, and MEP 111 will conduct the one-way DM operation towards the remote MEP, MEP 222.

```
Switch#ethernet y1731 delay-measurement aaa 00E0.0F5F.7459 one-way
Switch#
Send 5 packets, One-way ETH-DM Terminate.
```

31.2.4 Conducting the termination command

Syntax

To conduct the termination command, run the following command
ethernet y1731 terminate

Parameters

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to disable the delay-measurement function.

Example

The following example shows how to terminate the operation which is running in EXEC configuration mode:

```
Switch#
Switch#ethernet y1731 terminate
Switch#
```

31.3 CFM Maintenance Commands

31.3.1 loopback

Syntax

To use a designated MEP at the local terminal to conduct loopback towards another designated MEP at the remote terminal, run the following command.

ethernet cfm loopback mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*> **mac** <*AA:BB:CC:DD:EE:FF*> [**number** <*1-64*>]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
mepid	Stands for the MEPID of the local MEP.
mac	Stands for the MAC address of the remote MEP.
number	(optional parameter) Stands for the times of conducting loopback. It is 3 by default.

Command Mode

EXEC

Example

```
Switch#ethernet cfm loopback mdnf string mdn x manf string man x mepid 1 mac 00:15:E9:43:AD:E3 number 3
```

Related Command

None

31.3.2 linktrace

Syntax

To use a designated local MEP to conduct linktrace towards a designated remote MEP, run the following command.

ethernet cfm linktrace mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*> **mac** <*AA:BB:CC:DD:EE:FF*> [**ttl** *{1-255}* | **fdb-only** *{yes}*]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
mepid	Stands for the MEPID of the local MEP.
mac	Stands for the MAC address of the remote MEP.
ttl	(optional parameter) Stands for the tt1 value. It is 64 by default.
fdb-only	(optional parameter) Means to use the forward database or not. It is yes by default.

Command Mode

EXEC

Example

```
Switch#ethernet cfm linktrace mdnf s mdn x manf string man x mepid 1 mac 00:15:E9:43:AD:E3 ttl 64
```

Related Command

None

31.3.3 Deleting the Linktrace Result Table

Syntax

To delete the linktrace result table of a designated MEP, run the following command.

clear ethernet cfm linktrace mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> [**mepid** <*1-8191*>]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
mepid	Stands for the MEPID of the local MEP.

Command Mode

EXEC

Example

```
Switch#clear ethernet cfm linktrace mdnf string mdn x manf string man x mepid 1
```

Related Command

None

31.3.4 Setting the Size of the Linktrace Result Table

Syntax

To set the size of the linktrace result table (that is, the number of linktraces which can be conducted concurrently), run the following command.

ethernet cfm linktrace table-size *<1-16>*

Parameters

Parameters	Description
table-size	Stands for the size of the linktrace result table.

Command Mode

Global configuration mode

Example

```
Switch_config#ethernet cfm linktrace table-size 1
```

Related Command

None

31.3.5 Setting the Number of Entries in the Linktrace Result Table

Syntax

To set the maximum number of entries that are received each time by the linktrace result table, run the following command.

ethernet cfm linktrace entry-number *<2-4095>*

Parameters

Parameters	Description
entry-number	Stands for the number of the entries in the linktrace result table.

Command Mode

Global configuration mode

Example

```
Switch config#ethernet cfm linktrace entry-number 2009
```

Related Command

None

31.3.6 Setting the aging time of the linktrace result table

Syntax

To set the maximum number of entries that are received each time by the linktrace result table (Unit: min), run the following command.

ethernet cfm linktrace hold-time *<1-29>*

Parameters

Parameters	Description
hold-time	Stands for the aging time of the linktrace result table. Unit: minute

Command Mode

Global configuration mode

Example

```
Switch_config#ethernet cfm linktrace hold-time 10
```

Related Command

None

31.3.7 Deleting the MEP Statistics Data

Syntax

To delete the statistics data of a designated MEP, run the following command.

ethernet cfm mep clear mdnf *{string}* **mdn** *<char_string>* **manf** *{string}* **man** *<char_string>* **mepid** *<1-8191>*

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
mepid	Stands for the MEPID of a designated MEP.

Command Mode

Physical interface mode

Example

```
Switch_config_g0/1#ethernet cfm mep clear mdnf string mdn x manf string man x mepid 1
```

Related Command

None

31.4 CFM Control Commands

31.4.1 CFM Stack Control Command

Syntax

To enable or disable the whole CFM protocol stack, run the following command.

ethernet cfm *{enable | disable}*

Parameters

None

Command Mode

Global configuration mode

Example

```
Switch_config#ethernet cfm enable
```

Related Command

None

31.4.2 CFM Interface Control Command

Syntax

To enable or disable the CFM function of the current interface, run the following command.

ethernet cfm *{enable | disable}*

Parameters

None

Command Mode

Physical interface mode

Example

```
Switch_config_g0/1#ethernet cfm enable
```

Related Command

None

31.4.3 MIP Control Command

Syntax

To enable or disable the MIP of a designated VLAN on the current interface, run the following command.

ethernet cfm mip *{enable | disable}* **vlan** *<1-4094>*

Parameters

None

Command Mode

Physical interface mode

Example

```
Switch_config_g0/1#ethernet cfm mip enable vlan 1
```

Related Command

None

31.4.4 MEP Control Command

Syntax

To enable or disable a designated MEP, run the following command.

ethernet cfm mep *{enable | disable}* **mdnf** *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*>

Parameters

None

Command Mode

Physical interface mode

Example

```
Switch_config_g0/1#ethernet cfm mep enable mdnf string mdn x manf string man x mepid 1
```

Related Command

None

31.4.5 CC Control Command

Syntax

To enable or disable the CCM transmission function of a designated MEP, run the following command.

ethernet cfm mep *{cci-enable | cci-disable}* **mdnf** *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*>

Parameters

None

Command Mode

Physical interface mode

Example

```
Switch_config_g0/1#ethernet cfm mep cci-disable mdnf string mdn x manf string man x mepid 1
```

Related Command

None

31.5 CFM Query Commands

31.5.1 Browsing the CFM Protocol Stack

Syntax

To browse the CFM protocol stack, run the following command.

show ethernet cfm stack

Parameters

None

Command Mode

Non-user mode

Example

```
Switch_config#show ethernet cfm stack
```

Related Command

None

31.5.2 Browsing the CFM Interface

Syntax

To check the relevant information of CFM interface, run the following command.

show ethernet cfm interface [<*interface_name*>]

Parameters

None

Command Mode

Non-user mode

Example

```
Switch_config#show ethernet cfm interface g0/1
```

Related Command

None

31.5.3 Browsing the Locally Stored Information about the Remote MEP

Syntax

To browse the detailed or brief information about all remote MEPs, which together with a designated local MEP belong to the same maintenance association, or about a designated remote MEP, run the following command.

show ethernet cfm rmep mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> [**mepid** <*1-8191*>] [**rmepid** <*1-8191*>] [**view** *{detail | brief}*]

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
mepid	Stands for the MEPID of the local MEP, which together with the to-be-browsed remote MEP belongs to the same maintenance association.
rmepid	Stands for the MEPID of the to-be-browsed remote MEP.
view	Means to browse the detailed information or the brief information. It is the detailed information that will be browsed by default.

Command Mode

Non-user mode

Example

```
Switch_config#show ethernet cfm rmep mdnf string mdn x manf string man x mepid 1 rmepid 2 view brief
```

Related Command

None

31.5.4 Browsing the LinkTrace Result Table

Syntax

To browse the linktrace result table which is carried out by a specified TID of a specific MEP, run the following command.

show ethernet cfm linktrace mdnf *{string}* **mdn** <*char_string*> **manf** *{string}* **man** <*char_string*> **mepid** <*1-8191*> **tid** <*0-4294967295*>

Parameters

Parameters	Description
mdnf	Stands for the format of the name of the maintenance domain. At present only the char-string format is supported.
mdn	Stands for the name of the maintenance domain. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
manf	Stands for the format of the name of the maintenance association. At present only the char-string format is supported.
man	Stands for the name of the maintenance association. It is in character string format with 1 to 42 printable characters and all characters should be capital sensitive.
mepid	Stands for the MEPID of the local MEP, which together with the to-be-browsed remote MEP belongs to the same maintenance association.
tid	Stands for the TID that is returned during linktrace.

Command Mode

Non-user mode

Example

```
Switch_config#show ethernet cfm linktrace mdnf string mdn x manf string man x mepid 1 tid 19830719

**** [RESULT FOR READING LINKTRACE REPLY] ****

                ================================================
                                ID :0x12E97BF (19830719)【Event ID of the presently running LT】
                                TTL :0x00000004(4)  【TTL value of the presently running LT】
                            TOTAL LTRs:1【LTRs returned by the remote terminal of the result table】
                              MAX LTRs:100【receiving at most 100 LTRs】
                            NEXT ORDER:2【The next expected LTR order ID】

                                【The total information of one Linktrace is shown above】
                ==================== LTRs ====================

                                order:1【Order ID of this LTR】
                                  TTL:3【TTL vlaue in the responsed LTRs】
                                FwdYes:NO【Whether the local node forwards LTM】
                             TerminalMEP:NO【Whether the local node is the terminal MEP】
                          Last Egress ID:0 - 00:E0:0F:DC:02:11【MAC of the previous hop】
                          Next Egress ID:0 - 00:00:00:00:00:00【MAC of the next hop, and if the result is 0 it means there is no
next hop】
                             Relay Action:(1)HIT【Field of the Relay action: HIT means just hitting successively】
                          Ingress Action:OK(1)【state of the ingress port: OK】
                    Ingress MAC Address:00:E0:0F:81:11:1C【MAC of the ingress port】
```

```
Ingress Port ID format:MAC-ADDRESS(3)【ID format of the ingress port: MAC format】
Ingress Port ID (hex):00 E0 0F 81 11 1C【Identifier of the ingress port：00 E0 0F 81 11 1C】
```

Related Command

None

31.5.5 Browsing the whole running status of CFM

Syntax

To browse the whole running status of CFM, run the following command.

show ethernet cfm running-info

Parameters

None

Command Mode

All modes except the user mode

Example

```
Switch_config#show ethernet cfm running-info
```

Related Command

None

31.6 Y.1731 Show Command

31.6.1 Showing the statistics about the one-way delay measurement

Syntax

To show the statistics about the one-way delay measurement, run the following command.

show ethernet y1731 delay-measurement *MEGID*

Parameters

Parameters	Description
MEGID	Stands for the name of MEG, which is a character string with a length of 1 to 13.

Default Value

None

Usage Guidelines

This command is used to only display the statistics of the one-way delay measurement.

Example

The following example shows how to display the statistics of the one-way delay measurement of MEG aaa in EXEC or global mode.

```
Switch#show ethernet y1731 delay-measurement aaa
MEG one way delay measurement:
        FDV current: 0ms
        FDV min: 0ms
        FDV max: 0ms
Switch#
```

31.6.2 Showing the information of MEG continuous detection

Syntax

To show the information of MEG continuous detection, run the following command.

show ethernet y1731 detect *MEGID* **[***MEPID***]**

Parameters

Parameters	Description
MEGID	Displays the detection information about the designated MEG.
MEPID	(optional parameter) Stands for the identifier of MEP should be known well.

Default Value

None

Usage Guidelines

When MEPID is not entered, the detection information about all local MEPs of MEG will be shown.

Example

The following example shows the fault detection of MEP 111 of MEG aaa.

```
Switch_config#show ethernet y1731 detect bbb 2
Ethernet Continuity Check:
        (F)Fail, stand for defect exist
        (N)Normal, stand for defect inexistence
LocMEP CC-Status   SFAIL LOC    MIS    UMEP   UMEL   UPER   AIS    RDI    LCK
2          Enabled      N       N      N      N      N      N      N      N      N
LocMEP   PeerMEP RDI       LOC       MAC
2          1             N         N         00E0.0FD2.FE17
```

31.6.3 Displaying the configuration of MEP and MIP on a port

Syntax

To display the configuration of MEP and MIP on a port, run the following command.

show ethernet y1731 interface *interface-name*

Parameters

Parameters	Description
interface-name	Name of the interface, such as f0/1 and fastethernet0/1

Default Value

None

Usage Guidelines

None

Example

```
Switch_config#show ethernet y1731 interface g0/4
GigaEthernet0/4:
MEP list:
    MEGID          MEPID   Level   Vlanid  MAC                 Direction
    bbb            2       3       1       00E0.0F68.7FBA      DOWN
MIP list:
    Type    Level   MAC
    MIP     4       00E0.0F68.7FBE
Switch_config#
```

31.6.4 Displaying the configuration of all MEG or the detailed configuration about a certain MEG

Syntax

To display the configuration of all MEG or the detailed configuration about a certain MEG, run the following command.

show ethernet y1731 meglist **[** *MEGID* **]**

Parameters

Parameters	Description
MEGID	Displays the detailed information about the designated MEG.

Default Value

None

Usage Guidelines

If MEGID is not entered, the information about all MEGs will be displayed.

Example

```
Switch_config#show ethernet y1731 meglist
MEG list:
    MEGID              Level    Vlan
    aaa                3        1
    bbb                3        1
    ccc                1        1
Total entries displayed: 3
Switch_config#show ethernet y1731 meglist aaa
MEG ID: aaa          Level: 3   Vlan: 1      CC-Status: Enabled
MEP mep: 1-2
Local MEP list:
    MEPID   Port        MAC                 Direction
    2       Fas0/8      00E0.0F5F.745D      UP
```

31.6.5 Displaying the information about all configured MIPs

Syntax

To display the information about all configured MIPs, run the following command.

show ethernet y1731 miplist

Parameters

None

Default Value

None

Usage Guidelines

None

Example

```
Switch_config#
Switch_config#show ethernet y1731 miplist
MIP list:
Type    Level   Port        MAC
MIP     7       Fas0/4      00E0.0FC1.003A
```

```
MIP     5       Fas0/1      00E0.0FC1.0037
```

31.6.6 Displaying some statistics of Y.1731 module

Syntax

To display some statistics information about the Y.1731 module, including statistics of the received and transmitted OAM packets and the system error, run the following command.

show ethernet y1731 traffic

Parameters

None

Default Value

None

Usage Guidelines

None

Example

```
Switch_config#
Switch_config#show ethernet y1731 traffic
ethernet y1731 traffic/errors:
        Total output CCM frames: 223933
        Total output LBM frames: 67
        Total output LTM frames: 41
        Total output AIS frames: 0
        Total output 1DM frames: 1067
        Total output DMM frames: 60
        Total input CCM frames: 160778
        Total input LBM frames: 30
        Total input LBR frames: 67
        Total input LTM frames: 0
        Total input LTR frames: 41
        Total input AIS frames: 0
        Total input 1DM frames: 0
        Total input DMM frames: 0
        Total input DMR frames: 60
        Total memory allocation failures: 0
```

```
        Total system failures: 0
Switch_config#
```

31.7 Y1731 Clear Command

31.7.1 Deleting the transmission statistics information about the OAM packets and the system error information

Syntax

To delete the transmission statistics information about the OAM packets and the system error information, run the following command.

clear ethernet y1731 counters

Parameters

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC

Example

The command is used to delete the transmission statistics information about the OAM packets and the system error information.

```
Switch#clear ethernet y1731 counters
```

31.7.2 Deleting the statistics information about the one-way delay measurement carried out by a designated MEG

Syntax

To delete the statistics information about the one-way delay measurement carried out by a designated MEG, run the following command.

clear ethernet y1731 delay-measurement *MEGID*

Parameters

Parameters	Description
MEGID	Stands for the name of MEG, which is a character string with a length of 1 to 13.

Default Value

None

Usage Guidelines

None

Command Mode

EXEC

Example

The following example shows how to delete the statistics information about the one-way delay measurement carried out by MEG aaa.

```
Switch#clear ethernet y1731 delay-measurement aaa
```

Chapter 32 DHCP-relay Snooping Configuration Commands

The DHCP-relay snooping configuration commands include:

- ip dhcp-relay snooping
- ip dhcp-relay snooping vlan
- ip dhcp-relay snooping database-agent
- ip dhcp-relay snooping db-file
- ip verify source vlan
- ip arp inspection vlan
- ip source binding
- arp inspection trust
- dhcp snooping trust
- ip-source trust
- show ip dhcp-relay snooping
- show ip dhcp-relay snooping binding
- debug ip dhcp-relay snooping
- debug ip dhcp-relay event
- debug ip dhcp-relay binding

32.1.1 ip dhcp-relay snooping

Syntax

To enable or disable the DHCP-relay snooping function in a VLAN, run ip dhcp-relay snooping. To resume the corresponding default settings, run no dhcp-relay snooping.

ip dhcp-relay snooping

no ip dhcp-relay snooping

Parameters

None

Default Value

The dhcp-relay snooping function is disabled by default.

Usage Guidelines

None

Example

The following example shows how to enable the DHCP snooping function:

```
Switch_config#ip dhcp-relay snooping
Switch_config#
```

32.1.2 ip dhcp-relay snooping vlan

Syntax

ip dhcp-relay snooping vlan *vlan_id*

no ip dhcp-relay snooping vlan *vlan_id*

Parameters

Parameters	Description
vlan_id	Stands for the ID of a VLAN. Value range: 1-4094

Default Value

None

Usage Guidelines

This command is used to configure the VLAN of DHCP snooping.

Example

The following example shows how to enable snooping detection for DHCP packets on VLAN 2.

```
Switch_config#ip dhcp-relay snooping vlan 2
Switch_config#
```

32.1.3 ip dhcp-relay snooping vlan vlan_id max-client

Syntax

ip dhcp-relay snooping vlan *vlan_id* **max-client** *number*

no ip dhcp-relay snooping vlan *vlan_id* **max-client**

Parameters

Parameters	Description
Vlan id	Stands for the ID of a VLAN. Value range: 1-4094
number	Allowable maximum number of users: 0-65535

Default Value

The default maximum number of users is 65535.

Usage Guidelines

You can use this command to set the maximum users in a VLNA of DHCP snooping. During this settings, the principle "first come and first be distributed" will be followed. When the number of users in the VLAN reaches the maximum value, new clients are then forbidden to distribute.

Example

The following example shows that snooping check will be conducted towards the DHCP packets in VLAN2 and the allowable maximum number of users is 3.

```
Switch_config#ip dhcp-relay snooping vlan 2 max-client 3
```

```
Switch_config#
```

32.1.4 ip dhcp-relay snooping database-agent

Syntax

To bind DHCP snooping to standby TFTP server, run ip dhcp-relay snooping database-agent A.B.C.D.

ip dhcp-relay snooping database-agent *A.B.C.D*

no ip dhcp-relay snooping database-agent *A.B.C.D*

Parameters

Parameters	Description
A.B.C.D	Means the IP address of the TFTP server.

Default Value

There is no standby servers by default.

Usage Guidelines

If the address of the TFTP server is not configured, the binding backup is not conducted.

Example

The following example shows how to set the address of a server of backing up DHCP snooping binding to 192.168.1.1.

```
Switch_config#ip dhcp-relay snooping database-agent 192.168.1.1
Switch_config#
```

32.1.5 ip dhcp-relay snooping db-file

Syntax

ip dhcp-relay snooping db-file *name [timestamp]*

no ip dhcp-relay snooping db-file *[timestamp]*

Parameters

Parameters	Description
Name	File name which is saved during DHCP snooping binding backup.
timestamp	Timestamp which is the file name of the binding backup.

Default Value

There is no file.

Usage Guidelines

If the file name is not configured, the binding backup is not conducted.

Example

The following example shows how to set the file name of binding backup to dhcp_binding.txt.

```
Switch_config#ip dhcp-relay snooping db-file dhcp_binding.txt
Switch_config#
```

32.1.6 ip dhcp-relay snooping write-time

Syntax

ip dhcp-relay snooping write-time *num*

no ip dhcp-relay snooping write-time

Parameters

Parameters	Description
Num	Stands for the interval of backing up the DHCP snooping binding (2-1440).

Default Value

The default value of the interval is 30 minutes.

Usage Guidelines

The binding update will be checked during interval configuration. If the binding is updated, the binding information need be backed up.

Example

The following example shows how to set the interval of backing up the binding to 60 minutes.

```
Switch_config#ip dhcp-relay snooping write-time 60
Switch_config#
```

32.1.7 ip dhcp-relay snooping write-immediately

Syntax

ip dhcp-relay snooping write-immediately

no ip dhcp-relay snooping write-immediately

Parameters

None

Default Value

None

Usage Guidelines

If there is entry update, it will write into the entry database immediately. It is recommended that the function is not enabled when there is plenty of entries. Otherwise, the performance may be affected.

Example

The following example shows how to backup the binding entry after the configuration is updated.

```
Switch_config#ip dhcp-relay snooping write-immediately
Switch_config#
```

32.1.8 ip dhcp-relay snooping log

Syntax

ip dhcp-relay snooping log

no ip dhcp-relay snooping log

Parameters

None

Default Value

None

Usage Guidelines

After the log function is enabled, the syslog will report if there is packets of dhcp server on non-trust port, which indicates that there is illegal dhcp server on the port reporting syslog.

Example

The following example shows how to enable the DHCP-relay snooping function:

```
Switch_config#ip dhcp-relay snooping log
Switch_config#
```

32.1.9 ip dhcp-relay snooping rapid-refresh-bind

Syntax

To enable rapid update of DHCP snooping, run ip dhcp-relay snooping rapid-refresh-bind.

ip dhcp-relay snooping rapid-refresh-bind

no ip dhcp-relay snooping rapid-refresh-bind

Parameters

None

Default Value

None

Usage Guidelines

After this function is enabled, the DHCP attack of fake MAC will be closed; when the client is allowed to change the access port, the IP address can be directly acquired without waiting for the expiration of the IP lease.

If the client change the access port after the function is disabled, the device enabling snooping will take it as dhcp packet attack of fake mac and the dhcp packet will be dropped.

Example

None

32.1.10 dhcp-relay snooping information option

Syntax

ip dhcp-relay snooping information option [format snmp-ifindex | manual | hn-type [host]]

no ip dhcp-relay snooping information option [format snmp-ifindex | manual | hn-type [host]]

Parameters

Parameters	Description
format snmp-ifindex	Fills in option 82 in SNMP ifindex mode (optional).
format manual	Uses the manual configuration to fill in option82 (optional).
format hn-type [host]	Uses the Cisco format to enter option82 (optional). Host means the configuration device is the master switch.

Default Value

Option 82 will not be added to or removed from the report by default.

Usage Guidelines

This command is used to set whether DHCP option82 can be handled when a switch is conducting DHCP snooping. If format snmp-ifindex is specified, you should use SNMP ifindex to fill in option82; if format manual is specified, you should use the character string, which is set by the command "dhcp snooping information circuit-id string" on all ports, to full in the circuit-id option of option82; in other cases, fill in option82 according to the rules of RFC3046.

Example

The following example shows how to fill in option 82 in SNMP ifindex mode.

```
Switch_config#ip dhcp-relay snooping
Switch_config#ip dhcp-relay snooping information option format snmp-ifindex
```

The following example shows how to fill in option 82 in manual mode.

```
Switch_config#ip dhcp-relay snooping
Switch_config#ip dhcp-relay snooping vlan [WORD]      //[WORD] stands for the vlan name for start up the snooping
function.
Switch_config# ip dhcp-relay snooping information option format manual
```

32.1.11 ip verify source vlan

Syntax

ip verify source vlan *vlanid*

no ip verify source vlan *vlanid*

Parameters

Parameters	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094

Default Value

None

Usage Guidelines

This command is used to configure a VLAN for monitoring the source IP address. The "no" form of this command is used to cancel this VLAN. If the source IP address and source MAC address of the IP packet is not the client's legal address, which is distributed by the DHCP server and listened by DHCP snooping, the vlan in which IP source address will take the kind of packets as illegal ones and drop them.

Example

The following example shows how to conduct source IP address monitoring to the packets from all physical interfaces (except trusted interfaces) in VLAN2.

```
Switch_config#ip verify source vlan 2
Switch_config#
```

32.1.12 ip arp inspection vlan

Syntax

ip arp inspection vlan *vlanid*

no ip arp inspection vlan *vlanid*

Parameters

Parameters	Description
vlanid	Stands for the ID of a VLAN. Value range: 1-4094

Default Value

None

Usage Guidelines

This command is used to configure a VLAN for monitoring the source address of the ARP packet. The "no" form of this command is used to cancel this VLAN. In the VLAN where monitoring the source address of the ARP packets is enabled, if SIP and SMAC of an ARP packet, which correspond to the IP address and MAC address of the client that the DHCP server distributes to the client, are unsuitable, the ARP packet will be dropped.

Example

The following example shows how to conduct source address monitoring to the ARP packets from all physical interfaces (except trusted interfaces) in VLAN2.

```
Switch_config#ip arp inspection vlan 2
Switch_config#
```

32.1.13 ip source binding

Syntax

To add MAC-to-IP binding to an interface, run ip source binding xx-xx-xx-xx-xx-xx A.B.C.D interface name.

ip source binding *xx:xx:xx:xx:xx:xx A.B.C.D* **interface** *name* **vlan** *vlan-id*

no ip source binding *xx:xx:xx:xx:xx:xx A.B.C.D* **vlan** *vlan-id*

Parameters

Parameters	Description
xx:xx:xx:xx:xx:xx	MAC Address
A.B.C.D	IP address
Name	Means a name of an interface.
vlan-id	Stands for VLAN ID.

Default Value

None

Usage Guidelines

None

Example

The following example shows how to bind MAC address 08:00:3e:00:00:01 to IP address 192.168.1.2 on interface GigaEthernet0/1.

```
Switch_config#ip source binding    08:00:3e:00:00:01 192.168.1.2 interface GigaEthernet0/1
Switch_config#
```

32.1.14 arp inspection trust

Syntax

arp inspection trust

no arp inspection trust

Parameters

None

Default Value

The default interface is a distrusted one.

Usage Guidelines

The ARP monitoring is not conducted to the ARP-trusted interface. The "no" form of this command is used to configure the default value of this interface.

Example

The following example shows how to set interface GigaEthernet 0/1 to an ARP-trusted interface.

```
Switch_config_g0/1#arp inspection trust
```

32.1.15 dhcp snooping trust

Syntax

dhcp snooping trust

no dhcp snooping trust

Parameters

None

Default Value

The default interface is a distrusted one.

Usage Guidelines

DHCP snooping is not conducted to the DHCP-trusted interface. The "no" form of this command is used to resume the default value of this interface.

Example

The following example shows how to set interface GigaEthernet 0/1 to an DHCP-trusted interface.

```
Switch_config_g0/1#dhcp snooping    trust
```

32.1.16 dhcp snooping deny

Syntax

dhcp snooping deny

no dhcp snooping deny

Parameters

None

Default Value

Snooping monitoring is allowed on the default interface.

Usage Guidelines

After this command is configured, DHCP snooping trust, IP-sourcetrust and ARP inspection trust are automatically enabled. The "no" form of this command is used to configure the default value of this interface.

Example

The following example shows how to disable DHCP snooping on interface GigaEthernet0/1.

```
Switch_config_g0/1#dhcp snooping deny
```

32.1.17 dhcp snooping information circuit-id

Syntax

dhcp snooping information circuit-id {**string** *STRING* | **hex** *xx-xx-xx-xx-xx-xx*}

Parameters

Parameters	Description
string *STRING*	Stands for the character string carried by the sub-option of option82 circuit-id.
hex *xx-xx-xx-xx-xx-xx*	Stands for the hexadecimal character string carried by the sub-option of option82 circuit-id.

Default Value

None

Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (the switch of manually set optio82 need be opened. See the command, ip dhcp-relay snooping information option format manual)

Example

The following example shows how to set option82 to group1 manually on interface g0/3, which belongs to interface g0/3.

```
Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 1

Switch_config#ip dhcp-relay snooping information option format manual

Switch_config#interface g0/3

Switch_config_g0/3#dhcp snooping information circuit-id string group1
```

32.1.18 dhcp snooping information remote-id string

Syntax

dhcp snooping information remote-id {**string** *STRING* | **hex** *xx-xx-xx-xx-xx-xx*}

Parameters

Parameters	Description
string STRING	Stands for the character string carried by option82 remote-id.
hex xx-xx-xx-xx-xx-xx	Stands for the hexadecimal character string carried by the sub-option of option82 remote-id.

Default Value

None

Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (the switch of manually set optio82 need be opened. See the command, ip dhcp-relay snooping information option format manual)

Example

The following example shows how to set option82 to group1 manually on interface g0/3, which belongs to interface g0/3.

```
Switch_config# ip dhcp-relay snooping

Switch_config# ip dhcp-relay snooping vlan 1

Switch_config#ip dhcp-relay snooping information option format manual

Switch_config#interface g0/3

Switch_config_g0/3# dhcp snooping information remote-id string group1
```

32.1.19 dhcp snooping information vendor-specific

Syntax

dhcp snooping information vendor-specific { string *STRING* **| hex** *xx-xx-xx-xx-xx-xx* **}**

Parameters

Parameters	Description
string STRING	Stands for the character string carried by option82 verdor-specific.
hex xx-xx-xx-xx-xx-xx	Stands for the hexadecimal character string carried by the sub-option of option82 verdor-specific.

Default Value

None

Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (the switch of manually set optio82 need be opened. See the command, ip dhcp-relay snooping information option format manual)

Example

The following example shows how to use the hexadecimal 00-00-00-09-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34 to set option82 option vendor-specific (suboption 9)

```
Switch_config# ip dhcp-relay snooping

Switch_config# ip dhcp-relay snooping vlan 1

Switch_config#ip dhcp-relay snooping information option format manual

Switch_config#interface g0/3

Switch_config_g0/3# dhcp snooping information vendor-specific hex
00-00-00-09-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34
```

32.1.20 dhcp snooping information append

Syntax

dhcp snooping information append

dhcp snooping information append first-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| hostname | vlanip }**

dhcp snooping information append second-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| hostname | vlanip }**

no dhcp snooping information append

no dhcp snooping information append first-subop9-param

no dhcp snooping information append second-subop9-param

Parameters

Parameters	Description
first-subop9-param hex [*xx-xx-xx-xx-xx-xx*]	Stands for the Hex system of the first parameter carried by option82 vendor-specific (suboption9).
second-subop9-param hex [*xx-xx-xx-xx-xx-xx*]	Stands for the Hex system of the second parameter carried by option82 vendor-specific (suboption9).
hostname	Option82 vendor-specific（suboption9）Stands for the parameter of the suboption is the host name
vlanip	Option82 vendor-specific（suboption9）Stands for the parameter of the suboption is IP of interface vlan

Default Value

None

Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping.

This command without parameters acts as a switch command. When append is enabled, the information of this command will be added to suboption9 of option82. The added information is first-subop9-param and second-subop9-param.

Example

The following example shows how to enrich dhcp packets with option82 on interface g0/3 and set suboption 9 added parameter 1 with the hexadecimal 61-62-63-61-62-63.

```
Switch_config_g0/3# dhcp snooping information append
Switch_config_g0/3#dhcp snooping information append first-subop9-param hex 61-62-63-61-62-63
Here 61-62-63-61-62-63 is the Hex system of the to-be-added parameter.
```

32.1.21 dhcp snooping information drop

Syntax

dhcp snooping information drop

no dhcp snooping information drop

Parameters

None

Default Value

None

Usage Guidelines

This command can be set on each port that connects the client.

After this command is set, the request packets that contain option82 will be dropped on the stipulated port.

Example

The following example shows how to drop dhcp packets with option82 on g0/3.

```
Switch_config_g0/3# dhcp snooping information drop
```

32.1.22 ip-source trust

Syntax

ip-source trust

no ip-source trust

Parameters

None

Default Value

The default interface is a distrusted one.

Usage Guidelines

Source IP address snooping is not conducted to the source-IP-trusted interface. The "no" form of this command is used to resume the default value of this interface.

Example

The following example shows how to set interface GigaEthernet0/1 to a source-ip-trusted interface.

```
Switch_config_g0/1#ip-source trust
```

32.1.23 show ip dhcp-relay snooping

Syntax

show ip dhcp-relay snooping

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the information about DHCP-snooping configuration.

Example

The following example shows how to display the information about DHCP-relay snooping.

```
Switch_config#show ip dhcp-relay snooping
```

32.1.24 show ip dhcp-relay snooping binding

Syntax

show ip dhcp-relay snooping binding [all]

Parameters

None

Default Value

None

Usage Guidelines

This command is used to display the binding information about DHCP-relay snooping.

If the all parameter is in the command sentence, all binding information about DHCP-relay snooping will be displayed.

Example

The following example shows how to display the information about DHCP-relay snooping binding.

```
Switch_config#show ip dhcp-relay snooping binding
```

32.1.25 debug ip dhcp-relay snooping

Syntax

debug ip dhcp-relay snooping

no debug ip dhcp-relay snooping

Parameters

None

Default Value

None

Usage Guidelines

This command is used to enable or disable the debugging switch of DHCP-relay snooping.

Example

The following example shows how to enable the debugging switch of DHCP-relay snooping.

```
Switch#debug ip dhcp-relay snooping
Switch#
```

32.1.26 debug ip dhcp-relay event

Syntax

debug ip dhcp-relay event

no debug ip dhcp-relay event

Parameters

None

Default Value

None

Usage Guidelines

This command is used to enable or disable the event debugging switch of DHCP-relay.

Example

The following example shows how to enable the debugging switch of DHCP-relay event.

```
Switch#debug ip dhcp-relay event
Switch#
```

32.1.27 debug ip dhcp-relay binding

Syntax

debug ip dhcp-relay binding

no debug ip dhcp-relay binding

Parameters

None

Default Value

None

Usage Guidelines

This command is used to enable or disable the debugging switch of DHCP-relay snooping binding.

Example

The following example shows how to enable the debugging switch of DHCP-relay snooping binding.

```
Switch#debug ip dhcp-relay binding
Switch#
```

Chapter 1 MACFF Configuration Commands

MACFF configuration commands include:

macff enable

macff vlan vlan_id enable

macff vlan vlan_id default-ar A.B.C.D

macff vlan vlan_id other_ar A.B.C.D

debug macff

macff enable

Syntax

To enable or disable the MACFF function globally, run the following command. To return to the default setting, use the no form of this command.

macff enable

no macff enable

Parameters

None

Default Value

MACFF function is disabled by default.

Usage Guidelines

None

Example

The following example shows how to enable the MACFF function.

```
Switch_config#macff enable

Switch_config#
```

macff vlan vlan_id enable

Syntax

macff vlan vlan_id enable

no macff vlan vlan_id enable

Parameters

Parameters	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094

Default Value

Chapter 33 MACFF Configuration Commands

MACFF configuration commands include:

- macff enable
- macff vlan *vlan_id* enable
- macff vlan *vlan_id* default-ar *A.B.C.D*
- macff vlan *vlan_id* other_ar *A.B.C.D*
- debug macff

33.1 macff enable

Syntax

To enable or disable the MACFF function globally, run the following command. To return to the default setting, use the no form of this command.

macff enable

no macff enable

Parameters

None

Default Value

MACFF function is disabled by default.

Usage Guidelines

None

Example

The following example shows how to enable the MACFF function.

```
Switch_config#macff enable
Switch_config#
```

33. 1 macff vlan vlan_id enable

Syntax

macff vlan *vlan_id* **enable**

no macff vlan *vlan_id* **enable**

Parameters

Parameters	Description
vlan id	Stands for the ID of a VLAN. Value range: 1-4094

Default Value

None

Usage Guidelines

The command is used to send MAC-Based VLAN.

Example

The following example shows how to enable MACFF on VLAN 2 and the default gateway address is 192.168.1.1.

```
Switch_config#arp 192.168.1.1 00:e0:0f:17:92:ed vlan 2
Switch_config#macff vlan 2 enable
Switch_config#
```

33.3 macff vlan *vlan_id* default-ar *A.B.C.D*

Syntax

To bind DHCP snooping to standby TFTP server, run ip dhcp-relay snooping database-agent A.B.C.D.

macff vlan *vlan_id* **default-ar** *A.B.C.D*

no macff vlan *vlan_id* **default-ar** *A.B.C.D*

Parameters

Parameters	Description
A.B.C.D	IP address of the default gateway

Default Value

None

Usage Guidelines

This command is used when you set the IP address of the client host and the default gateway manually. Of course, you also need to add the DHCP snooping binding table manually.

Example

The following example shows how to set the address of MACFF binding gateway in vlan1 to 192.168.1.1 and the client's address to 192.168.1.10.

```
Switch_config#arp 192.168.1.1 00:e0:0f:17:92:ed vlan 1
Switch_config#ip source binding 6c:62:6d:59:18:b6 192.168.1.10 interface GigaEthernet0/1
Switch_config# macff vlan 1 default-ar 192.168.1.1
Switch_config#
```

33.4 macff vlan *vlan_id* other_ar *A.B.C.D*

Syntax

macff vlan *vlan_id* **other_ar** *A.B.C.D*

no macff vlan *vlan_id* **other_ar** *A.B.C.D*

Parameters

Parameters	Description
A.B.C.D	Stands for the IP address of service AR.

Default Value

None

Usage Guidelines

When the network segment where the client host is has other service ARs and these ARs are only accessed by the client directly without the need of gateway to forwarding packets, this command can be used to add these service ARs.

Example

The following example shows how to set an AR with its IP being 192.168.2.254 and its MAC being 00:e0:0f:23:02:fc on port g0/1 in vlan1.

```
Switch_config#arp 192.168.2.254 00:e0:0f:23:02:fc vlan 1
Switch_config#interface g0/1
Switch_config_g0/1# dhcp snooping trust
Switch_config_g0/1#exit
Switch_config#macff vlan 1 other_ar 90.1.1.1
```

33.5 macff disable

Syntax

macff disable

no macff disable

Parameters

None

Default Value

A specified port is allowed to enable MACFF.

Usage Guidelines

Though MACFF is enabled in a VLAN, MACFF can be disabled on one of the ports in this VLAN. The DHCPR snooping functionality is not affected on this port after disabled its MACFF functionality.

Example

The following example shows how to disable MACFF on port g0/1.

```
Switch_config_g0/1#macff disable
Switch_config_g0/1#
```

33.6 debug macff

Syntax

debug macff

no debug macff

Parameters

None

Default Value

None

Usage Guidelines

This command is used to enable or disable the MACFF debugging switch.

Example

The following example shows how to enable the debugging switch of MACFF.

```
Switch_config#debug macff
Switch_config#
```

Chapter 34 IEEE1588 Transparent Clock Configuration Commands

34.1 IEEE1588 transparent clock configuration command

The IEEE1588 transparent clock configuration commands are:

- ptp enable (Global)
- ptp enable (port)
- ptp start
- ptp sync-mechanism
- ptp domain
- ptp domain-filter
- ptp e2e-record-timeout
- debug ptp
- show ptpt

34.1.1 ptp enable (Global)

Command description

ptp enable

no ptp enable

Parameters

None

Default Value

None

Instructions

This command is used to enable or disable the IEEE1588 transparent clock function. The transparent clock is abbreviated as TC, and it is divided into two modes: E2E transparent clock and P2P transparent clock according to the different methods of link delay measurement. The transparent clock achieves accurate synchronization between the master and slave clocks by modifying the dwell time introduced by the synchronization message through the intermediate device.

Command mode

Global configuration mode

Example

The following command will enable the IEEE1588 transparent clock function.

```
Switch_config# ptp enable Switch_config#
```

34.1.2 ptp enable (port)

Command description

ptp enable

no ptp enable

Parameters

None

Default Value

None

Instructions

This command is used to enable or disable the ptp function on the Layer 3 port.

Command mode

Port configuration mode

Example

The following command will enable the IEEE1588 transparent clock function on interface vlan 1 port.

Switch_config# interface vlan 1 Switch_config_v1#ptp enable Switch_config_v1#

34.1.3 ptp start

Command description

ptp start {l2|l3}

no ptp start

Parameters

Parameters	Parameters Description
L2	Create a Layer 2 PTP port for Ethernet
L3	Create a Layer 3 PTP port that works on IP / UDP

Default Value

None

Instructions

Before performing PTP communication, you must first create a number of PTP ports on the transparent clock to connect them to the master and slave clocks, respectively. We can use the "ptp start" command in port mode to create and delete PTP ports. All ports on the switch support PTP.

After the “no ptp enable” command is configured globally, all the created PTP ports will be deleted automatically.

Use the "ptp start l2" command to create a Layer 2 PTP port. This port will accept and send Ethernet-based PTP packets. Use the "ptp start l3" command to create a Layer 3 PTP port. This port will accept and send IP / UDP-based PTP packets. The "ptp start l2" command and the "ptp start l3" command can be switched directly without additional delete operations.

Use the "no ptp start" command to delete the PTP port without additional Parameters.

Command mode

Port configuration mode

Example

The following command will create a Layer 2 PTP port on G0 / 24.

```
Switch_config_g0/24# ptp start l2
Switch_config_g0/24#
```

Use the following command to change the Layer 2 PTP port on G0 / 24 to a Layer 3 PTP port.

```
Switch_config_g0/24# ptp start l3
Switch_config_g0/24#
```

Use the following command to delete the PTP port on G0 / 24.

```
Switch_config_g0/24# no ptp start
Switch_config_g0/24#
```

34.1.4 ptp sync-mechanism

Command description

ptp sync-mechanism { straight-forward | store-forward}

Parameters

Parameters	Parameters Description
straight-forward	Set the processing mode of Sync / Follow Up messages to direct forwarding
store-forward	Set the processing mode of Sync / Follow Up messages to store and forward

Default Value

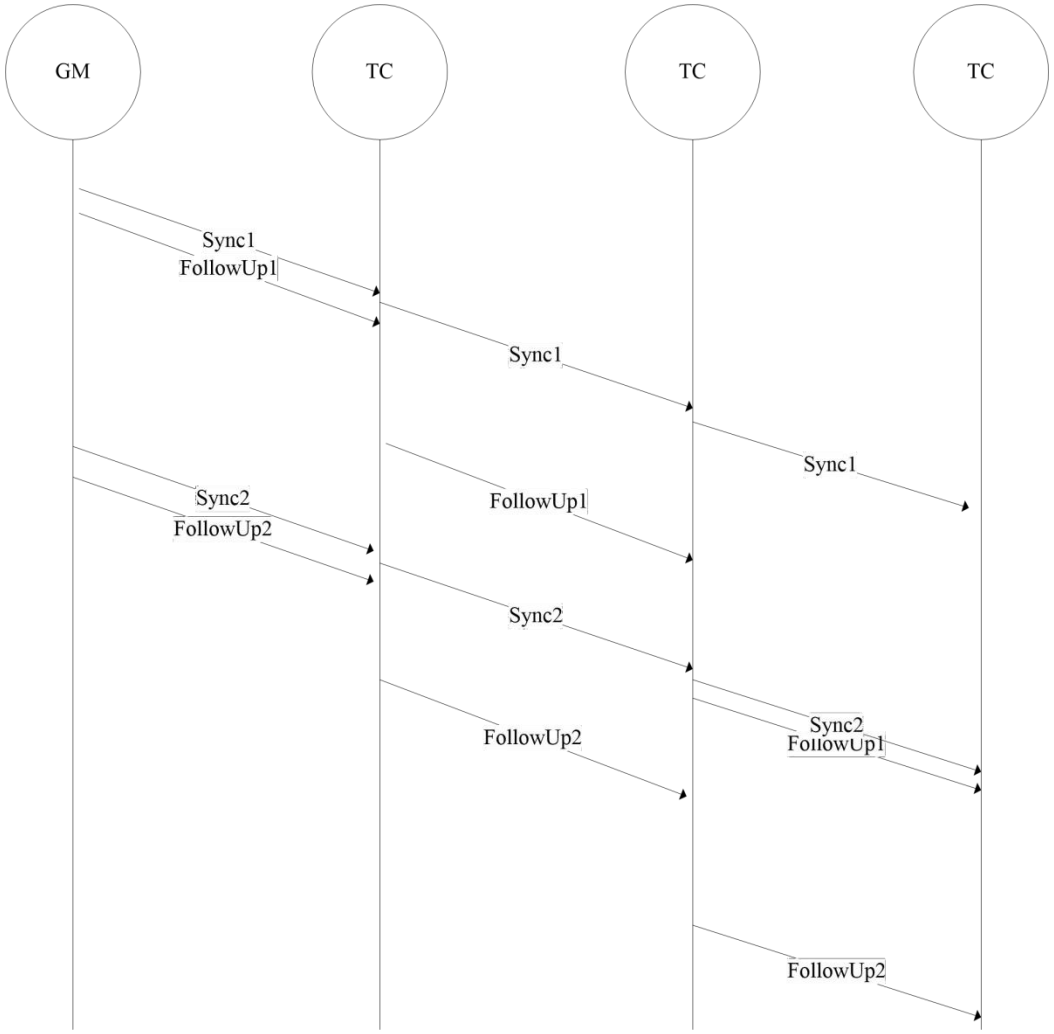
straight-forward

Instructions

This command is mainly used to set the forwarding mode of Sync / Follow_Up packets. You can switch between direct forwarding and store-and-forward. The default is the direct forwarding mode, that is, the PTP port forwards the Sync packet immediately after receiving it.

After receiving the corresponding Follow_Up packet, it repackages the Follow_Up packet and forwards it from the corresponding PTP port.

This mode may cause out-of-order problems in the case of multi-level transparent clock cascading, as shown in the following figure:



In the direct forwarding mode, the processing time of the Sync message is significantly shorter than the Follow_Up message. After multi-level TC concatenation, Sync2 has been received before the Follow_up1 is received from the clock. This situation may cause the slave clock to malfunction.

For this reason, we specially designed the store-and-forward mode, that is, the PTP port does not forward immediately after receiving the Sync message, but after receiving the corresponding Follow_Up message, the two are processed together to avoid the problem of disorder.

Command mode

Global configuration mode

Example

The following command sets the transparent clock to direct forwarding mode.

```
Switch_config#ptp sync-mechanism straight-forward
Switch_config#
```

The following command sets the transparent clock to direct forwarding mode.

```
Switch_config#ptp sync-mechanism store-forward
Switch_config#
```

34.1.5 ptp domain

Command description

```
ptp domain number

no ptp domain
```

Parameters

Parameters	Parameters Description
number	PTP domain number, range 0 ~ 3

Default Value

0

Instructions

Configure the domain to which the PTP port belongs. The default is domain 0. The IEEE1588 protocol defines four domains, which are domain 0, domain 1, domain 2, and domain 3.

Command mode

Interface configuration mode

Example

The following command will configure the PTP port to work on domain 1 on G0 / 24.

```
Switch_config_g0/24# ptp domain 1 Switch_config_g0/24#
```

34.1.6 ptp domain-filter

Command description

```
ptp domain-filter
```

no ptp domain-filter

Parameters

None

Default Value

Open

Instructions

Set the domain filtering function, which is enabled by default. We can manage the "sharding" of PTP devices by dividing the domains. PTP devices in different subdomains cannot perform time synchronization. After the domain filtering function is enabled, PTP packets in other domains will be discarded; if the domain filtering function is disabled, the transparent clock will not perform domain checking.

Command mode

Global configuration mode

Example

The following command will enable domain filtering.

```
Switch_config#ptp domain-filter
Switch_config#
```

The following command will turn off domain filtering.

```
Switch_config#no ptp domain-filter
Switch_config#
```

34.1.7 ptp e2e-record-timeout

Command description

ptp e2e-record-timeout time

no ptp e2e-record-timeout

Parameters

Parameters	Parameters Description
time	Delay_Req packet record timeout time, range 0 ~ 10

Default Value

5 (32s)

Instructions

Configure the timeout period of the Delay_Req record to prevent the Delay_Req record from being released when the Delay_Resp message is lost.

Command mode

Global configuration mode

Example

The following command will configure the timeout of the Delay_Req record to 1024s.

```
Switch_config#  ptp e2e-record-timeout 10
Switch_config#
```

34.1.8 debug p2p

Command description

```
debug ptp {errors|rx-packet|tx-packet |sync|e2e|p2p}
```

Parameters

Parameters	Parameters Description
errors	View PTP error log
rx-packet	View the received PTP packets
tx-packet	View the sent PTP packets
sync	View the status of the transparent clock processing Sync packets
e2e	Viewing the Transparent Clock Processing of Delay_Req Packets
p2p	View the path_delay calculation of the PTP port

Default Value

None

Instructions

The debugging information output during the transparent clock operation is mainly used to understand the PTP operation and error location.

34.1.9 show ptp

Command description

```
show ptp [interface intf-id]
```

This command is used to display PTP configuration information.

Parameters

Parameters	Parameters Description
intf-id	Specific physical port.

Default Value

None

Instructions

Display the configuration information on the IEEE1588 transparent clock.

Command mode

Management configuration mode

Example

```
Switch#show ptp
IEEE1588 Transparent Clock Default Data Set
clock identity      .. 00-E0-0F-FF-FE-DB-0B-54
number of ports  300
delay mechianism        E2E
primary domain  0
Pdelay_Req interval     0
Domain Control
domain filter       ON
```

Chapter 35 L2 Channel Configuration Commands

35.1 L2 Channel Configuration Commands

The following is a L2 tunnel monitoring command:

- l2protocol-tunnel
- no spanning-tree

35.1.1 L2 protocol-tunnel

Syntax

To configure the layer-2 (L2) protocol tunnel, run the following command.

```
[no] l2protocol-tunnel [stp]
```

Parameters

None

Default Value

By default, the tunnel function of any L2 protocol is not enabled on the port of the switch.

When the tunnel function is enabled, the tunnel function of all supported L2 protocols is enabled if no specific L2 protocol is designated.

Usage Guidelines

Currently only STP supports the tunnel function in our switches.

Example

The following example shows how to enable the tunnel function of the STP (including STP/PVST) on interface g0/2.

```
Switch_config# interface g0/2
Switch_config_g0/2# l2protocol-tunnel stp
```

35.1.2 no spanning-tree

Syntax

To disable the STP of a port, run the following command.

```
no spanning-tree
```

Parameters

None

Default Value

STP can be enabled on all switch's ports by default.

Usage Guidelines

This command is used to disable STP on the port of a tunnel entrance, preventing this port from influencing the devices that access the tunnel by sending the STP packets.

Example

The following example shows how to disable STP on port g0/2:

```
Switch_config# interface g0/2
Switch_config_g0/2# no spanning-tree
```

Chapter 36 Loopback Detection Configuration Commands

Loopback Detection Configuration Commands include:

- loopback-detection
- loopback-detection enable
- loopback-detection vlan-control
- loopback-detection hello-time
- loopback-detection recovery-time
- loopback-detection control
- loopback-detection dest-mac
- loopback-detection existence
- loopback-detection frames-threshold
- loopback-detection frames-monitor
- show loopback-detection
- show loopback-detection interface

36.1 Loopback-detection

Syntax

To enable global loopback detection, run the following command. To return to the default setting, use the no form of this command.

[no] loopback-detection

Parameters

None

Default Value

Loopback detection is globally disabled by default.

Command Mode

Global configuration mode

Usage Guidelines

None

Example

```
Switch#config
Switch_config#
Switch_config#loopback-detection
```

36.2 Loopback-detection Enable

Syntax

To enable or disable loopback detection on a port, run the following command.

[no] loopback-detection enable

Parameters

None

Default Value

Loopback detection is disabled on a port by default.

Command Mode

Port configuration mode

Usage Guidelines

This command can be used to enable or disable loopback detection on a specified port. However, this setting takes effect only after loopback detection is enabled globally.

Example

```
Switch_config#
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection enable
```

36.3 Loopback-detection vlan-control

Syntax

To set a port to perform loopback detection toward a specified VLAN, run the following command.

[no] loopback-detection vlan-control vlan-list

Parameters

Parameters	Description
vlan-list	Stands for a VLAN specified by a port. It ranges from 1 to 4094, and up to 10 VLANs can be specified.

Default Value

None

Command Mode

Port configuration mode

Usage Guidelines

After loopback detection is configured on a specified VLAN, the port transmits multiple detection packets of specified VLAN tag regularly and the number of these detection packets transmitted by this port can be up to 10.

Example

```
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection vlan-control 1-5
```

36.4 Loopback-detection Hello-time

Syntax

To set the transmission period of loopback detection packets, run the following command.

[no] loopback-detection hello-time hello-time

Parameters

Parameters	Description
hello-time	Stands for the transmission period of loopback packets, whose unit is second.

Default Value

3 seconds

Command Mode

Port configuration mode

Usage Guidelines

None

Example

None

36.5 Loopback-detection Recovery-time

Syntax

To set the recovery time of a port after being controlled, run the following command.

[no] loopback-detection recovery-time recovery-time

Parameters

Parameters	Description
recovery-time	Stands for the recovery time of a port after being controlled, whose unit is second.

Default Value

10 seconds

Command Mode

Port configuration mode

Usage Guidelines

None

Example

None

36.6 Loopback-detection Control

Syntax

To set a port to be controlled, run the following command.

[no] loopback-detection control { block|learning|shutdown}

Parameters

Parameters	Description
block	Sets a port to be blocked.
learning	Sets a port to be learning.
shutdown	Sets a port to be shutdown.

Default Value

None

Command Mode

Port configuration mode

Usage Guidelines

When a port detects loopback exists in its network, you can perform corresponding control actions to this port by setting control functions. The controlled states of a port include block, nolearn, shutdown and trap. When a controlled state is configured and loopback exists on a port, the trap message be transmitted. It is not configured by default.

After loopback detection is enabled globally, the port on which loopback detection is enabled transmits the loopback detection packets and receives the already transmitted loopback detection packets. Four control actions are conducted on the port:

block : This means to block the port. When loopback is found, this port will be isolated from other ports and the packets going into this port cannot be forwarded to other ports. This port is then in protocol down state and its MAC address table ages.

nolearn: This means forbidding this port to learn MAC addresses. Upon the discovery of loopback on a port, this port will not learn MAC addresses and at the same time age its MAC address table.

Shutdown: Disable the port. When detecting the loopback, the port forwards trap warning information, ages the MAC address table and automatically disables the port (error-disable). Thus, the port cannot forward the packet until the error-disable-recover time.

trap: It means that the port only reports alarms. When loopback is discovered, the port will only report alarms and age its MAC address table.

When a port is blocked, the packets entering into this port cannot be forwarded by this port and this port will go on transmitting loopback detection packets at the same time; when loopback disappears, the port will recover itself automatically. Loopback disappearance takes place if the port has not received loopback detection packets within 10 seconds. In block state

the port protocol is down, while in shutdown state the port's link is down directly.

Example

```
Switch#config
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection control block
```

36.7 Loopback-detection dest-mac

Syntax

To set the destination MAC address of loopback detection packets on a port, run the following command.

[no] loopback-detection dest-mac mac-addr

Parameters

Parameters	Description
mac-addr	Stands for the MAC address that corresponds to a MAC VLAN entry.

Default Value

The default destination MAC address is 01-80-C2-00-00-0a.

Command Mode

Port configuration mode

Usage Guidelines

None

Example

```
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection dest-mac 1111.1111.1111
```

36.8 Loopback-detection Existence

Syntax

To set a standard to judge whether loopback exists on a port when this port is enabled or its link state is UP, run the following command.

[no] loopback-detection existence

Parameters

None

Default Value

Loopback is nonexistent by default.

Command Mode

Port configuration mode

Usage Guidelines

This command is mainly used to solve the problem that loopback exists on a port or not when this port is up and its loopback detection function takes effect. When the controlled action of this port is set to shut down, it is improper to regard that loopback exists on this port for a shutdown port has already not forwarded packets. There is no loopback by default.

Example

None

36.9 Loopback-detection frames-threshold

Syntax

To configure the upper threshold the loop detection frame received every minute, run the following command.

[no] loopback-detection frames-threshold frames-threshold

Parameters

Parameters	Description
frames-threshold	The upper threshold the loop detection frame received every minute (100-200)

Default Value

The default upper threshold is 10.

Command Mode

Port configuration mode

Usage Guidelines

None

Example

```
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection frames-threshold 20
```

36.10 Loopback-detection frames-monitor

Syntax

To configure enable or disable frame number detection function, run the following commands.

[no] loopback-detection frames-monitor

Parameters

None

Default Value

Disabled.

Command Mode

Port configuration mode

Usage Guidelines

None

Example

```
Switch#config
Switch_config#interface g0/1
Switch_config_g0/1#loopback-detection frames-monitor
```

36.11 Show Loopback-detection

Syntax

To display the configuration details of loopback detection, run the following command.

show loopback-detection

Parameters

None

Default Value

None

Command Mode

EXEC mode, Global configuration mode or interface mode

Usage Guidelines

This command is used to display the global or port's loopback detection configurations and port status.

Example

```
Switch#show loopback-detection
Loopback-detection is enable

Interface state information
Port          Status    dest MacAddress Control    VLAN
------------  --------- ---------------------- ----------   -------------------------------
      G0/1        UP    1234.5678.9abc BLOCK      1-5
      G0/2        UP    0180.c200.000a WARNING
      G0/3        UP    0180.c200.000a BLOCK
      G0/4        UP    0180.c200.000a WARNING
      G0/5        UP    0180.c200.000a WARNING
      G0/6        UP    0180.c200.000a WARNING 1-8
      G0/7        UP    0180.c200.000a WARNING
      G0/8        UP    0180.c200.000a WARNING
      G0/9        UP    0180.c200.000a WARNING
     G0/10        UP    0180.c200.000a WARNING
     G0/11        UP    0180.c200.000a WARNING
     G0/12        UP    0180.c200.000a WARNING
     G0/13        UP    0180.c200.000a WARNING
     G0/14        UP    0180.c200.000a WARNING
     G0/15        UP    0180.c200.000a WARNING
     G0/16        UP    0180.c200.000a WARNING
```

36.12 Show Loopback-detection

Syntax

To display the information about the loopback detection port, run the following command.

show loopback-detection intf-id

Parameters

Parameters	Description
Interface Intf-id	Displays the designated port.

Default Value

None

Command Mode

EXEC mode, Global configuration mode or interface mode

Usage Guidelines

This command is mainly used to display the status of the loopback detection port.

Example

```
Switch#show loopback-detection interface g0/1
Receive Packets :0
Transmit Packets: 20
Discard Packets:0
HelloTimeOut:10
RecoverTimeOut:26
```

Chapter 37 QoS Configuration Commands

37.1 QoS Configuration Commands

QoS configuration commands include:

- cos default
- cos map
- dscp map
- scheduler weight bandwidth
- scheduler policy
- policy-map
- classify
- action
- qos policy
- show policy-map
- trust

37.1.1 cos default

Syntax

To configure the default COS value, run cos default cos.

cos default cos

no cos default

Parameters

Parameters	Description
cos	The COS value ranges between 0 and 7.

Default Value

The default COS value is 0.

Usage Guidelines

This command is run in layer-2 interface configuration mode or in global configuration mode.

If this command is run in global configuration mode, default CoS in all ports are affected. If this command is run on a layer-2 interface, the CoS on this interface will be affected.

Example

The following example shows how to set the CoS value of the untagged frame received by interface g0/1 to 4.

```
Switch_config#inter g0/1
Switch_config_g0/1#cos default 4
```

37.1.2 cos map

Syntax

To set the CoS priority queues, use the cos map command.

cos map quid cos1..cosn

no cos map

Parameters

Parameters	Description
quid	Stands for the ID of the CoS priority queue, 1 to 8.
cos1..cosn	CoS value defined by IEEE802.1p, ranging between 0 and 7

Default Value

CoS Value	S Priority Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Usage Guidelines

This command is run in layer-2 interface configuration mode or in global configuration mode.

If this command is run in global configuration mode, CoS priority queues in all ports are affected. If this command is run on a layer-2 interface, the CoS priority queues on this interface will be affected.

Example

The following example shows how to map CoS 0-2 to CoS priority queue 1 and CoS 3 to CoS priority queue 2.

```
Switch_config # cos map 1 0 1 2
Switch_config # cos map 2 3
```

37.1.3 dscp map

Syntax

To set the CoS priority queues according to dscp, use the cos map command.

dscp map word {cos cos-value}

no dscp map

Parameters

Parameters	Description
word	Dscp range table, for instance, (1,3,5,7) , (1, 3-5,7), (1-7).
cos cos-value	The priority cos of Dscp mapping, 0-7.

Default Value

None

Usage Guidelines

This command is run in global configuration mode.

Example

The following example shows how to map dscp 0-2 to Cos priority queue.

```
Switch_config#dscp map 0-2 cos 1
```

37.1.4 scheduler weight bandwidth

Syntax

To set the bandwidth of the CoS priority queue, run the following command.

scheduler weight bandwidth weight1...weightn

no scheduler weight bandwidth

Parameters

Parameters	Description
weight1…weight8	Values of eight CoS priority queues WRR/WFQ, ranging between 0 and 127.

Default Value

The weight value of each CoS priority queue is same. All weight values of eight CoS priority queues are 1.

Usage Guidelines

This command is run in layer-2 interface configuration mode or in global configuration mode.

If this command is run, the bandwidth of all priority queues on all interfaces are affected. Before the command is run, only the bandwidth of the priority queue will be affected. This command validates only when the queue schedule mode is set to WRR/WFQ. This command decides the bandwidth weight value of the CoS priority queue when the WRR/WFQ schedule policy is used.

The weight of the queue after the third queue can be configured to 0. Once the weight of a queue is configured to 0, the queue after that is compelled to 0, then the hybrid mode will be applied.

Example

The following example shows how to set the weight values of eight CoS priority queues to 1, 2, 3, 4, 5, 6, 7 and 8 respectively.

```
Switch_config # scheduler weight bandwidth 1 2 3 4 5 6 7 8
```

37.1.5 scheduler policy

Syntax

To set CoS priority queue debug policy, use the scheduler policy command.

scheduler policy { sp | wrr | wfq | fcfs }

no scheduler policy

Parameters

Parameters	Description
sp	Uses the SP schedule policy.
wrr	Uses the WRR schedule policy.
wfq	Uses the WFQ schedule policy.
fcfs	Uses the FCFS schedule policy.

Default Value

The SP schedule policy is used by default.

Usage Guidelines

This command can be used in layer-2 interface configuration mode or in global configuration mode.

If this command is run, the port queue schedule policy on all interfaces are affected. Before the command is run, only the belonging port queue schedule policy will be affected. No fcfs command for the interface.

After this command is configured, the schedule mode of the interface is set to the designated value.

Example

The following example shows how to send transmission schedule mode to WRR.

```
Switch_config # scheduler policy wrr
```

37.1.6 policy-map

Syntax

To set the QoS policy map, run policy-map name.

policy-map name

no policy-map name

Parameters

Parameters	Description
name	Name of the QoS policy map, consisting of 1 to 20 characters.

Default Value

None

Usage Guidelines

Global Configuration mode

After the command is entered, the system enters the QoS policy mapping configuration mode. In this mode, the following commands are used:

- classify: Used to set the QoS flow.
- description: Used to describe the QoS policy map.
- exit: Used to exit from the QoS policy mapping configuration mode.
- no: Used to cancel the previously-entered command.

- action: Used to define the QoS action.

Example

The following example shows how to set the QoS policy map.

```
Switch_config # policy-map myqos
```

37.1.7 classify

Syntax

To configure the matchup data flow of the QoS policy map, run the following command. To return to the default setting, use the no form of this command.

classify {**any** | **cos** *cos* | **icos** *icos* | **vlan** *vlanid* | **ivlan** *ivlanid* | **ethernet-type** *ethernet-type* | **precedence** *precedence-value* | **dscp** *dscp-value* | **tos** *tos-value* | **diffserv** *diffserv-value* | **ip** *ip-access-list* | **ipv6** *ipv6-access-list* | **mac** *mac-access-list* }

no classify { **cos** | **icos** | **vlan** | **ivlan** | **ethernet-type** | **precedence** | **dscp** | **tos** | **diffserv** | **ip** | **ipv6** | **mac** }

Parameters	Description
any	Matches up with any packet.
cos cos	Configures the matching COS value; the valid range is 0 to 7
icos icos	Configures the matching interior tag COS value; the valid range is 0 to 7.
vlan vlanid	Configures the matching VLAN; the valid range is 1 to 4094
ivlan ivlanid	Configures interior tag vlan id. 1-4094.
ethernet-type ethernet-type	Configures the packet type, 0x0600-0xFFFF
precedence precedence-value	The priority field in tos of ip packet (5-7 of tos), 0-7.
dscp dscp-value	Dscp field in tos of ip packet (2-7 of tos), 0~63.
tos tos-value	tos in the ip packet represents delay, throughput, reliability and cost field (1-4 of tos), 0~15.
diffserv diffserv-value	All tos field in Ip packet: 8, 0-255.
ip ip-access-list	Configures the name of the matched IP access list.. The name has 1 to -20 characters.
ipv6 ipv6-access-list	Configures the name of the matched IPV6 access list. The name has 1 to 20 characters.
mac mac-access-list	Configures the name of the matched MAC access list. The name has 1 to 20 characters.

Default Value

Any packet is matched by default.

Usage Guidelines

QoS policy map configuration mode

All data flows in a QoS policy map must have the same mask value. The port number in the IP access list must be a definite value, not a value range.

The IP access list and the MAC access list which are used to match up with the data flows can be configured no more than 16 regulations, or the configuration will fail. When the action in the regulation is permit, the regulation is used to differentiate the data flows; when the action in the regulation is deny, the regulation has no function.

When the QinQ mode is enabled, that is, when the dot1q-tunnel command is configured, the ivlan and icos commands need be configured when the vlan or the cos value of the source packet is matched.

Example

```
Switch-policy-map#classify vlan 4
```

37.1.8 action

Syntax

To configure the data flow policy of a QoS policy map, run the following commands.

action{**bandwidth** *max-band* | **cos** *cos* **| drop | dscp** *dscp-value* **| precedence** *precedence-value* **| forward | icos** *icos* **| ivlanID** { **add** *addivlanid* | *ivlanid*}**| monitor** *session-value* **| quequ** *quequ-value* **| redirect** *interface-id* **| stat-packet | stat-byte | vlanID** { **add** *addvlanid* | *vlanid*} **| copy-to-CPU**}

no action {**bandwidth | cos | drop | dscp | precedence | forward | | icos | ivlanID | monitor | quequ | redirect | stat-packet | stat-byte | vlanID | copy-to-CPU**}

Parameters

Parameters	Description
bandwidth max-band	Maximum bandwidth to a class, the range is 1 to 163840. Unit: 64Kbps.
cos cos	Sets the matched COS field to cos-value 0-7.
drop	Drops the matched packets.
dscp dscp-value	Sets the matched DSCP field to dscp-value 0~63.
precedence precedence-value	The priority field in tos of ip packet (5~7 of tos). 0-7.
forward	Conducts no operations to the matched packets.
icos icos	Sets the matched COS field to cos-value 0-7.
ivlan {add ivlanid | ivlanid}	Sets replacing or adding interior vlanid; the range is 1-4094.
monitor session-value	Sends the packets to monitor interface; the range is 1-4.
quequ quequ-value	Sets the queue mapping value 1-8.
redirect interface-id	Redirects the egress port of the matched flow.
stat-packet	Calculates the number of packets.
stat-byte	Calculates the number of bytes.
vlanID { add vlanid | vlanid }	Sets replacing or adding exterior vlanid; the range is 1-4094.
copy-to-CPU	Sets forwarding the packet to CPU.

Default Value

None

Usage Guidelines

QoS policy map configuration mode

After enabling dot1q function, vlan and cos on the downlink port takes effect only when ivlan and icos are configured.

When Monitor is applied to the egress, an independent policymap must be configured. Otherwise, the result may turn to abnormal.

In igress direction, the action of vlan and ivlan conflicts with dscp, precedence, bandwidth, cir, mirror, stat or redirect. They cannot be configured simultaneously.

In igress direction, the action of cos and ivlan conflicts with dscp, precedence, bandwidth, cir, mirror, stat or redirect. They cannot be configured simultaneously.

In egress direction, the action of cos and ivlan conflicts with dscp, precedence, bandwidth, cir, mirror, stat or redirect. They cannot be configured simultaneously.

Example

```
Switch-policy-menabap#action redirect g0/1
```

37.1.9 qos policy

Syntax

To configure the QoS policy of a port, run the following command.

[**no**] **qos policy** *name* {**igress**}

Parameters

Parameters	Description
name	Stands for the name of QoS policy mapping.
ingress	Functions on the ingress port.

Default Value

None

Usage Guidelines

This command can be used in layer-2 interface configuration mode or in global configuration mode.

The flow of most actions in the igress direction can be correctly matched up when they are known unicasts.

Example

The following example shows how to configure the pmap QoS policy on interface g0/1.

```
Switch_config#inter g0/1
Switch_config_g0/1# qos policy pmap ingress
```

37.1.10 show policy-map

Syntax

To display all or some designated QoS policy maps, run the following command.

show policy-map {*policy-map-name* | **interface** [*interface-id*] | **global** }

Parameters

Parameters	Description
policy-map-name	Stands for the name of a QoS policy map.
interface [interface-id]	Stands for the policy of interface application
global	Stands for the policy of global configuration

Default Value

None

Usage Guidelines

None

Example

The following example shows how to display all QoS policy maps.

```
Switch_config#show policy-map
policy-map          1
    classify any
    action redirect g0/1
policy-map          11
    classify any
    action
Switch_config#
```

37.1.11 trust

Syntax

To show how to set the trust mode, run the following command.

[**no**]**qos trust** { *cos* | *dscp* | *untrust* }

Parameters

Parameters	Description
cos	Stands for the trust mode.
dscp	The trust mode.
untrust	The untrust mode.

Default Value

None

Usage Guidelines

The command is applicable in the global configuration mode.

Example

The following example shows how to set the trust mode cos.

```
Switch_config#qos trust cos
```

Chapter 38 DoS-Attack Prevention Configuration Commands

38.1 DoS-Attack Prevention Configuration Commands

DoS-Attack Prevention Configuration Commands include:

- dos enable
- show dos

38.1.1 dos enable

Syntax

dos enable {all | icmp *icmp-value* **| ip | l4port | mac | tcpflags | tcpfrag** *tcpfrag-value* **| tcpsmurf | icmpsmurf | ipsmurf }**

no dos enable { **all | icmp** *icmp-value* **| ip | l4port | mac | tcpflags | tcpfrag** *tcpfrag-value* **| tcpsmurf | icmpsmurf | ipsmurf** }

Parameters

Parameters	Description
all	Enables to prevent all kinds of DoS attacks.
icmp icmp-value	Enables detection ICMP packeticmp-valueis the maximum length of the ICMP packet. The ICMP packet and ICMPv6 packet whose length is larger thanicmp-valuewill be dropped.
ip	Prevents those DoS attack packets whose source IP addresses are equal to the destination IP addresses.
l4port	Starts to check the L4 packets whose source port is equal to the destination port.
mac	Prevents those packets whose source MACs equal to destination MACs.
tcpflags	Starts to check the TCP packets with illegal flags.
tcpfrag tcpfrag-value	Starts to check the DoS attack packet of TCP fragment. Here, the tcpfrag-value parameter means the minimum TCP header, whose default value is 20.
tcpsmurf	Prevents those TCP packets whose destination addresses equal to broadcast addresses.
icmpsmurf	Prevents those ICMP packets whose destination addresses equal to broadcast addresses.
ipsmurf	Prevents those ICMP packets whose destination addresses equal to broadcast addresses.

Default Value

DoS attack prevention is disabled by default.

Usage Guidelines

DoS attack prevention is configured in global mode.

The DoS IP sub-function can drop those IP packets whose source IPs are equal to the destination IPs. Prevents LAND attack.

The DoS ICMP sub-function can drop the following two kinds of packets: 1. ICMP ping packets whose size is larger than icmp-value; 2. ICMP packets, ICMPv6 packets. Prevents PING attack.

The DoS l4port sun-function can drop those TCP/UDP packets whose source port is equal to the destination port.

The DoS mac sub-function can check packet MAC address and prevents those packets whose source MAC addresses equal to destination MAC address.

The DoS tcpflags sub-function can drop the following 4 kinds of TCP packets: 1. TCP SYN flag=1 & source port<1024; 2.TCP control flags = 0 & sequence = 0; 3.TCP FIN URG PSH =1 & sequence = 0; 4.TCP FIN SYN =1.

The DoS tcpfrag sub-function can drop the following two kinds of TCP packets: 1. The TCP header is smaller than the first TCP fragment of tcpfrag-value; 2. TCP fragments whose offset values are 1. Prevents tear drop attack.

The DoS tcpsmurf sub-function can prevent tcpmurf attack and those TCP packets whose destination addresses are broadcast addresses.

The DoS icmpsmurf sub-function can prevent icmpsmurf attack and those ICMP packets whose destination addresses are broadcast addresses.

The DoS icmpsmurf sub-function can prevent icmpsmurf attack and those IP packets whose destination addresses are broadcast addresses.

Example

The following example shows how to set the global DoS attack prevention function to prevent those IP packets whose source IPs are destination IP addresses.

```
Switch_config#dos enable ip
```

The following example shows how to detect illegal TCPflag packets.

```
Switch_config#dos enable tcpflags
```

38.1.2 show dos

Syntax

To show all DoS attack prevention functions that users have set, run this command.

show dos

Parameters

None

Default Value

None

Usage Guidelines

EXEC mode

Example

The following example shows how to display all DoS attack prevention functions.

```
Switch_config#dos enable all
Switch_config#show dos
dos enable icmp
dos enable ip
dos enable l4port
dos enable mac
dos enable tcpflags
dos enable tcpfrag
dos enable tcpsmurf
dos enable icmpsmurf
dos enable ipsmurf

Switch_config#
```

The following example shows how to set dos enable ip to display the sub-function that users have set.

```
Switch_config#dos enable ip
Switch_config#show dos
dos enable ip
```

Chapter 39 Attack Prevention Configuration Commands

39.1 Attack prevention configuration commands

39.1.1 filter period

filter period *time*
Configure the attack detection period.
no filter period
Restore the attack detection period to the Default Value.

Parameters

Parameters	ParametersDescription
time	Attack detection detection period in seconds. The attack source sends more than A certain number of messages are considered an attack. Range: 1-600 seconds.

Default Value

time Default Value is 10 seconds

Command mode

Global configuration state

Example

```
Switch_config# filter period 15
```

Related commands

filter threshold

39.1.2 filter threshold

filter threshold *type value*
Configure the number of packets received during the detection period as an attack. Can be set differently for different message types.

no filter threshold *type*
Restore the detection threshold of a certain type of packets to the Default Value.

Parameters

Parameters	Parameters Description
type	Message types, including: ARP, BPDU, DHCP, IGMP, ICMP, IP.
value	Attack detection is considered an attack when it receives value packets in any period. Range: 5-2000.

Default Value

value Default Value is 1000 messages

Command mode

Global configuration state

Example

```
Switch_config# filter threshold ip 1500
```

Related commands

filter period

39.1.3 filter block-time

filter block-time *value*
Configure how long the attack source is blocked after an attack is detected in Raw mode.
no filter block-time
The time to resume blocking the attack source is the Default Value.

Parameters

Parameters	ParametersDescription
value	The time, in seconds, that the attack source is blocked after an attack is detected. Range: 1-86400. Attack prevention configuration commands

Default Value

value Default Value is 300 seconds

Command mode

Global configuration state

Example

```
Switch_config# filter block-time 600
```

Related commands

filter period
filter threshold

39.1.4 filter polling period

filter polling period *time*
Configure the polling cycle of attack sources in hybrid mode.
no filter polling period
The cycle of polling the attack source in the hybrid mode (Hybrid) is set to the Default Value.

Parameters

Parameters	Parameters Description
time	The period of polling detection after blocking the attack source, in seconds. Range: 1-600.

Default Value

time Default Value is 10 seconds

Command mode

Global configuration state

Example

```
Switch_config# filter polling period 20
```

Related commands
filter polling threshold
filter polling auto-fit

39.1.5 filter polling threshold

filter polling thredhold *type value*
Configure the number of attack packets received in one polling detection period in the mixed mode to consider that the attack source still exists. Can be set differently for different message types.
no filter polling threshold *type*
The packet threshold for resuming the rotation training test is the Default Value.

Parameters

Parameters	Parameters Description
type	Message types, including: ARP, BPDU, DHCP, IGMP, ICMP, IP.
value	When a value packet is received within any one polling period, the attack source is considered to still exist. Range: 1-2000.

Default Value

value Default Value is 750 messages

Command mode

Global configuration state

Example

```
Switch_config# filter polling threshold ip 1500
```

Related commands

filter polling period
filter polling auto-fit

39.1.6 filter polling auto-fit

filter polling auto-fit Attack prevention configuration commands
Configure the period and threshold parameters for poll detection to update automatically when the parameters detected by the attack source change. The command Default Value is valid. The polling period is equal to the attack detection period. The polled packet threshold is equal to three-quarters of the attack detection packet threshold.
no filter polling auto-fit
Cancel the automatic update of Polling Detection Parameters.

Parameters

None

Command mode

Global configuration state

Example

```
Switch_config# filter polling auto-fit
```

Related commands

filter polling period
filter polling threshold

39.1.7 filter igmp

filter igmp
Allow detection of IGMP attacks.
no filter igmp
Turn off detection of IGMP attacks.

Parameters

None

Command mode

Global configuration state

Example

```
Switch_config# filter igmp
```

Related commands

filter enable

39.1.8 filter ip source-ip

filter ip source-ip
Allow detection of IP attacks
no filter ip source-ip
Turn off detection of IP attacks.

Parameters

None

Command mode

Global configuration state and physical port configuration state.
This function takes effect when both global and physical ports are configured.

Example

```
Switch_config# filter ip source-ip
Switch_config# interface g0/1
switch_config_g0/1# filter ip source-ip
```

Related commands
filter enable

39.1.9 filter icmp

filter icmp
Allow detection of ICMP attacks.
no filter icmp
Turn off detection of ICMP attacks.

Parameters

No attack prevention configuration commands

Command mode

Global configuration state and physical port configuration state.
This function takes effect when both global and physical ports are configured.

Example

```
Switch_config# filter icmp
Switch_config# interface g0/1
switch_config_g0/1# filter icmp
```

Related commands

filter enable

39.1.10 filter dhcp

filter dhcp
Allow detection of DHCP attacks.
no filter dhcp
Turn off detection of DHCP attacks.

Parameters

None

Command mode

Global configuration state and physical port configuration state.
This function takes effect when both global and physical ports are configured.

Example

```
Switch_config# filter dhcp
Switch_config# interface g0/1
switch_config_g0/1# filter dhcp
```

Related commands

filter enable

39.1.11 filter arp

filter arp
Allow detection of ARP attacks.
no filter arp
Turn off detection of ARP attacks.

Parameters

None

Command mode

Physical interface configuration state

Example

```
Switch_config_g0/1# filter arp
```

Related commands

filter enable

39.1.12 filter bpdu

filter bpdu
Allow detection of BPDU attacks.
no filter bpdu
Turn off detection of BPDU attacks.

Parameters

None

Command mode

Physical interface configuration

Example

```
Switch_config_g0/1# filter bpdu
```

Related commands

filter enable

39.1.13 filter mode

filter mode [raw | hybrid]
Configure the mode of the Filter.

Parameters

Parameters	ParametersDescription
raw	Configure Filter to Raw mode.
hybrid	Configure the Filter to Hybrid mode.

Default Value

Filter Default Value is Hybrid mode.

Command mode

Global configuration state

Example

```
Switch_config# filter mode raw
```

Related commands

filter enable

39.1.14 filter enable

filter enable
Enable attack detection globally.
no filter enable
Globally turn off attack detection. All blocked attack sources will be unblocked.

Parameters

None

Command mode

Global configuration state

Example

```
Switch_config# filter enable
```

Related commands

None

39.1.15 show filter

show filter
Display the working status of the current switch attack prevention function
show filter summary
Displays the current Parameters configuration and statistics of the anti-attack function.

Parameters

None

Command mode

Non-user mode

Example

```
Switch#show filter
Filter period 600 seconds, polling interval 600 seconds
Filter thresholds:
Filter type(major code)      Minor code      Threshold      Polling
arp                          A               5              3
```

```
bpdu                    B              1000          750
dhcp                    D              1000          750
ip                      I              1000          750
icmp                    I              1000          750
igmp                    I              1000          750


Filters blocked:
Cause      Address            Seconds    Discard     Rate     Polling    Interface
arp        0000.abcd.1234     7.41       0           0/0      592.59     G0/1

Filters counting:
Cause      Address            Seconds      Count     Interface
arp        0000.abcd.1234     15.59        1         G0/1
```

Filters blocked: Indicates the MAC address, blocked time, and source port of the attack source that has been blocked.

Filters counting: It indicates that the MAC address of the attack source, the length of time currently recorded, the number of packets received during this time, and the source port may be detected.

domain number	sync mode	master port
0	straight_forward	G0/20
1	straight_forward	(null)
2	straight_forward	(null)
3	straight_forward	(null)

```
delay-req record timeout 32(s)
IEEE 1588 on port G0/18 enabled
Port Data Set
clock identity       .. 00-E0-0F-FF-FE-DB-0B-66
port number       1
log pdelay interval       0
current path delay       000000000.000000000
domain number  0

Request_Respond Mechanism (E2E) on port G0/18 is ON
current sequece id 59983

IEEE 1588 on port G0/20 enabled

Port Data Set
clock identity ..... 00-E0-0F-FF-FE-DB-0B-68
port number       2
log pdelay interval       0
current path delay       000000000.000000000
domain number  0
Request_Respond Mechanism (E2E) on port G0/20 is ON
 current sequece id 0
Switch#
```

Chapter 40 IP Addressing Configuration ommands

40.1 Addressing Configuration Commands

IP addressing configuration commands include:

- arp
- arp scan
- arp timeout
- clear arp-cache
- ip address
- ip directed-broadcast
- ip forward-protocol udp
- ip helper-address
- ip host name
- ip proxy-arp
- ip unnumbered
- keepalive
- show arp
- show hosts
- show ip interface

40.1.1 arp

To configure the static ARP which will permanently be stored in the ARP cache, run arp [vrf *vrf-name*] *ip-addresshardware-address* [alias]. To delete the configured static ARP, run no arp [vrf *vrf-name*] *ip-address*.

arp [vrf *vrf-name*] *ip-address hardware-address* [alias]
no arp [vrf *vrf-name*] *ip-address*

Parameter

Parameter	Description
Vrf-name	VRF name (for the VRF version)
ip-address	IP address of the local link interface
hardware-address	Physical address of the local link interface
alias	(optional) the router will answer the ARP request from the IP address.

Default

No permanent static ARP mapping exists in the ARP cache.

Command Mode

Global configuration mode

Usage Description

A common host can support the dynamic ARP resolution; hence, you need not specially configure the static ARP mapping for the host. The vrf subcommand is used to specify which VRF the ARP item belongs to.

Example

The following command shows that the MAC address of the host with IP address 1.1.1.1 is set to 00:12:34:56:78:90.

arp 1.1.1.1 00:12:34:56:78:90

Related command

clear arp-cache

40.1.2 arp timeout

To configure the timeout value of the dynamic ARP item in the ARP cache, run arp timeout seconds. To resume the **Default** value of the ARP item, run no arp timeout or **Default** arp timeout.

```
arp timeout seconds
 no arp timeout
Default arp timeout
```

Parameter

Parameter	Description
seconds	Timeout value of the dynamic ARP item in the ARP cache, which means that the ARP cache obtained through dynamic resolution on the port will not be released at the timeout time

Default

180 seconds (3 minutes)

Command Mode

Interface configuration mode

Usage Description

If the timeout value of the dynamic ARP item is configured on the non-arp interface, the configuration is invalid. You can run show interface to display the timeout time of the ARP items on the port. See the following information:

ARP type: ARPA, ARP timeout 00:03:00

Example

The following **Example** shows that the timeout time of the dynamic ARP mapping on interface Ethernet 1/0 is set to 900 seconds, which enables the ARP cache to be refreshed rapidly.

```
interface ethernet 1/0
arp timeout 900
```

Related command

show interface

40.1.3 clear arp-cache

To delete all dynamic ARP cache, run the following command:

clear arp-cache

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

The following command is used to delete all dynamic ARP cache.

clear arp-cache

Related command

Arp

40.1.4 ip address

To configure the IP address of the interface and the network mask simultaneously, run ip address. Currently, the IP addresses cannot be clearly classified into A type, B type and C type. However, the multicast address and the broadcast address cannot be used. Except the Ethernet, multiple interfaces of other types of network can work on the same network segment. The network segment configured by the Ethernet interface cannot be same to that configured by other types of interfaces, unnumbered interfaces excluded. One main address and multiple accessory addresses can be configured on an interface. The accessory address can be configured only after the main address is configured, while the main address can be deleted only after all accessory addresses are deleted. If the upper-layer application does not specify the source address of the system-generated IP packet, the router will adopt the IP address (configured on the transmitter interface and is in the same network segment as the gateway); if the IP address cannot be determined, the main address of the transmitter interface will be adopted. If the IP address of an interface is not configured and the interface is not an unnumbered interface, the IP packets will not be handled on the interface.

To delete an IP address or stop the IP packets from being handled on an interface, run

no ip address.

ip address *ip-address mask* [secondary]

no ip address *ip-address* mask no ip address

Parameter

Parameter	Description
ip-address	IP address
mask	Mask of the IP network
secondary	(optional) specifies an accessory IP address. If the IP address is not specified, it must be a main IP address.

Default

No IP addresses is configured on the interface.

Command Mode

Interface configuration mode

Usage Description

If you configure the accessory IP address on a physical network segment through the router, you must configure the accessory IP address of the same logical network segment for other systems on the same physical network segment; otherwise, the routing loop will be easily generated.

When the OSPF protocol is used, make sure that the accessory address and the main address of an interface must be in the same OSPF area.

Example

The following **Example** shows that the main address on interface Ethernet1/0 is set to 202.0.0.1, network mask is set to 255.255.255.0 and two accessory IP addresses are set to 203.0.0.1 and 204.0.0.1 respectively.

```
interface ethernet1/0
ip address 202.0.0.1 255.255.255.0
ip address 203.0.0.1 255.255.255.0 secondary
ip address 204.0.0.1 255.255.255.0 secondary
```

40.1.5 ip directed-broadcast

Toforward the directed IP broadcast and transmit the packets in the physical broadcast form, run IP directed-broadcast [access-list-namer].

```
ip directed-broadcast [access-list-namer]
no ip directed-broadcast
```

Parameter

Parameter	Parameter Description
access-list-name	Name of the access list, which is an optional. If the access list is defined, only broadcast packets permitted by the access list can be forwarded.

Default

The directed IP broadcast will not be forwarded by **Default**

Command Mode

Interface configuration mode

Example

The following **Example** shows how to configure the directed IP broadcast forwarding on interface Ethernet1/0.

```
interface ethernet 1/0
ip directed-broadcast
```

40.1.6 ip forward-protocol udp

To specify which UDP packets to be forwarded after IP helper-address is configured on the interface, run ip forward-protocol udp [*port*].

```
ip forward-protocol udp [port]
no ip forward-protocol udp [port]
Default ip forward-protocol udp
```

Parameter

Parameter	Description
ISDN(BRI)	(optional) destination port which the to-be-forwarded UDP packets is transmitted to

Default

The NETBIOS Name Service packet is forwarded.

Command Mode

Global configuration mode

Usage Description

The NETBIOS Name Service packet is forwarded by **Default**; to stop forwarding the NETBIOS Name Service packet, run either of the following two commands:

```
no ip forward-protocol udp netbios-ns
no ip forward-protocol udp 137
```

To stop forwarding all UDP packets, run the following command:

no ip forward-protocol udp

Example

Router_config#ip forward-protocol udp 137

Related command

ip helper-address

40.1.7 ip helper-address

To forward the directed IP packets to the designated IP helper address (unicast address or broadcast address), run ip helper-address. You can configure multiple helper addresses on each interface.ip helper-address *address*

no ip helper-address [*address*]

Parameter

Parameter	Description
address	IP helper address

Default

The IP helper address is not configured.

Command Mode

Interface configuration mode

Usage Description

The command is invalid on the X.25 interface, because the router cannot identify physical broadcasts.

Example

The following **Example** shows how to set the IP helper address on interface ethernet1/0 to 1.0.0.1.

interface ethernet 1/0
ip helper-address 1.0.0.1

Related command

ip forward-protocol udp

40.1.8 ip proxy-arp

To enable the agent ARP on the interface, run ip proxy-arp. To disable the agent ARP on the interface, run no ip proxy-arp.

ip proxy-arp
no ip proxy-arp

Parameter

The command has no **Parameter**s or keywords.

Default

The agent ARP is conducted.

Command Mode

Interface configuration mode

Usage Description

When the router receives the ARP request, if the router has the route to the requested IP address and the routing interface is different from the request-received interface, the router will send the ARP response out through its own MAC address; after then, the actual data packet will be forwarded after it is received. In this way, a host can communicate with the remote host even if the host does not completely learn the network topology or the correct router is not set for the host. The host is in the same physical subnet as a remote host is.

If a host requires the router to provide the service, the host and the router must be in the same IP network, or at least the router takes that the IP address of the host and the router are in the same IP subnet, that is, they use different masks. The router, otherwise, cannot provide the service.

Example

The following **Example** shows how to enable the ARP agent on interface ethernet1/0.

```
interface ethernet 1/0
ip proxy-arp
```

40.1.9 ip unnumbered

To set an interface to an unnumbered interface to enable the IP process function without configuring the IP address, run ip unnumbered *type number*. To stop the IP process on the interface, run no ip unnumbered.

ip unnumbered *type number*

no ip unnumbered

Parameter

Parameter	Description
type number	Type and number of an interface whose IP address is configured The interface cannot be the unnumbered interface which has adopted the IP address of other interfaces.

Default

The function is disabled.

Command Mode

Interface configuration mode

Usage Description

You need not configure the unique IP address for the point-to-point link interface. You can run the command to directly handle the IP and specify the valid IP address of other interfaces as the source address of the packets transmitted from the interface. The IP address is thus

saved. The point-to-point interface can be called as the unnumbered interface. IP packets generated on the unnumbered interface, such as route-refresh packets, will use the valid IP addresses configured on the command-designated interface. The address must be used to determine which routing processes are sending the refresh packets on the interface. However, it has the followinglimitations:

The command can set serial interfaces/channel interfaces that are encapsulated by HDLC, PPP, LAPB and SLIP to unnumbered interfaces. However, the command cannot be used on the X.25 interface and the SMDS interface.

You cannot check whether the interface works normally through the ping command. However, you can use SNMP to check the state of the interfaceremotely.

The command realizes its function based on the regulation in RFC 1195 that the valid IP address cannot be configured on the interface.

Pay attention to the serial links (between different networks) that adopt the IP address of other interfaces; any routing protocol running on the serial link cannot broadcast any information about each subnet.

Example

The following **Example** shows how to set interface serial0/0 to an unnumbered interface and adopt the valid IP address, 1.0.0.1, which configured on interface ethernet0/1, as the source address of the packet transmitted from the interface.

```
interface ethernet 0/1
ip address 1.0.0.1 255.255.255.0
interface serial 0/0
ip unnumbered ethernet 1/0
```

40.1.10 keepalive

To test the reachablity of the host and the connectivity of the network, run the following command:

```
keepalive [ group group-id ] [ source source-address ] [interval interval-time] [number number] destination destination-address
```

Parameter

Parameter	Description
group *group-id*	Multiple keepalive commands can be configured and can be identified by the group ID. The **Default** value of the group ID is 0.
source *source-address*	Specifies the source IP address adopted by the packet. **Default**: the main IP address of the transmitted interface
interval *interval-time*	Interval for transmitting the packet, whose unit is second **Default** value: 1 second
number *number*	Number of the transmitted packets Its **Default** value is 5.
destination *destination-address*	Destination host

Command Mode

EXEC or global configuration mode

Usage Description

The keepalive command supports the broadcast address and the multicast address. If the address is the limited broadcast address or the multicast address, the ICMP response packet will be transmitted on all interfaces supporting broadcasts and multicasts.

The command need not wait for the ICMP response packet, which only transmits the designated number of ICMP packets to the destination address regularly.

Example

The following shows that two keepalive commands are configured.

You can make a configuration that 10 ICMP request packets are transmitted from source address 192.168.20.230 to destination address 192.168.20.1 every 10 seconds. The packet-transmitting port is determined through destination address 192.168.20.1 and the routing protocol.

keepalive group 1 destination 192.168.20.1 source 192.168.20.230 interval 10 number 10

You can make a configuration that five ICMP request packets are transmitted from source address 172.16.20.232 to destination address 172.16.20.5 every second. The packet-transmitting port is determined through destination address 172.16.20.2 and the routing protocol.

keepalive group 2 destination 172.16.20.2 source 172.16.20.232

40.1.11 show arp

To display all ARP items, including the ARP mapping of the IP address for the interface, static ARP mapping and dynamic ARP mapping, run the following command:

show arp [vrf *vrf-name*]

Parameter

Parameter	Description
Vrf-name	ARP item which specifies which VRF to be displayed

Command Mode

EXEC

Usage Description

The displayed information shows in the following table:

Parameter	Description
Protocol	Protocol type, such as the IP protocol
Address	Address type, such as the IP address
Age	Lifetime, that is, the duration of ARP item from its generation (unit: minute) The fact that the router uses the ARP item does not affect the value.
Hardware Address	Physical address corresponding to the network address, which is null for the resolved item
Type	Type of packet encapsulation used by the interface, including ARPA and SNAP
Interface	Interface relative with the network address

Example

The following command is used to display the ARP cache.

```
router#show arp
Protocol  IP Address  Age(min)  Hardware Address  Type Interface
IP  192.168.20.77  11  00:30:80:d5:37:e0 ARPA Ethernet1/0
IP  192.168.20.33  0  Incomplete
IP  192.168.20.22  -  08:00:3e:33:33:8a ARPA Ethernet1/0
IP  192.168.20.124  0  00:a0:24:9e:53:36 ARPA Ethernet1/0
IP  192.168.0.22  -  08:00:3e:33:33:8b ARPA Ethernet1/1
```

40.1.12 show ip hosts

To display all items in the hostname-address cache, run the following command:

```
show ip hosts
```

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

The following **Example** shows how to display all hostname-address mappings:

show ip hosts

Related command

```
clear ip host
```

40.1.13 show ip interface

To display the IP configuration of the interface, run the following command:

```
show ip interface [type number]
```

Parameter

Parameter	Description
type	Type of the interface, which is optional
number	Number of the interface, which is optional

Command Mode

EXEC

Usage Description

If the link layer of an interface can effectively transmit and receive the data, the interface is available, whose state is Protocol Up. If an IP address is configured on the interface, the router will add an direct-through route to the routing table. If the link-layer protocol is disabled, that is, if the link-layer protocol is Protocol Down, the direct-through route will be deleted. If the interface type and the number of the interface is specified, only the information about the specified interface is displayed. Otherwise, the information about the IP configuration of all interfaces is displayed.

Example

The following **Example** shows that the IP configuration of interface e0/1 is displayed.

```
Router#show ip interface e0/1
Ethernet1/0 is up, line protocol is up
 IP address : 192.168.20.167/24
Broadcast address : 192.168.20.255
Helper address : not set
MTU : 1500(byte)
Forward Directed broadcast : OFF
Multicast reserved groups joined:
224.0.0.9 224.0.0.6 224.0.0.5 224.0.0.2
224.0.0.1
Outgoing ACL : not set
Incoming ACL : not set
 IP fast switching : ON
IP fast switching on the same interface : OFF
ICMP unreachables : ON
ICMP mask replies : OFF
 ICMP redirects : ON
```

The following table gives a detailed description to some **Parameter**s in the previous **Example**.

Domain	Description
Ethernet1/0 is up	If the hardware of the interface is available, the interface will be identified as up. If the interface is available, its hardware and line protocols must be in the up state.
line protocol is up	If the interface can provide bidirectional communication, the line protocol will be identified as up. If the interface is available, its hardware and line protocols of the interface must be in the up state.
IP address	IP address of an interface and network mask
Broadcast address	Displays the broadcast address.
MTU	Displays the IP MTU configured on the interface.
Helper address	Displays the IP helper address.
Directed broadcast forwarding	Forwards the directed broadcast packets.

Domain	Description
Multicast reserved groups joined	Multicast groups added to the interface
Outgoing ACL	Outgoing access control list used by the interface
Incoming ACL	Incoming access control list used by the interface
IP fast switching	Enables fast switching on the interface by the router.
Proxy ARP	Enables the proxy ARP on the interface.
ICMP redirects	Forwards the ICMP redirect packet on the interface.
ICMP unreachables	Forwards the ICMP-unreachable packet on the interface.
ICMP mask replies	Forwards the ICMP-mask-replies packet on the interface.

40.2 NAT Configuration Commands

NAT configuration commands include:

- ip nat
- ip nat local-service
- ip nat enable-peek
- ip nat inside destination
- ip nat inside source
- ip nat outside source
- ip nat pool
- ip nat translation
- clear ip nat statistics
- clear ip nat translation
- show ip nat statistics
- show ip nat translations
- debug ip nat

40.2.1 ip nat

ip nat {inside | outside | mss inside | outside | mss }
no ip nat {inside | outside | mss *MSS-value*}

Parameter

Parameter	Description
Inside	Shows that the interface connects the internal network (NAT is applied on the network).
Outside	Shows that the interface connects the exterior network (NAT is applied on the network).
mss *MSS-value*	Sets MSS to MSS-value after ip nat outside must be configured.

Default

The communication volume transmitted or received by the interface does not obey the NAT regulation.

Command Mode

Interface configuration mode

Usage Description

Only the packets forwarded between interior interfaces and exterior interfaces can be translated. Each boundary router where the NAT function is applied must be specified at least one interior interface and one exterior interface.

You can run IP NAT to specify that the communication volume coming from the interface or transmitted to the interface obeys NAT; to forbid the NAT function on the interface, run no IP nat.

NOTE: The ip nat mss command can be configured only on the interface of IP NAT outside. Its function is to modify the maximum segment size (MSS) in the synchronous TCP packets that are transmitted from the interior network. To forbid the interface to modify MSS, run no ip nat mss.

Example

The following **Example** shows that the IP address of packets from host 192.168.1.0 or host 192.168.2.0 is translated to the unique IP address of network 171.69.233.208/28 and MSS is modified to 1432.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208

interface ethernet 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
ip nat mss 1432

interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside

ip access-list standard a1
```

permit 192.168.1.0 255.255.255.0
permit 192.168.2.0 255.255.255.0

40.2.2 ip nat local-service

ip nat local-service {icmp | udp | tcp } disable
no ip nat local-service {icmp | udp | tcp } disable

Parameter

Parameter	Description
Icmp	Icmp packet
Udp	Udp packet
Tcp	Tcp packet

Default

None

Command Mode

Interface configuration mode

Usage Description

The command is used to the NAT regulations. By **Default**, all ICMP/UDP/TCP packets to access the local router are permitted on the router's interface which is identified as the NAT exterior port. The command can limitedly prevent exterior network users from viciously attack the router; however, the packets which normally access the router will be dropped.

To forbid the local ICMP/UDP/TCP packets to access the local router through the router's interface which is identified as the NAT exterior port, you need configure the ip nat local-service {icmp | udp | tcp } disable command. You can use the "no" form of the command to resume the **Default** state.

NOTE: The command can be configured only on the router's interface where the NAT-identified exterior port lies and can be used to disable only the interface toreceive the ICMP/UDP/TCP packets.

40.2.3 ip fastaccess

ip fastaccess deny {tcp | udp | icmp} {*port number*}
no ip fastnat deny {tcp | udp | icmp} {*port number*}

Parameter

Parameter	Description
Deny	Defines the regulations of the deny packets.
Tcp	Defines the regulations of the tcp packets.
Udp	Defines the regulations of the udp packets.
Icmp	Defines the regulations of the icmp packets.
Port number	Number of the TCP/UDP port, ranging between 1 and 10000

Default

None

Command Mode

Interface configuration mode

Usage Description

Because the ip fastaccess command is used to limit packet forwarding on the basis of the transmission layer, the general access list will be used if packet forwarding is limited based on the IP address.

Advice: If you want to constrain interior users through general access lists in the premises of using dynamic NAT regulations, you are strongly recommended to use the NAT-adopted access list. This method can greatly improve the performance especially for the access lists which require to define many regulations.

40.2.4 ip fastnat 1to1

ip fastnat 1to1 outside {*interface-type number*} [backup-outside {*interface-type number*}] inside {*interface-type number*} [privateservices] [extend]

no ip fastnat

Parameter

Parameter	Description
outside *interface-type number*	Designated network interface which is identified as NAT OUTSIDE, which is the exit of the main line
backup-outside *interface-type number*	Designated network interface which is identified as NAT INSIDE, which is the exit of the backup line
inside interface type number	Designated network interface which is identified as NAT INSIDE, which is the entrance of the backup line
privateservices	(optional) Enables the private service.
extend	(optional) Enables the expanded access list.

Default

None

Command Mode

Global configuration mode

Usage Description

The command has requirements for network environment. For details, see the configuration manual.

If the private service or expanded access control list is not used, do not use the privateservices option or the extend option.

40.2.5 ip nat inside destination

To enable the NAT of the interior destination address, run ip nat inside destination. To delete the dynamic connection with the address pool, run no ip nat inside destination.

```
ip nat inside destination list access-list-name pool name
no ip nat inside destination list access-list-name
```

Parameter

Parameter	Description
list name	Name of the standard IP access control list, which is used to translate the packets with the destination address through the global address in the designated address pool
pool name	Name of the address pool During the dynamic translation, the address pool will distribute interior local IP addresses.

Default

The interior destination address is not translated.

Command Mode

Global configuration mode

Usage Description

The command is used to create the dynamic address translation in the access control list form. For the packets from the address matched with the standard access control list, the global address allocated by the designated address pool will be used to translate. The address pool is specified by the ip nat pool command.

Example

The following **Example** shows that the packets from network 171.69.233.208 are translated to the address of the interior host whose destination address lies at network segment 192.168.2.208.

```
ip nat pool net-208 192.168.2.208 192.168.2.223 255.255.255.240
ip nat inside destination list a1 pool net-208
interface ethernet 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
ip access-list standar a1
```

permit 171.69.233.208 255.255.255.240

40.2.6 ip nat inside source

To enable the NAT of the interior source address, run ip nat inside source. To delete the static translation or the dynamic connection with the address pool, run no ip nat inside source.

Dynamic NAT:

ip nat inside source {list *access-list-name*} {interface *type number* | pool *pool-name*} [overload]

no ip nat inside source {list *access-list-name*} {interface *type number* | pool *pool-name*} [overload]

Static NAT for a single address:

ip nat inside source {static {*local-ip global-ip*}

no ip nat inside source {static {*local-ip global-ip*} Static port NAT:

ip nat inside source {static {tcp | udp *local-ip local-port* {*global-ip* | interface *type number*} *global-port*}

no ip nat inside source {static {tcp | udp *local-ip local-port* {*global-ip* | interface *type number*} *global-port*}

Static NAT of the network segment:

ip nat inside source {static {network local-network global-network *mask*}

no ip nat inside source {static {network local-network global-network *mask*}

Parameter

Parameter	Description
List access-list-name	Name of the IP access control list The packets whose source addresses matches the access control list will be translated by the global address of the address pool.
pool name	Name of the address pool where the global IP addresses are dynamically distributed
interface type number	Specifies the network interface.
Overload	(optional) enables the router to use one global address for multiple local addresses. After the overload **Parameter** is set, multiple sessions of similar hosts or different hosts will be differentiated by TCP numbers or UDP numbers.
static local-ip	Creates an independent static address translation. It is a local IP address which is distributed to the interior hosts. The local IP address can be selected freely or distributed from RFC 1918.
local-port	Sets the local TCP/UDP number, ranging between 1 and 65535.
static global-ip	Creates independent static address translation. That is, it is used to create an IP address through which an exterior network can access uniquely.
global-port	Sets the global TCP/UDP number, ranging between 1 and 65535.
Tcp	Sets TCP port translation.
Udp	Sets UDP port translation.
network local-network	Sets the translation for the local network segment.
global-network	Sets the translation for the global network segment.
Mask	Sets the network mask for the network segment translation.

Default

The NAT of any interior source address does not exist.

Command Mode

Global configuration mode

Usage Description

The command has two modes: dynamic address translation and static address translation. The dynamic translation is created for the access control list form. For the packets from the address matched with the standard access control list, the global address allocated by the designated address pool will be used to translate. The address pool is specified by the ip nat pool command.

As a secondary method, the **Syntax** format with keyword STATIC need an independent static address translation to be created.

To enable the static NAT to support the PASV mode of FTP, those commands to match the overload type are required. When a static FTP mapping of NAT is set, the overload type transfer is needed and one of the addresses of the exterior-network interface following the PAT regulations must be the same as the exterior-network address of the static FTP.

Example

The following **Example** shows that the IP address of packets from host 192.168.1.0 or host 192.168.2.0 is translated to the unique IP address of network 171.69.233.208/28.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
interface ethernet 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
ip access-list standard a1
permit 192.168.1.0 255.255.255.0
permit 192.168.2.0 255.255.255.0
```

The following is an **Example** of using the PASV mode of the static FTP.

```
ip nat inside source static tcp 10.1.1.1 21 204.112.1.2 8021
ip nat inside source static tcp 10.1.1.1 20 204.112.1.2 8020
ip nat inside source list test1 interface f0/0
```

40.2.7 ip nat outside source

To enable the NAT of the exterior source address, run ip nat outside source. To delete the static items or dynamic connection, run no ip nat outside source.

NOTE: Dynamic NAT regulations and static network-segment NAT regulations cannot be deleted if they are being used.

Dynamic NAT:

ip nat outside source {list *access-list-name*} pool *pool-name*

no ip nat outside source {list *access-list-name*} pool *pool-name*

Static NAT for a single address:

ip nat outside source static {*global-ip local-ip*} no ip nat outside source static {*global-iplocal-ip*} Static port NAT:

ip nat outside source {static {tcp | udp *global-ip global-port local-ip local-port*}

no ip nat outside source {static {tcp | udp *global-ip global-port local-ip local-port*} Static NAT of the network segment:

ip nat outside source {static network *global-network local-network mask*}

no ip nat outside source {static network *global-network local-network mask*}

Parameter

Parameter	Description
List access-list-name	Name of the standard IP access control list The packets whose source addresses matches the access control list will be translated by the global address of the address pool.。
pool name	Name of the address pool where the global IP addresses are dynamically distributed
Static global-ip	Creates an independent static address translation. It is a global IP address which is distributed by the hosts creating the exterior network. The address can be distributed in the globally-routing network address space.
global-port	Sets the global TCP/UDP number, ranging between 1 and 65535.
Static local-ip	Creates independent static address translation. That is, it is used to create an local IP address of the exterior host througich an interior network can access uniquely. The address can be distributed in the address space which can be routed by the interior network.
local-port	Sets the local TCP/UDP number, ranging between 1 and 65535.
Tcp	Sets TCP port translation.
Udp	Sets UDP port translation.
network global-network	Sets the translation for the global network segment.
local-network	Sets the translation for the local network segment.
Mask	Sets the network mask for the network segment translation.

Default

The translation between the source addresses of the exterior network and the interior network address does not exist.

Command Mode

Global configuration mode

Usage Description

You probably use the illegal and abnormally-distributed IP address. You also probably use the IP address which is normally distributed to other networks. The fact that the IP address is legally used by the exterior network and also illegally used by the interior network is defined as address overlapping. The NAT can be used to translate the interior addresses which are overlapped with the exterior addresses. If the IP address of your single-connection network is same to the legal IP address of another network and you need communicate with these hosts or routers, you can use the function.

The command has two modes: dynamic address translation and static address translation. The dynamic translation is created for the access control list form. For the packets from the address matched with the standard access control list, the local address allocated by the designated address pool will be used to translate. The address pool is specified by the ip nat pool command.

As a secondary method, the **Syntax** format with keyword STATIC need an independent static address translation to be created.

Example

The following **Example** shows that the IP address of packets among hosts in network 9.114.11.0 is translated to the unique global IP address of network 171.69.233.208/28.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat pool net-10 10.0.1.0 10.0.1.255 255.255.255.0
ip nat inside source list a1 pool net-208 ip nat outside source list a1 pool net-10
interface ethernet 0
ip address 171.69.232.182 255.255.255.240
ip nat outside

interface ethernet 1
ip address 9.114.11.39 255.255.255.0
ip nat inside

ip access-list standard a1
permit 9.114.11.0 255.255.255.0
```

40.2.8 ip nat pool

To define an IP address pool for NAT, run ip nat pool. To delete the IP address pool with a designated name, run no ip nat pool.

ip nat pool name *start-ip end-ip netmask* [rotary]

no ip nat pool *name*

Parameter

Parameter	Description
Name	Name of the IP address pool
start-ip	Start IP address for defining the range of the IP address pool
end-ip	End IP address for defining the range of the IP address pool
Netmask	Subnet mask showing which bytes belong to the network and subnet and which bytes belong to the host parts; it can be used to specify the subnet mask of the network to which the addresses of the IP address pool belongs.
Rotary	Rotary address pool

Default

The IP address pool is not defined.

Command Mode

Global configuration mode

Usage Description

The command is used to define an IP address pool with the start IP address, end IP address and subnet mask.

Note: The rotary regulations of the IP address pool in the PAT regulations are shown in the following: only when all connections of an address are aging, the next address is required. That is, there is only one interior global address at the same time.

Example

The following **Example** shows that the IP address of packets from host 192.168.1.0 or host 192.168.2.0 is translated to the unique IP address of network 171.69.233.208/28.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208

interface ethernet 0
ip address 171.69.232.182 255.255.255.240
ip nat outside

interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside

ip access-list standard a1
permit 192.168.1.0 255.255.255.0
permit 192.168.2.0 255.255.255.0
```

40.2.9 ip nat service

The command is an entrance function provided for all services that NAT supports. Currently, only three kinds of services are provided. All services are disabled by **Default**.

```
ip nat service { h323 | privateservice | peek }
no ip nat service { h323 | privateservice | peek }
```

Parameter

None

Default

Shut down

Command Mode

Global configuration mode

Usage Description

The command is used to control the NAT support of h323.

Private service is a kind of support that the NAT does to the internal game server of the cyber bar, such as the legend. It can control the NAT support of the private service.

The peek **Parameter** realizes the NAT support to the game monitor server in the cyber bar. Through the client soft of, you can monitor internal users' surfing.

The “no” form of the command is used to disable corresponding functions.

Example

```
ip nat service privateservice ip nat service peek
ip nat service h323 no ip nat service peek
```

40.2.10 ip nat translation

You can run ip nat translation to do the following:

Modifying the timeout value of the NAT translation. You can run no ip nat translation
to close the timeout.

```
ip nat translation {timeout | udp-timeout | dns-timeout | tcp-timeout |
finrst-timeout | icmp-timeout | syn-timeout } seconds
no ip nat translation {timeout | udp-timeout | dns-timeout | tcp-timeout |
finrst-timeout | icmp-timeout | syn-timeout }
```

Modifying the values of some **Parameter**s for NAT translation items. You can use the "no" form of the command to delete the previous configuration or resume the **Default** values.

ip nat translation max-entries { host [*A.B.C.D* | any] } *numbers*
no ip nat translation max-entries { host [*A.B.C.D* | any] }

Parameter

Parameter	Description
Timeout	Specifies the timeout value of the dynamic translations except the overload translation. The Default value is 3600 seconds.
udp-timeout	Specifies the timeout value for the UDP port. The Default value is 300 seconds.
dns-timeout	Specifies the timeout value to connect the DNS. The Default value is 60 seconds.
tcp-timeout	Specifies the timeout value for the TCP port. The Default value is 3600 seconds.
finrst-timeout	Specifies the timeout value of the finish and reset TCP message, which is used to terminate a translation item. The Default value is 60seconds.
icmp-timeout	Sets the timeout time of the NAT of ICMP; the Default value is 60 seconds.
max-entries	Sets the maximum number of the NAT translation items; the Default value is 3000.
syn-timeout	Sets the NAT timeout time of the TCP SYN state; the Default value is 60 seconds.
Seconds	Specifies the timeout value of the port translation. The Default value is the value listed out at the Default part.
max-entries host *A.B.C.D*	For the specified internal IP address, you can control the maximum number of the NAT translation items. There is no Default value. You can use the "no" form of the command not to control the maximum number of the NAT translation items.
max-entries host any	For all internal IP addresses, the maximum number of the NAT translation items can be controlled by limiting the single IP address. The Default value is same to max-entries.

Default

timeout is 3600 seconds (1 hours)
udp-timeout is 300 seconds (5 minutes)
dns-timeout is 60 seconds (1 minute)
tcp-timeout is 3600 seconds (1 hours)
finrst-timeout is 60 seconds (1 minute)

Command Mode

Global configuration mode

Usage Description

After the port translation is configured, you can further control the translation items for each translation item contains more information about the communication volume. The UDP translation of the DNS times out five minutes later, while that of the domain system times out one minute later. If there is no RST or FIN in the data flow, TCP translation times out one hour later; if there is RST or FIN, it will time out one minute later.

Example

Example 1:

The following **Example** shows that the UDP port translation times out 10 minutes later.

ip nat translation udp-timeout 600

Example 2:

The following **Example** shows that the maximum number of the NAT translation items created by IP 192.168.20.1 is set to 100.

ip nat translation max-entries host 192.168.20.1 100

40.2.11 clear ip nat statistics

To delete the NAT statistics information, run clear ip nat statistics. clear ip nat statistics

Parameter

None

Command Mode

EXEC

Usage Description

You can use the command to resume all NAT statistics information to the original state. Note:

Only the statistics **Parameter** behind the packets dropped option can be deleted.

Example

```
Router#show ip nat statistics
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:
FastEthernet0/1
Inside interfaces:
FastEthernet0/0
Dynamic mappings:
--Inside Source
  access-list nat
  pool natp: netmask 255.255.255.0
  start 172.16.20.125 end 172.16.20.127
```

```
   total addresses 3, misses 0
--Inside Destination
--Outside Source、
Link items:
   PAT(ICMP=5 UDP=39 TCP=224 / TOTAL=268), Dynamic=6
Packets dropped:
--Protocol:
   Out: tcp 123, udp 39, icmp 10, others 6
   In: tcp 46, udp 109, icmp 0, others 10
--Configuration:
   max entries 0, max entries for host 178
Router#clear ip nat statistics
Router#show ip nat statistic
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:
FastEthernet0/1
Inside interfaces:
FastEthernet0/0
Dynamic mappings:
--Inside Source
   access-list nat
   pool natp: netmask 255.255.255.0
   start 172.16.20.125 end 172.16.20.127
   total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:
   PAT(ICMP=5 UDP=39 TCP=224 / TOTAL=268), Dynamic=6
Packets dropped:
--Protocol:
   Out: tcp 0, udp 0, icmp 0, others 0
   In: tcp 0, udp 0, icmp 0, fragments 0
--Configuration:
   max entries 0, max links for host 0
```

40.2.12 clear ip nat translation

To delete dynamic NAT from the translation item, run the following commands:

```
clear ip nat translation {* | [inside local-ip global-ip ] [outside local-ip global-ip]}

clear ip nat translation {tcp|udp} inside local-ip local-port global-ip global-port
[outside local-ip global-ip]
```

Parameter

Parameter	Description
*	Deletes all dynamic translation items.
Inside	Deletes the internal translation consisting of the global IP address and the local IP address.
global-ip	Specifies the global IP address.
local-ip	Specifies the local IP address.
Outside	Deletes the external translation consisting of the designated global IP address and the local IP address.
tcp|udp	Protocol
global-port	Specifies the global port for the corresponding protocol.
local-port	Specifies the local port for the corresponding protocol.

Command Mode

EXEC

Usage Description

You can run the command to delete the dynamic translation items before they time out.

Example

The following **Example** shows that the NAT translation items are displayed first and then the UDP translation items are deleted.

```
Router# show ip nat translation
Pro Inside global  Inside local Outside local       Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53         171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23  171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23  171.69.1.161:23
Router# clear ip nat translation udp inside 171.69.233.209 1220 192.168.1.95 1220
171.69.2.132 53 171.69.2.132 53
Router# show ip nat translation
Pro Inside global  Inside local Outside local       Outside global
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23 171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23  171.69.1.161:23
```

40.2.13 show ip nat statistics

To display the NAT statistics table, run show ip nat statistics. show ip nat statistics

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

The following information is displayed after you run show ip nat statistics.

```
Router# show ip nat statistics
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:
FastEthernet0/1
Inside interfaces:
FastEthernet0/0
Dynamic mappings:
--Inside Source
   access-list nat
   pool natp: netmask 255.255.255.0
   start 172.16.20.125 end 172.16.20.127
   total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:
   PAT(ICMP=0 UDP=5 TCP=24 / TOTAL=29), Dynamic=0
Packets dropped:
--Protocol:
   Out: tcp 0, udp 0, icmp 0, others 0
   In: tcp 46, udp 100, icmp 0, others 0
--Configuration:
   max entries 0, max links for host 0
```

The important fields in the output results are listed in table 2-1.

Table 2- 1 Field description of show ip nat statistics

Field	Description
Total active translations:	Number of designated translations activated in the system When an address translation regulation is created, the value increases by 1; when an address translation regulation is deleted or times out, the value decreases by 1.
Outside interfaces:	List of outside interfaces which are identified by the ip nat outside command.
Inside interfaces:	List of inside interfaces which are identified by the ip nat inside command.
Dynamic mappings:	Information about dynamic mapping
Inside Source:	Information about the inside source address translation
Access-list	Number of access lists for address translation
Pool	Name of the address pool
Netmask	IP network mask used by the address pool
Start	Start IP address of the address range

Field	Description
End	End IP address of the address range
Total addresses	Number of addresses in the pool, which can be used for address translation
Misses	Number of addresses which cannot be distributed from the address pool
Inside Destination:	Information about the inside destination address translation
Outside Source:	Information about the outside source address translation
Link items:	Number and type of translation items
PAT	Number of translation items under dynamic port translation regulations, among which madia stands for the RTP/RTCP session.
Dynamic	Number of translation items under dynamic address translation regulations including FTP-created translation items translated from static addresses
Packets dropped:	Type, number and reason of the dropped packets
Protocol	Number, protocol type and NAT direction of the dropped packets
Configuration	Number of packets which are dropped for an incorrect reason: max entries means that the maximum number of translation items is exceeded; max links for host means that the number of translation items permitted by each address or a specific address is exceeded.

40.2.14 show ip nat translations

To display the activated NAT address translation, run show ip nat translations. show ip nat translations [host *A.B.C.D* | tcp | udp | icmp | verbose]

Parameter

Parameter	Description
host *A.B.C.D*	(optional) Displays translation items A, B, C and D which have the inside local address.
Tcp	(optional) Displays translation items which bear the TCP session.
Udp	(optional) Displays translation items which bear the TCP session.
Icmp	(optional) Displays translation items which bear the ICMP session.
Verbose	(optional) Displays extra information about each translation item, including how long it has been created and how long it times out.

Command Mode

EXEC

Usage Description

Example

The following information is displayed after you run show ip nat translations. Two inside hosts and some outside hosts are switching packets without overload.

```
Router# show ip nat translations
Pro Inside local    Inside global       Outside local      Outside global
--- 192.168.1.95    171.69.233.209      ---      ---
--- 192.168.1.89    171.69.233.210      ---      --
```

(3)The following **Example** shows that, at the overload condition, three address translation items are activated, among which one is for DNS and the other two are for the TELNET session. Note: two different inside hosts can appear with the same outsideaddress.

```
Router# show ip nat translations
Pro Inside local    Inside global       Outside local      Outside global
udp 192.168.1.95:1220       171.69.233.209:1220171.69.2.132:53    171.69.2.132:53
tcp 192.168.1.89:11012    171.69.233.209:11012      171.69.1.220:23     171.69.1.220:23
tcp 192.168.1.95:1067       171.69.233.209:1067  171.69.1.161:23    171.69.1.161:23
```

The following **Example** shows the information with the verbose keyword.

```
Router# show ip nat translations verbose
Pro Inside local    Inside global       Outside local      Outside global
udp 192.168.1.95:1220    171.69.233.209:1220 171.69.2.132:53     171.69.2.132:53
create time 00:00:02 , left time 00:01:10 ,
tcp 192.168.1.89:11012 171.69.233.209:11012 171.69.1.220:23 171.69.1.220:23
create time 00:01:13 , left time 00:00:50 ,
tcp 192.168.1.95:1067     171.69.233.209:1067 171.69.1.161:23      171.69.1.161:23
create time 00:00:02 , left time 00:53:19 ,
```

Table 2- 2 Fields of output results for the show IP NAT Translations command

Field	Description
Pro	Defines the port protocol of the address.
Inside global	Legal IP address, standing for one or multiple inside local IP addresses connecting the exterior network
Inside local	IP address which is allocated to the inside host It may not a legal address provided by NIC or SP.
Outside local	IP address of an outside host when it looks like an inside network, which may not be a legal address provided by NIC or SP
Outside global	IP address of the outside host which is distributed by the owner
Create time	Creation time of the translation item (its unit is hour: minute: second)
Left time	Timeout time of the address translation

40.2.15 debug ip nat

To debug NAT, run debug ip nat.
debug ip nat {detail | h323}
no debug ip nat {detail | h323}

Parameter

None

Command Mode

EXEC

Usage Description

You can run debug ip nat detail to export the details about the translation procedure, including the source/destination IP address, port number and the reason of the failed translation.

You also can run debug ip nat h323 to export the details about the NAT translation of the H323 packets, including the H323 information identified by NAT, the IP address of the message or the translated address for the inside address.

Example

Example 1:

```
Router# debug ip nat detail
Ethernet1/1 recv ICMP Src 194.4.4.89 Dst 10.10.10.102 no link found
Ethernet1/0 send TCP Src 194.4.4.102:2000 Dst 192.2.2.1:21 no matched rule
```

Table 2- 3 Fields in the previous **Example**

Field	Description
Ethernet1/0	Type and number of the interface
send/recv	Send/receive
ICMP/TCP/UDP	ICMP/TCP/UDP protocol
Src 194.4.4.102:2000	Source IP address and port number
Dst 192.2.2.1:21	Destination IP address and port number
no link found	Means that the NAT translation item is not matched.
no matched rule	Means that the NAT regulations are not matched.

The first command line shows that the ICMP packets are received by interface Ethernet1/1 and the corresponding NAT translation items are not found.

The second command line shows that the TCP packets are transmitted from interface Ethernet1/0 and the matched NAT regulations are not found.

Example 2:

```
Router# debug ip nat h323
NAT:H225:[I] processing a Setup message
NAT:H225:[I] found Setup sourceCallSignalling
NAT:H225:[I] fix TransportAddress addr-192.168.122.50:11140
NAT:H225:[I] found Setup fastStart
NAT:H225:[I] Setup fastStart PDU length:18
NAT:H245:[I] processing OpenLogicalChannel message, forward channel 1
NAT:H245:[I] found OLC forward mediaControlChannel
NAT:H245:[I] fix TransportAddress addr-192.168.122.50:16517
NAT:H225:[I] Setup fastStart PDU length:29
NAT:H245:[I] processing OpenLogicalChannel message, forward channel 1
NAT:H245:[I] found OLC reverse mediaChannel
NAT:H245:[I] fix TransportAddress addr-192.168.122.50:16516
 NAT:H245:[I] found OLC reverse mediaControlChannel
NAT:H245:[O] fix TransportAddress addr-192.168.122.50:16517
NAT:H225:[O] processing an Alerting message
NAT:H225:[O] found Alerting fastStart
NAT:H225:[O] Alerting fastStart PDU length:25
NAT:H245:[O] processing OpenLogicalChannel message, forward channel 1
```

The important fields are described in the following table.

Field	Description
NAT	Means the packet has been translated by NAT.
RAS/H255/H245	Protocol type of the packet
O	Transmission direction of the packet: inside to outside
I	Transmission direction of the packet: outside to inside

40.3 DHCP Client Configuration Command

DHCP client configuration commands include:

- ip address dhcp
- ip dhcp client
- ip dhcp-server
- show dhcp lease
- show dhcp server
- debug dhcp

40.3.1 ip address dhcp

To obtain an IP address for the Ethernet interface through DHCP, run ip address dhcp. To delete the obtained IP address, run no ip address dhcp.

```
ip address dhcp
no ip address dhcp
```

Parameter

None

Default

None

Command Mode

Interface configuration mode

Usage Description

The ip address dhcp command allows the interface to obtain the IP address through the DHCP protocol, which is useful for dynamically connecting the Internet service provider (ISP) through the Ethernet interface. Once the dynamic IP address is obtained, the Ethernet interface can adopt the PAT technology to realize the network address translation (NAT).

If the ip address dhcp command is configured on the router, the router will transmit the DHCPDISCOVER message to the DHCP server.

If the no ip address dhcp command is configured on the router, the router will transmit the DHCP RELEASE message.

Example

The following **Example** shows that interface Ethernet1/1 obtains its IP address through the DHCP protocol.

```
interface Ethernet1/1
ip address dhcp
```

Related command

```
ip dhcp client
ip dhcp-server
show dhcp lease
show dhcp server
```

40.3.2 ip dhcp client

To configure the **Parameter** about the DHCP client of the local router, run ip dhcp client.

```
ip dhcp client { minlease seconds | retransmit count | retry_interval | select
seconds }

no ip dhcp client { minlease | retransmit | retry_interval | select }
```

Parameter

Parameter	Description
minlease seconds	(optional) the minimum lease time, ranging from 60 to 86400 seconds
retransmit count	(optional) retransmit times of the protocol packets, ranging between 1 and 10
retry_interval	(optional) Interval for retriggering the DHCP request, ranging between 1 and 1440 minutes
select seconds	(optional) interval for the select operation, ranging between 0 and 30

Default

The **Default** value of the minlease **Parameter** is 60 seconds.

The **Default** value of the retransmit **Parameter** is four times.

The **Default** value of the retry-interval **Parameter** is five seconds.

The **Default** value of the select **Parameter** is 0 seconds.

Command Mode

Global configuration mode

Usage Description

You can adjust these **Parameter**s according to the network structure and the DHCP server's requirements.

If the "no" forms of these commands are configured, the **Parameter**s are reset to the **Default** values defined by the system.

Example

The following **Example** shows that the receivable minimum lease time of the DHCP client on the router is set to 100 seconds.

ip dhcp client minlease 100

The following **Example** shows how to set the retransmission times of the protocol packets on the DHCP client to three times.

ip dhcp client retransmit 3

The following **Example** shows how to set the interval of retriggering the DHCP request on the DHCP client to 10 minutes.

ip dhcp client retry_interval 10

The following **Example** shows how to set the interval of selecting on the DHCP client to 10 seconds.

ip dhcp client select 10

Related command

ip address dhcp

ip dhcp-server

show dhcp lease

show dhcp server

40.3.3 ip dhcp-server

To specify the IP address of the DHCP server, run ip dhcp-server.

ip dhcp-server *ip-address*

no ip dhcp-server *ip-address*

Parameter

Parameter	Description
ip-address	IP address of the DHCP server

Default

The **Default** IP address of the DHCP server does not exist.

Command Mode

Global configuration mode

Usage Description

The command can be used to specify the IP address of the DHCP server, while the previously-designated IP address of the DHCP server will not be replaced.

You can use the "no" form of the command to delete the previously-configured IP address of the DHCP server.

Example

The following **Example** shows how to set the server with IP 192.168.20.1 to the DHCP server.

ip dhcp-server 192.168.20.1

Related command

ip address dhcp

ip dhcp client

show dhcp lease

show dhcp server

40.3.4 show dhcp lease

To check the DHCP server distribution information used by the current router, run

show dhcp lease. Show dhcp lease

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

The command can be used to check the DHCP server distribution information used by the current router.

Example

The following **Example** shows the DHCP server distribution information used by the router.

```
router#show dhcp lease
Temp IP addr: 192.168.20.3      for peer on Interface: Ethernet1/1
Temp sub net mask: 255.255.255.0
DHCP Lease server: 192.168.1.3, state: 4 Rebinding
DHCP transaction id: 2049
Lease: 86400 secs,          Renewal: 43200 secs,     Rebind: 75600 secs
Temp Default-gateway addr: 192.168.1.2
Next timer fires after: 02:34:26
Retry count: 1       Client-ID: router-0030.80bb.e4c0-Et1/1
```

Related command

```
ip address dhcp
ip dhcp client
ip dhcp-server
show dhcp server
 debug dhcp
```

40.3.5 show dhcp server

To display the known DHCP server information, run show dhcp server. show dhcp server

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

The command is used to display the information about the known DHCP server.

Example

The following **Example** shows the information about the known DHCP server.

```
router#show dhcp sever
DHCP Server 255.255.255.255
Leases: 0
Discovers: 62 Requests: 0       Declines: 0  Releases: 0
Offers:       0      Acks:  0       Naks: 0       Bad:   0
Subnet: 0.0.0.0,    Domain name:
```

Related command

```
ip address dhcp
 ip dhcp client
ip dhcp-server
show dhcp lease
```

40.3.6 debug dhcp

To check the treatment condition of the DHCP protocol, run debug dhcp.

```
debug dhcp <detail>
no debug dhcp <detail>
```

Parameter

Parameter	Description
detail	Displays the content of the DHCP packet.

Default

Relative information will not be displayed by **Default**.

Command Mode

EXEC

Usage Description

The following **Example** shows some important information about DHCP treatment:

```
router#debug dhcp
router#2000-4-22 10:50:40 DHCP: Move to INIT state, xid: 0x7
2000-4-22 10:50:40 DHCP: SDISCOVER attempt # 1, sending 277 byte DHCP packet
2000-4-22 10:50:40 DHCP:      B'cast on Ethernet1/1 interface from 0.0.0.0
2000-4-22 10:50:40 DHCP: Move to SELECTING state, xid: 0x7
2000-4-22 10:50:46 DHCP: SDISCOVER attempt # 2, sending 277 byte DHCPpacket
2000-4-22 10:50:46 DHCP:      B'cast on Ethernet1/1 interface from 0.0.0.0
2000-4-22 10:50:54 DHCP: SDISCOVER attempt # 3, sending 277 byte DHCPpacket
```

Related command

```
show dhcp lease
```

40.4 DHCP Server Configuration Commands

DHCP server configuration commands include:

- ip dhcpd ping packet
- ip dhcpd ping timeout
- ip dhcpd write-time
- ip dhcpd database-agent
- ip dhcpd pool
- ip dhcpd enable
- ip dhcpd disable

40.4.1 ip dhcpd ping packet

ip dhcpd ping packet *pkgs*

Parameter

Parameter	Description
pkgs	A Parameter used by the DHCP server to check whether the address has distributed the number of the transmitted ICMP packets.

Default

2

Command Mode

Global configuration mode

Usage Description

You can run the following command to configure whether the DHCP server has transmitted n ICMP packets when it check whether the address is distributed.

ip dhcpd ping packets *n*

Example

You can run the following command to configure whether the DHCP server has transmitted n ICMP packets when it check whether the address is distributed.

ip dhcpd ping packets 1

40.4.2 ip dhcpd ping timeout

Parameter

Parameter	Description
timeout	Timeout time for waiting the ICMP echo message when the DHCP server is used to check whether the address is distributed

Default

5

Command Mode

Global configuration mode

Usage Description

You can run the following command to set the timeout time for waiting the ICMP echo packet to n*100ms when it check whether the address is distributed.

ip dhcpd ping timeout *n*

Example

You can run the following command to set the timeout time for waiting the ICMP echo packet to 300ms when it check whether the address is distributed.

ip dhcpd ping timeout 3

40.4.3 ip dhcpd write-time

Parameter

Parameter	Description
time	Interval for the DHCP server to save the address distribution information to the database (unit: minute)

Default

0

Command Mode

Global configuration mode

Usage Description

The following command can be used to set the DHCP server to write the address distribution information to the database every n minutes.

ip dhcpd write-time *n*

Example

The following **Example** shows that the DHCP server is set to write the address distribution information to the database every two days.

ip dhcpd write-time 1440

40.4.4 ip dhcpd database-agent

Parameter

Parameter	Description
Ip address	IP address of the address distribution information after the DHCP server is saved on PC

Default

None

Command Mode

Global configuration mode

Usage Description

You can run the following command to configure the address of PC where the address distribution information of the DHCP server is stored:

ip dhcpd database-agent X．X．X．X

If the address is not configured, the address distribution information will be stored in the flash.

Note: To store the address distribution information, you need start the TFTP server on PC and at the same time the PC and the DHCP server must correctly connect.

Example

ip dhcpd database-agent 192.168.1.1

40.4.5 ip dhcp snooping arp

Parameter

None

Default

None

Command Mode

Global configuration mode

Usage Description

To enable the ARP mapping protection mechanism, run ip dhcp snooping arp. After the command is configured, the DHCP server will create an ARP mapping between the MAC address of the DHCP server and the distributed IP address and protect the ARP mapping.

Example

ip dhcp snooping arp

40.4.6 ip dhcpd pool

Parameter

Parameter	Description
name	Name of the DHCP address pool

Default

None

Command Mode

Global configuration mode

Usage Description

You can run the following command to add the name DHCP address pool and enter the DHCP address pool configuration mode.

ip dhcpd pool *name*

Example

The following command in the **Example** is used to add a test DHCP address pool and enter the DHCP address pool configuration mode.

ip dhcpd pool test

40.4.7 ip dhcpd enable

Parameter

None

Default

The DHCP service is disabled by **Default**.

Command Mode

Global configuration mode

Usage Description

You can run the following command to enable the DHCP service. After the DHCP service is enabled, the DHCP server supports the relay operation; for those address requests that cannot be distributed by themselves, the DHCP requests will be forwarded on the port where the ip-helper-address is configured.

ip dhcpd pool *name*

Example

The following command is used to open the DHCP service.

ip dhcpd enable

40.5 DHCP Address Pool Configuration Commands

DHCP address pool configuration commands include the following:

- network
- range
- **Default**-router
- dns-server
- domain-name
- lease
- netbios-name-server
- ip-bind

40.5.1 network

network *ip-addr netmask*

Parameter

Parameter	Description
ip-addr	Network address of the address pool for automatic distribution
netmask	Subnet mask

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can use the command to configure the network address of the address pool for automatic distribution.

Before the command is configured, make sure that the network number of the IP address for a port on the interface receiving the DHCP packet must be same to the network.

Example

The following **Example** shows how to set the network address of the DHCP address pool to 192.168.20.0 and the subnet mask to 255.255.255.0.

network 192.168.20.0 255.255.255.0

40.5.2 range

range *low-addr high-addr*

Parameter

Parameter	Description
low-addr	Start address of the automatic address distribution range
hogh-addr	End address of the automatic address distribution range

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can use the command to configure the automatic address distribution range. You can configure up to eight ranges for each address pool, while each range must be in the network. The command is used only for the automatic distribution mode.

Example

The following **Example** shows how to configure the address distribution range of the DHCP address pool to 192.168.20.210~192.168.20.219.

```
range 192.168.20.210 192.168.20.219
```

40.5.3 Default-router

```
Default-router ip-addr
```

Parameter

Parameter	Description
ip-addr	Default route which is distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can run the command to configure the **Default** route which is distributed to the client; up to four **Default** routes can be configured which are separated through space.

Example

The following **Example** shows how to configure the **Default** route of the DHCP client to 192.168.20.1.

Default-router 192.168.20.1

40.5.4 dns-server

dns-server *ip-addr* …

Parameter

Parameter	Description
ip-addr	DNS server address distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can run the command to configure the address of the DNS server which is distributed to the client; up to four DNS servers can be configured which are separated through space.

Example

The following **Example** shows how to configure the address of the DNS server distributed to the client to 192.168.1.3.

dns-server 192.168.1.3

40.5.5 domain-name

domain-name *name*

Parameter

Parameter	Description
name	Domain name distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can run the command to configure the domain name which is distributed to the client.

Exampl

The following **Example** shows how to configure the domain name to test.domain.

domain-name test.domain

40.5.6 lease

lease {days [*hours*][*minutes*] | infinite}

Parameter

Parameter	Description
days	Days distributed by the address
hours	Hours distributed by the address
minutes	Minutes distributed by the address
infinite	Means that the addresses will be distributed permanently.

Default

one day

Command Mode

DHCP address pool configuration mode

Usage Description

You can run the command to configure the time limitation of the address which is distributed to the client.

Example

The following **Example** shows how to configure the time limitation of the address which is distributed to the client to 12 hours and two days.

Lease 2 12

40.5.7 netbios-name-server

netbios-name-server *ip-addr*

Parameter

Parameter	Description
ip-addr	Address of the netbios name server distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can run the command to configure the address of the netbios name server which is distributed to the client; up to four netbios name servers can be configured which are separated through space.

Example

The following **Example** shows how to configure the address of the DNS server distributed to the client to 192.168.1.10.

netbios-name-server 192.168.1.10

40.5.8 ip-bind

ip-bind *ip-addr* [hardware-address] [identifier] [host-name]

Parameter

Parameter	Description
ip-addr	Host address used for manual distribution
hardware-address	Binds the IP address to the hardware address. The hardware address is in the hex format: 00-12-3F-28-AE-35.
identifier	Binds the IP address to the identifier of the host which is in the hex format or in the format of the inverted command and character string.
host-name	Binds the IP address to the host name which is in the character string format.

Default

None

Command Mode

DHCP address pool configuration mode

Usage Description

You can use the command to configure the host's address of the address pool for automatic distribution.

Example

The following command is used to bind the manually-distributed address 192.168.20.200 to the hardware address 00-12-3F-28-AE-35.

Ip-bind 192.168.20.200 hardware-address 00-12-3F-28-AE-35

The following command is used to bind the manually-distributed address 192.168.20.200 to the host's name -315.

Ip-bind 192.168.20.200 host-name -315

ip-bind *ip-addr* hardware-address

ip-bind *ip-addr* hardware-address *hardware-address*{ type}

Parameter

Parameter	Description
hardware-address	Matches the hardware address of the client.
type	Means the type of the hardware address.

Default value

The **Default** value of the "type" **Parameter** is 1, standing for Ethernet.

Command Mode

DHCP address pool configuration mode

Instruction

This command can be used to configure the hardware address, which is used to match the hardware address. The format of the hardware address is like ab:cd:ef:gh. This command is used only in manual distribution mode.

Example

The following **Example** shows how to set the hardware address of the manual-DHCP-distribution address pool to 10:a0:0c:13:64:7d.

ip-bind *ip-addr* hardware-address 10:a0:0c:13:64:7d

40.5.9 ip-bind ip-addr client-identifier

ip-bind *ip-addr* client-identifier *unique-identifier*

Parameter

Parameter	Description
unique-identifier	Matches the ID of the client.

Default value

None

Command Mode

DHCP address pool configuration mode

Instruction

This command is used to configure the client ID which is used to match the client. The format of the client ID is like ab.cd.ef.gh. This command is used only in manual distribution mode.

Example

The following **Example** shows how to set the client ID of the manual-DHCP-distribution address pool to 10:a0:0c:13:64:7d.

ip-bind *ip-addr* client-identifier 01.10.a0.0c.13.64.7d

40.5.10 ip-bind ip-addr client-name

ip-bind *ip-addr* client-name *name*

Parameter

Parameter	Description
name	Means the name of the client.

Default value

None

Command Mode

DHCP address pool configuration mode

Instruction

This command is used to configure the host name which is distributed to the client. This command is used only in manual distribution mode.

Example

The following **Example** shows how to set the name of the client to test.

ip-bind *ip-addr* client-name test

40.6 DHCP Debugging Commands

DHCP debugging commands include:

- debug ip dhcpd packet
- debug ip dhcpd event

40.6.1 debug ip dhcpd packet

debug ip dhcpd packet

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

You can run the command to open the debugging switch of the DHCPD packet.

Example

The following command is used to enable the debugging switch of the DHCPD packet.

debug ip dhcpd packet

40.6.2 debug ip dhcpd event

debug ip dhcpd event

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

You can run the command to open the debugging switch of the DHCPD event.

Example

The following command is used to enable the debugging switch of the DHCPD event.

debug ip dhcpd event

DHCPD management commands DHCP management commands include:

show ip dhcpd statistic

- show ip dhcpd binding
- clear ip dhcpd statistic
- clear ip dhcpd binding

40.6.3 show ip dhcpd statistic

Parameter

None

Default

None

Command Mode

All modes except the user mode

Usage Description

You can run the command to display the DHCPD statistics information, including the number of all types of packets and the number of automatically- or manually-distributed addresses.

Example

The following command is used to display the DHCPD statistics information. Show ip dhcpd statistic

40.6.4 show ip dhcpd binding

show ip dhcpd binding {*ip-addr*}

Parameter

Parameter	Description
ip-addr	Address whose binding information requires to be displayed

Default

The binding information of all addresses is displayed.

Command Mode

All modes except the user mode

Usage Description

You can run the following command to display the binding information, IP address, hardware address, binding type and timeout time about the DHCPD.

Example

The following command is used to display the DHCPD binding information.

Show ip dhcpd binding

40.6.5 show ip dhcpd pool

Parameter

None

Default

None

Command Mode

All modes except the user mode

Usage Description

You can run the command to display the information about the DHCPD address pool, including the network number of the address pool,

address range, number of the distributed addresses, number of the temporarily-deserted addresses, number of the addresses that can be distributed, manually-distributed IP address and hardware address.

Example

The following command is used to display the statistics information about the DHCPD address pool.

show ip dhcpd pool

40.6.6 clear ip dhcpd statistic

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

You can run the command to delete the statistics information about the number of the packets.

Example

The following command is used to delete the statistics information about the number of the packets.

Clear ip dhcpd statistic

40.6.7 lear ip dhcpd binding

clear ip dhcpd binding {*ip-addr*|*}

Parameter

Parameter	Description
ip-addr	Address whose binding information requires to be deleted
*	Deletes all binding information.

Default

The designated address binding information is deleted.

Command Mode

EXEC

Usage Description

You can run the command to delete the binding information about the designated address.

Example

The following command is used to delete the binding information about address 192.168.20.210.

clear ip dhcpd binding 192.168.20.210

The following command is used to delete the binding information about address 192.168.20.210 and address 192.168.20.211.

clear ip dhcpd binding 192.168.20.210 192168.20.211

The following command is used to delete all binding information.

clear ip dhcpd binding *

40.6.8 clear ip dhcpd abandoned

Parameter

None

Default

None

Command Mode

EXEC

Usage Description

You can run the command to delete the abandon identifier.

Example

The following **Example** shows how to delete the abandon identifier.

Clear ip dhcpd abandoned

40.7 IP Server Configuration Commands

IP server configuration commands include:

- clear tcp
- clear tcp statistics
- debug arp
- debug ip icmp
- debug ip packet
- debug ip raw
- debug ip rtp
- debug ip tcp packet
- debug ip tcp transactions
- debug ip udp
- ip mask-reply

- ip mtu
- ip redirects
- ip route-cache
- ip source-route
- ip tcp synwait-time
- ip tcp window-size
- ip unreachables
- show ip cache
- show ip irdp
- show ip sockets
- show ip traffic
- show tcp
- show tcp brief
- show tcp statistics
- show tcp tcb

40.7.1 clear tcp

To delete a TCP connection, run the following command:

clear tcp {*local host-name port* remote *host-name port* | tcb *address*}

Parameter

Parameter	Description
local host-name port	IP address and TCP port of the local host
remote host-name port	IP address and TCP port of the remote host
tcb address	Address of the transmission control block (TCB) for the to-be-deleted TCP connection TCB is an internal identifier of the TCP connection, which can be obtained through the show tcp brief command.

Command Mode

EXEC

Usage Description

The clear tcp command is mainly used to delete the terminated TCP connection. Sometimes, because of communication line faults, TCP connection or the peer host is restarted and the TCP connection is actually closed. The TCP connection has no communication, so the system does not know that the TCP connection is already closed. In this case, the clear tcp command is used to close the invalid TCP connection. The clear tcp local *host-name port* remote *host-name port* command is used to close the TCP connection between the IP address or port of the local host and the IP address or port of the remote host. The clear tcp tcb address command is used to close the TCP connection identified by the designated TCB address.

Example

The following **Example** shows that the TCP connection between 192.168.20.22:23 (local) and 192.168.20.120:4420 (remote). The show tcp brief command is used to display the information of the local and remote hosts of the current TCP connection.

```
Router#show tcp brief

TCB             Local Address               Foreign Address     State
0xE85AC8            192.168.20.22:23            192.168.20.120:4420     ESTABLISHED

0xEA38C8   192.168.20.22:23  192.168.20.125:1583     ESTABLISHED
Router#clear tcp local 192.168.20.22 23 remote 192.168.20.120 4420 Router#show tcp brief

TCB   Local Address      Foreign Address             State
0xEA38C8   192.168.20.22:23  192.168.20.125:1583         ESTABLISHED
```

The following **Example** shows how to clear the TCP connection whose TCB address is 0xea38c8. The show tcp brief command displays the TCB address of the TCP connection.

```
Router#show tcp brief
TCB   Local Address      Foreign Address   State
0xEA38C8   192.168.20.22:23  192.168.20.125:1583     ESTABLISHED
Router#clear tcp tcb 0xea38c8 Router#show tcp brief
TCB   Local Address      Foreign Address   State
```

Related command

```
show tcp
show tcp brief
show tcp tcb
```

40.7.2 clear tcp statistics

To clear the statistics data about TCP, run the following command:

clear tcp statistics

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

The following **Example** shows how to delete the TCP statistics information:

```
Router#clear tcp statistics
```

Related command

show tcp statistics

40.7.3 debug arp

To display the ARP interaction information, such as ARP request transmitting, ARP response receiving, ARP request receiving and ARP response transmitting, run debug arp. When the router and host cannot communicate with each other, you can run the command to analyze the ARP interaction information. You can run no debug arp to stop displaying the ARP interaction information.

```
debug arp
no debug arp
```

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

```
Router#debug arp
Router#IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, Ethernet1/0
 IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:
00:00:00:00:00, wrong cable, Ethernet1/1
IP ARP: created an incomplete entry for IP address 192.168.20.77, Ethernet1/0
IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, Ethernet1/0
 IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, Ethernet1/0
```

The first information line shows that the router receives an ARP request from Ethernet 1/0. The ARP is sent from a host whose IP address is 192.168.20.116 and MAC address is 00:90:27:a7:a9:c2 and received by a host whose IP address is 192.168.20.111. The ARP request requires the MAC address of the destination host.

IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, Ethernet1/0

The second information line shows that the router receives an ARP address request with IP 192.168.20.139 from interface Etherner 1/1. However, according to the interface configuration of the router, the interface is not in the network claimed by the host. The reason may lie in the incorrect host configuration. If the router creates an ARP cache according to the information, it cannot communicate with a host having the same address though the host connects an interface normally.

IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:
00:00:00:00:00, wrong cable, Ethernet1/1

The third line shows that, before the router resolves the MAC address of host 192.168.20.77, an incomplete ARP item must be created in the ARP cache for the host; after the ARP response is received, the MAC address is entered. According to the configuration of the router, the host connects interface Ethernet1/0.

IP ARP: created an incomplete entry for IP address 192.168.20.77, Ethernet1/0

The fourth information shows that the router transmits the ARP request from interface Ethernet 1/0, the IP address of the router is 192.168.20.22, the MAC address of the interface is 08:00:3e:33:33:8a and the IP address of the requested host is 192.168.20.77. The four information line has connection with the third information line.

IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, Ethernet1/0

The fifth information line shows the router receives the ARP response which is transferred from host 192.168.20.77 to the router's interface

192.168.20.22 on interface Ethernet 1/0, telling that the MAC address is 00:30:80:d5:37:e0. The fifth information line has connection with the third and fourth information lines.

IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, Ethernet1/0

40.7.4 debug ip icmp

To display the interaction information of ICMP, run debug ip icmp. To close the debugging output, run no debug ip icmp.

```
debug ip icmp
no debug ip icmp
```

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Usage Description

The command is used to display the received and transmitted ICMP packets, helping to resolve the end-to-end connection problem. To understand the detailed meaning of the debug ip icmp command, see RFC 792, "Internal Control Message Protocol".

Example

```
Router#debug ip icmp
Router#ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48
ICMP: rcvd echo from 192.168.20.125, len 40
ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40
ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36 ICMP: sent dst (192.168.20.22) protocol unreachable to 192.168.20.124, len 36
ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36
ICMP: rcvd dst (22.0.0.3) host unreachable from 192.168.20.26, len 36
ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36
ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36

The first information line is explained as follows:
ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48
```

Domain	Description
ICMP:	Displays the information about ICMP.
Sent	Transmits the ICMP packets.
pointer indicating	Type of the ICMP packet, which shows the original IP packet is incorrect and specifies the incorrect domain Other types of ICMP packet include: echo reply dst unreachable，including: ---net unreachable ---host unreachable ---protocol unreachable ---port unreachable ---fragmentation needed and DF set ---source route failed ---net unknown ---destination host unknown ---source host isolated ---net prohibited ---host prohibited ---net tos unreachable ---host tos unreachable source quench redirect, including: ---net redirect ---host redirect ---net tos redirect ---host tos redirect echo router advertisement router solicitation time exceeded，including： ---ttl exceeded ---reassembly timeout Parameter problem, including: ---pointer indicating ---option missed ---bad length timestamp timestamp reply information request information reply mask request mask reply If it is the unknown ICMP type, the system will display the ICMP type and its code.

Domain	Description
to 192.168.20.124	The destination address of the ICMP packet is 192.168.20.124, which is also the source address of the original packet triggering the ICMP packet.
(dst was 192.168.20.22)	The destination address of the original packet leading to the ICMP packet is 192.168.20.22.
len 48	The length of the ICMP packet is 48 bytes, the length of IP header excluded.

The second information line is explained as follows:

ICMP: rcvd echo from 192.168.20.125, len 40

Domain	Description
rcvd	Receives the ICMP packet.
echo	Request response packet
from 192.168.20.125	The source address of the ICMP packet is 192.168.20.125.

The third information line is explained as follows:

ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40

Domain	Command
src 192.168.20.22	Means the source address of the ICMP packet is 192.168.20.22.
dst 192.168.20.125	Means the destination address of the ICMP packet is 192.168.20.125.

Different types of ICMP packets have different formats when the ICMP packet is generated.

For **Example**, the ICMP redirect packet adopts the following format:

ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36 ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36

The first information line shows that the redirect ICMP packet from host 192.168.20.77 is received and gateway 192.168.20.26 is recommended to forward the packet to destination host 22.0.0.3; the length of the ICMP packet is 36 bytes.

The second information line shows the redirect ICMP packet is sent to host 192.168.20.124. The redirect ICMP packet notifies the host of using gateway 192.168.20.77 to send packets to host 22.0.0.5. The length of the ICMP packet is 36 bytes.

For the DST unreachable ICMP packet, the following format is adopted for printing:

ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len36

ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len36

The first information line shows that, because the router cannot route a certain IP packet, the destination-unreachable ICMP packet will be sent to source host 192.168.20.124. The length of the ICMP packet is 36 bytes.

The second information line shows that the router receives an ICMP packet from host 192.168.20.26, notifying that the destination host 2.2.2.2 cannot be reached. The length of the ICMP packet is 36 bytes.

40.7.5 debug ip packet

To display the IP interaction information, run debug ip packet. You can run no debug ip packet to stop displaying the IP interaction information.

debug ip packet [detail] [*ip-access-list-name*]
no debug ip packet

Parameter

Parameter	Description
detail	(optional) exports the protocol information encapsulated in the IP packet, including protocol number, UDP, number of the TCP port and type of the ICMP packet.
ip-access-list-name	(optional) name of the IP access list for filtering and exporting information Only the information about the IP packet which meets the requirement of the designated IP access list can be exported.
access-group	(optional) name of the IP access list for filtering and exporting information Only the information about the IP packet which meets the requirement of the designated IP access list can be exported.
interface	(optional) name of the port for filtering and exporting information Only the information about the IP packet which meets the requirement of the designated port can be exported.

Command Mode

EXEC

Usage Description

The command helps you to know the final direction of each received or locally-generated IP packet flow and detect the reason of communication problems.

The following are potential reasons:

- Forwarded
- Forwarded as the broadcast or multicast packet
- Failed addressing when the IP packet is forwarded
- Forwarding the redirect packet
- Rejected because of having the source route option
- Rejected because of illegal IP options
- Source route
- Locally-transmitted packets need fragmentation, while the DF bit is reset.

- Receiving the packets
- Receiving IP fragments
- Transmitting packets
- Transmitting the broadcast/multicast
- Failed addressing of locally-generated packets
- Locally-generated packets being fragmented
- Received packets being filtered
- Transmitted packets being filtered
- Encapsulation of the link layer failed (only for Ethernet)
- Unknown protocol

If you use the command, lots of output information will appear; you had better run the router at a relatively free time, or the system's performance may be badly affected. Additionally, you had better filter the information output through the access list, enabling the system to display the information that interests users.

Command Mode

EXEC

Example

```
router#debug ip packet
router#IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, redirected
IP: s=192.168.20.22 (local), d=192.168.20.120 (Ethernet1/0), g=192.168.20.120, len=56,
sending
IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, forward IP: s=192.168.20.81 (Ethernet1/0),
d=192.168.20.22 (Ethernet1/0), len=56, rcvd
```

Domain	Description
IP	Means that the information is about the IP packet.
s=192.168.20.120 (Ethernet1/0)	Source address of the IP packet and the name of the interface receiving the packet
d=19.0.0.9 (Ethernet1/0)	Destination address of the IP packet and the name of the interface transmitting the packet (if the routing succeeds)
g=192.168.20.1	Destination address of the next hop of the IP packet, which may be the gateway address or the destination address
len	Length of the IP packet

Domain	Description
redirected	Means the router will send the ICMP redirected packet to the source host of the ICMP packet. The following are other cases: Forward—the packet is forwarded. forward directed broadcast---Packets are forwarded as the directed broadcast and packets will be transformed as the physical broadcast on the transmission interface unroutable---The addressing of the packet fails and and the packet will be dropped. source route---Source route rejected source route---Because the system does not support the source route, the packets with the IP source route are rejected. Bad options—the IP option is incorrect and the packet will be dropped. need frag but DF set---The local packet need be fragmented; however, the DF is reset. rcvd---the packet is received by the local host. rcvd fragment---The fragment of the packet is received. sending---The locally-generated packet is being sent. sending broad/multicast---The locally-generated broadcast/multicast packet is being sent. sending fragment---The locally-fragmented IP packet is being sent. denied by in acl---The packet is denied by the ACL of the receiver interface. denied by out acl---The packet is denied by the transmitter interface. unknown protocol---unknown protocol encapsulation failed---the protocol encapsulation fails in the Ethernet. When the to-be-transmitted packet is dropped on the Ethernet interface becase of ARP resolution failure, the information appears.

The first information line shows that the router has received an IP packet; its source address is 192.168.20.120 and destination address is 19.0.0.9; it is from the network segment connected by interface Ethernet 1/0; the transmitter interface determined by the routing table is interface Ethernet1/0; the gateway's address is 192.168.20.1 and the length of the packet is 60 bytes. The gateway and the source host which transmits the IP packet are connected on the same network, that is, the network connected by interface Ethernet 1/0 of the router. Hence, the router transmits the ICMP redirect packet.

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60,

redirected

The second information line describes the transmission of the ICMP redirect packet. The source address is the local address 192.168.20.22 and the destination address is the source addresss of the previous packet, that is, 192.168.20.120. The ICMP redirect packet is transmitted

from interface Ethernet1/0 to the destination directly, so the address of the gateway is the destination address 192.168.20.120. The length of the ICMP redirect packet is 56 bytes.

IP: s=192.168.20.22 (local), d=192.168.20.120 (Ethernet1/0), g=192.168.20.120, len=56,

sending

The third information line shows that the IP layer receives an IP packet. The source address of the packet is 192.168.20.120; the transmitter interface is interface Ethernet1/0; the destination address of the packet is 19.0.0.9. Through the routing table, the packet is found to forward to interface Ethernet1/0; the address of the gateway is 192.168.20.77 and the length of the packet is 60 bytes.

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.77, len=60, forward

The fourth information line shows that the IP layer receives an IP packet. The source address is 192.168.20.81 and the receiver interface is Ethernet1/0; the destination address is 192.168.20.22, which is an IP address configured on interface Ethernet1/0 of the router; the length of the packet is 56 bytes.

IP: s=192.168.20.81 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=56, rcvd

The output of the debug ip packet detail command is described in the following. Only newly-added parts are described.

router#debug ip packet detail

```
router#IP: s=192.168.12.8 (Ethernet1/0), d=255.255.255.255 (Ethernet1/0), len=328, rcvd, UDP: src=68, dst=67
IP: s=192.168.20.26 (Ethernet1/0), d=224.0.0.5 (Ethernet1/0), len=68, rcvd, proto=89
IP: s=192.168.20.125 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=84, rcvd, ICMP: type=0, code = 0
IP: s=192.168.20.22 (local), d=192.168.20.124 (Ethernet1/0), g=192.168.20.124, len=40,
sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK
```

Domain	Description
UDP	Protocol name, such as UDP, ICMP or TCP Other protocols are presented with the protocol number.
type, code	Type and code of the ICMP packet
src, dst	Source port and destination port of the UDP/TCP packet
seq	Sequence number of the TCP packet
ack	Acknowledge number of the TCP packet
win	Windows value of the TCP packet
ACK	ACK in the control bit of the TCP packet is reset, indicating that the acknowledge number is valid. Other control bits include SYN, URG, FIN, PSH and RST.

The first information line shows that the UDP packet is received. The source port is 68 and the destination port is 67.

IP: s=192.168.12.8 (Ethernet1/0), d=255.255.255.255 (Ethernet1/0), len=328, rcvd, UDP: src=68, dst=67

The second information line shows that the protocol number of the received packet is 89.

IP: s=192.168.20.26 (Ethernet1/0), d=224.0.0.5 (Ethernet1/0), len=68, rcvd, proto=89

The third information line shows that the ICMP packet is received. Both the packet type and the code are 0.

IP: s=192.168.20.125 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=84, rcvd, ICMP: type=0, code = 0

The fourth information line shows that the TCP packet is transmitted. The source port is 1024, the destination port is 23, the sequence number is 75098622, the acknowledge number is 161000466, the size of the receiver window is 17520 and the ACK bit is reset. For the meanings of these domains, see *RFC 793— TRANSMISSION CONTROL PROTOCOL*.

IP: s=192.168.20.22 (local), d=192.168.20.124 (Ethernet1/0), g=192.168.20.124, len=40,

sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK

The following describes how to use the ACL. For **Example**, to display the information about the packet whose source address is 192.168.20.125, you need to define the abc ACL and then allow the IP packets whose source address is 192.168.20.125. At last, you can use the ACL through the debug ip packet command.

```
Router#config
Router_config#ip access-list standard abc
 Router_config_std_nacl#permit 192.168.20.125
Router_config_std_nacl#exit
Router_config#exit
Router#debug ip packet abc
Router#IP: s=192.168.20.125 (Ethernet0/1), d=192.168.20.22 (Ethernet0/1), len=48, rcvd
```

In the previous commands, the standard ACL is used. However, the expanded ACL can also be used.

Related command

debug ip tcp packet

40.7.6 debug ip raw

To display the information about IP interaction, run debug ip raw [detail] [*access-list-group*] [*interface*]. To stop displaying information about IP interaction, run no debug ip raw.

```
debug ip raw [detail] [access-list-group] [interface]
no debug ip raw
```

Parameter

Parameter	Description
detail	(optional) exports the protocol information encapsulated by the IP packet, such as the protocol number, number of the UDP port and the TCP port, and type of the TCP packet.
access-group	(optional) name of the IP ACL which is used to filter the output information Only the information about the IP packets that comply with the designated IP ACL can be exported.
interface	(optional) interface name which is used to filter the output information Only the information about the IP packets that comply with the designated port can be exported.

Command Mode

EXEC

Usage Description

The command helps you to know the final destination of each received or locally-generated IP flows and to find the reason of the communication problem.

The following are potential cases:

- Forwarded
- Forwarded as the broadcast/multicast packet
- Addressing failed when the IP packet is forwarded
- Forwarding the redirect packet
- Rejected because of having the source route option
- Rejected because of illegal IP options
- Source route
- Locally-transmitted packets need fragmentation, while the DF bit is reset.
- Receiving the packets.
- Receiving IP fragments
- Transmitting the packet
- Transmitting the broadcast/multicast
- Failed addressing of locally-generated packets
- Locally-generated packets being fragmented
- Received packets being filtered
- Transmitted packets being filtered
- Encapsulation of the link layer failed (only for Ethernet)
- Unknown protocol

If you use the command, lots of output information will appear; you had better run the router at a relatively free time, or the system's performance may be badly affected. Additionally, you had better filter the information output through the access list, enabling the system to display the information that interests users.

Example

The **Example** is the same to that of the debug ip packet command.

Related command

debug ip tcp packet

40.7.7 debug ip rtp

To display the information about the header compression, run debug ip rtp {header-compression|packets|rtcp}.You can run no debug ip rtp {header-compression|packets |rtcp} to stop displaying the information about the header compression.

```
debug ip rtp {header-compression|packets |rtcp}

no debug ip rtp {header-compression|packets |rtcp}
```

Parameter

Parameter	Description
header-compress	RTP/UDP/IP header compression
packets	Packets about data interaction of the RTP/UDP/IP header compression
rtcp	Packets about data interaction of the TCP/IP header compression

Command Mode

EXEC

Usage Description

The command helps you to understand the whole process of header compression and interaction.

If you use the command, lots of output information will appear; you had better run the router at a relatively free time, or the system's performance may be badly affected.

Example

```
router # debug ip rtp header-compress
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: new connection, conn 0,
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7078, Gen =0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7079, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7080, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7081, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7082, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7083, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7084, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7085, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7086, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4024, Gen =0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7087, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4025, Gen = 0
```

2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4026, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7088, Gen =0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7089, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4027, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7090, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4028, Gen =0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7091, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4029, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7092, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4030, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7093, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7094, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4032, Gen =0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7095, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4033, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7096, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4034, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7097, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7098, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4036, Gen =0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7099, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4037, Gen = 0

```
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7100, Gen =0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4038, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7101, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: tossing error packet 2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7102, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4040, Gen =0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7103, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4041, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7104, Gen = 0
 2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4042, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7105, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7106, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4044, Gen =0
 2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7107, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4045, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7108, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4046, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7109, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7110, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4048, Gen = 0 no deb all
```

40.7.8 debug ip tcp packet

To display the information about receiving and transmitting the TCP packet, run debug ip tcp packet. To stop displaying relative information, run no debug ip tcp packet.

debug ip tcp packet

no debug ip tcp packet

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

```
Router#debug ip tcp packet
Router#tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659460
        DATA 1 ACK 3130379810 PSH WIN 4380
tcp: I ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 3130379810
        DATA 2 ACK 50659460 PSH WIN 16372
tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659461
        DATA 50 ACK 3130379812 PSH WIN 4380
tcp: O FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 50659511
        ACK 3130379812 FIN WIN 4380
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
        ACK 50659511 WIN 16321
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
        ACK 50659512 WIN 16321
tcp: I FIN_WAIT_2 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
        ACK 50659512 FIN WIN 16321
tcp: O TIME_WAIT 192.168.20.22:23 192.168.20.125:3828 seq 50659512
        ACK 3130379813 WIN 4380
tcp: I LISTEN 0.0.0.0:23 0.0.0.0:0 seq 3813109318
       DATA 2 ACK 8057944 PSH WIN 17440
tcp: O LISTEN 0.0.0.0:23 0.0.0.0:0 seq 8057944
```

RST

Domain	Description
tcp:	Information about the TCP packets
O	Transmits the TCP packets.
ESTABLISHED	Current state of the TCP connectionFor the description of the TCP connection's state, see the description of the debug ip tcp transactions command.
192.168.20.22:23	The source address of the packet is 192.168.20.22 and the source port is 23.

Domain	Description
192.168.20.125:3828	The destination address of the packet is 192.168.20.125 and the destination port is 3828.
seq 50659460	The sequence number of the packet is 50659460.
DATA 1	Means that the packet contains only one effective byte.
ACK 3130379810	The acknowledgement number of the packet is 3130379810.
PSH	PSH is reset in the control bit of the packet. Other control bits include ACK, FIN, SYN, URG and RST.
WIN 4380	Window domain of the packet used to notify the peer end to receive the cache size, which is 4380 bytes currently
I	Receives the TCP packet.

If a domain of the previous domains does not appear, the domain has no effective value in the TCP packet.

Related command

debug ip tcp transactions

40.7.9 debug ip tcp transactions

To display the important interaction information about TCP, such as the state change of the TCP connection, run debug ip tcp transactions. To stop displaying relative information, run no debug ip tcp transactions.

```
debug ip tcp transactions

no debug ip tcp transactions
```

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

```
Router#debug ip tcp transactions
Router#TCP: rcvd connection attempt to port 23
TCP: TCB 0xE88AC8 created
TCP: state was LISTEN -> SYN_RCVD [23 -> 192.168.20.125:3828]
TCP: sending SYN, seq 50658312, ack 3130379657 [23 -> 192.168.20.125:3828]
TCP: state was SYN_RCVD -> ESTABLISHED [23 -> 192.168.20.125:3828]
TCP: connection closed by user, state was LISTEN [23 -> 0.0.0.0:0]
TCP: state was TIME_WAIT -> CLOSED [23 -> 192.168.20.125:3827]
TCP: TCB 0xE923C8 deleted
```

```
TCP: TCB 0xE7DBC8 created
TCP: connection to 192.168.20.124:513 from 192.168.20.22:1022, state was CLOSED to SYN_SENT
TCP: sending SYN, seq 52188680, ack 0 [1022 -> 192.168.20.124:513]
 TCP: state was SYN_SENT -> ESTABLISHED [1022 ->192.168.20.124:513]
TCP: rcvd FIN, state was ESTABLISHED -> CLOSE_WAIT [1022 -> 192.168.20.124:513]
TCP: connection closed by user, state was CLOSE_WAIT [1022 -> 192.168.20.124:513]
TCP: sending FIN [1022 -> 192.168.20.124:513]
TCP: connection closed by user, state was LAST_ACK [1022 -> 192.168.20.124:513]
TCP: state was LAST_ACK -> CLOSED [1022 -> 192.168.20.124:513]
TCP: TCB 0xE7DBC8 deleted
```

Domain	Description
TCP:	Displays the TCP interaction information.
rcvd connection attempt to port 23	Receives the connection request from the peer port 23, that is, the TELNET port.
TCB 0xE88AC8 created	Generates a new control block for the TCP connection, which is identified as 0xE88AC8.
state was LISTEN -> SYN_RCVD	Means that the TCP state machine changes from LISTEN to SYN_RCVD. The states of the TCP include: LISTEN—waiting for the TCP connection request from any remote host SYN_SENT—Sending out the connection request to trigger the TCP connection negotiation and then waiting for the peer's response SYN_RCVD—receiving the connection request from the peer, sending out the acknowledgement response and also sending out its connection request, and waiting for the connection request acknowledgement from the peer ESTABLISHED—means that the connection is created; the connection is in the data transmission phase; the data of the upper-layer application can be received and transmitted. FIN_WAIT_1—Means that the connection termination request has been transmitted and the response and connection termination request from the peer are being waited. FIN_WAIT_1—Means that the connection termination request has been transmitted and the response from the peer has been received, while the connection termination request from the peer is being waited. CLOSE_WAIT—Means the connection termination request of the peer is received and the local response has been sent out, and now the local user is being waited to close the connection. Once the user requires closing the connection, the system will send the connection termination request.

Domain	Description
state was LISTEN -> SYN_RCVD	CLOSING—Means the connection termination request has been sent to the peer and the peer's connection termination request is also received and the corresponding response is also sent out, and now is waiting for the peer to acknowledge the local connection termination request. LAST_ACK—Means that the connection termination request from the peer is received and acknowledged, and now the connection termination request is transmitted and the response is waited. TIME_WAIT—Means that a sufficient time is needed to ensure that the peer has already received the local acknowledgement of the peer's connection termination request and the connection packet still being transmitted in the network is waited to be sent to the destination or be dropped. CLOSED—Means that there is no connection or the connection has been completed shut down. For more detailed information, see *RFC 793, TRANSMISSION CONTROL PROTOCOL*.
[23 -> 192.168.20.125:3828]	The content in the bracket is explained as follows: The first domain (23) stands for the local TCP port. The second domain (192.168.20.125) stands for the remote IP address. The third domain (3828) stands for the remote TCP port.
sending SYN	Transmits a connection request out (the SYN of the control bit in the TCP header is reset). Other TCP control bits include SYN, ACK, FIN, PSH, RST and URG.
seq 50658312	The sequence number of the transmitted packet is 50658312.
ack 3130379657	The acknowledgement number of the transmitted packet is 3130379657.
rcvd FIN	Means that the connection termination request is received (FIN in the control bit of the TCP header is reset).
connection closed by user	Means that the upper-layer application requires closing the TCP connection.
Connection timed out	Means that the connection is closed because it times out.

Related command

debug ip tcp packet

40.7.10 debug ip udp

To display the information about UDP interaction, run debug ip udp. To stop displaying the information about UDP interaction, run no debug ip udp.

```
debug ip udp
no debug ip udp
```

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

```
Router#debug ip udp
Router#UDP: rcvd src 192.168.20.99(520), dst 192.168.20.255(520), len = 32
UDP: sent src 192.168.20.22(20001), dst 192.168.20.43(1001), len = 1008
```

Domain	Description
UDP:	Means that the information is about the UDP packet.
rcvd	Means that the packet is received.
sent	Means that the packet is transmitted.
src	Stands for the source IP address and UDP port of the UDP packet.
dst	Stands for the destination IP address and UDP port of the UDP packet.
len	Stands for the length of the message.

The first information shows that the UDP packet is received. Its source address is 192.168.20.99 and its source port is port 520; its destination address is 192.168.20.255 and its destination port is port 520; the length of the packet is 32 bytes.

The second information shows that the UDP packet is transmitted. Its source address is 192.168.20.22 and its source port is port 20001; its destination address is 192.168.20.43 and its destination port is port 1001; the length of the packet is 1008 bytes.

40.7.11 ip mask-reply

To enable the router to answer the request of the IP mask on the designated interface, run ip mask-reply. To disable this function, run no ip mask-reply.

```
ip mask-reply
no ip mask-reply
Default ip mask-reply
```

Parameter

The command has no **Parameter**s or keywords.

Default

The IP mask request is not answered.

Command Mode

Interface configuration mode

Example

```
interface ethernet 1/1 ip mask-reply
```

40.7.12 ip mtu

To set the MTU of the IP packet transmitted from an interface, run ip mtu *bytes*. To reuse the **Default** value of MTU, run no ip mtu.

```
ip mtu bytes
no ip mtu
```

Parameter

Parameter	Description
bytes	Maximum IP transmission length which is counted with bytes

Default

The physical media of the interfaces are different, while the MTU on the interfaces are same. Sixty-eight bytes is the minimum MTU.

Command Mode

Interface configuration mode

Usage Description

If the length of the IP packet exceeds the IP MTU configured on the interface, the router will fragment the packet. Devices on the same physical media can communicate with each other only when they are configured with the same MTU. The MTU value will affect the value of the IP MTU. If the value of IP MTU and that of MTU are same, the value of IP MTU will automatically change to the new value of MTU when the MTU value changes. However, the value of MTU will not change if the value of IP MTU changes.

The minimum value of the IP MTU is 68 bytes, and its maximum value cannot exceed the MTU value configured on the interface.

Example

The following **Example** shows how to set the IP MTU of the interface to 200:

```
interface serial0/0
ip mtu 200
```

Related command

mtu

40.7.13 ip redirects

To transmit the IP ICMP, redirect packet, run ip redirects. To stop transmitting the IP ICMP redirect packet, run no ip redirects.

```
ip redirects
no ip redirects
```

Parameter

The command has no **Parameter**s or keywords.

Default

In general, the IP redirect packet is transmitted by **Default**. However, the function that the IP redirect packet can be transmitted will be automatically disabled if the hot-standby router protocol is configured on the interface. If the configuration of the hot-standby router protocol is cancelled later, the function cannot be automatically enabled.

Command Mode

Interface configuration mode

Usage Description

When the router detects that the forwarding interface of the gateway is the same as that of the received packet during the transmission of packets and if the packet-transmitting host directly connects the logic network of the interface, the router can transmit an ICMP redirect packet according to the protocol, notifying the source host of directly taking that router as the gateway for the destination address of the packet without packet forwarding through this router.

If the hot-standby router protocol is configured on an interface, the transmission of IP redirect packet may cause the loss of the packet.

Example

The following **Example** shows how to enable the function of transmitting the ICMP redirect passage on interface ethernet1/0:

```
interface ethernet 1/0
 ip redirects
```

40.7.14 ip route-cache

To enable the route cache on an interface to forward the IP packet, run ip route-cache. To forbid the route cache on an interface, run no ip route-cache.

```
ip route-cache
no ip route-cache
ip route-cache same-interface
no ip route-cache same-interface
```

Parameter	Description
same-interface	Allows the IP packet to be rapidly forwarded from the received interface.

Default

Fast switching is allowed on an interface, while fast switching is forbidden on the same interface.

Command Mode

Interface configuration mode

Usage Description

The route cache can conduct the load balance to the forwarded packets based on the source/destination address.

If the route cache is enabled, the packet forwarding rate of the router will be improved. However, the route cache should be forbidden on the low-speed line (64k or even less than 64k).

You can run ip route-cache same-interface to allow rapid IP switching on the same interface, that is, the receiver interface is same to the transmitter interface. In general, the function is not recommended to be enabled because the function conflicts with the redirect function of the router. If you have an incompletely-connected network, such as a frame-relay network, you can enable the function on the frame-relay interface. For **Example**, in a frame-relay network consisting of routers A, B and C, there are only links from A to B and from B to C, the communication between router A and router C must be forwarded through router B. In this case, router B receives a packet from router A through a DLCI of an interface, and then transmits the packet to router C through another DLCI of the same interface.

Example

The following command is used to allow fast switching on the same interface.

ip route-cache same-interface

The following command is used to forbid fast switching even on the same interface.

no ip route-cache

The following command is used to forbid fast switching only on the same interface.

no ip route-cache same-interface

The following command is used to enable the **Default** setting (allowing fast switching, the same interface excluded).

ip route-cache

Related command

show ip cache

40.7.15 ip source-route

To enable the router to handle the IP packet with the source IP route option, run ip source-route. To enable the router to drop the IP packet with the source IP route option, run no ip source-route.

ip source-route

no ip source-route

Parameter

The command has no **Parameter**s or keywords.

Default

The IP packet with the source IP route option is handled.

Command Mode

Global configuration mode

Example

The following **Example** shows how to enable the router to handle the IP packet with the source IP route option.

ip source-route

Related command

ping

40.7.16 ip tcp synwait-time

To set the timeout time for the router to wait for the successful TCP connection, run ip tcp synwait-time *seconds*. To resume the **Default** timeout time, run no ip tcp synwait-time.

```
ip tcp synwait-time seconds
no ip tcp synwait-time
```

Parameter

Parameter	Description
seconds	Time for the TCP connection, whose unit is second the valid vale ranges between 5 and 300 seconds. The Default value is 75.

Default

75 seconds

Command Mode

Global configuration mode

Usage Description

When the router triggers the TCP connection and if the TCP connection is not established in the designated wait time, the router views that the connection fails and then sends the result to the upper-layer program. You can set the wait time for creation of the TCP connection. The **Default** value of the wait time is 75 seconds. The option has no relation with the TCP connection packet which is forwarded through the router, but has relation with the TCP connection of the router itself.

To know the current value, you can run ip tcp synwait-time?. The value in the square bracket is the current value.

Example

The following **Example** shows how to set the wait time of creating TCP connection to 30 seconds:

```
Router_config#ip tcp synwait-time 30
 Router_config#ip tcp synwait-time ?
<5-300>[30] seconds     -- wait time
```

40.7.17 ip tcp window-size

To set the size of the TCP window, run ip tcp window-size *bytes*. To resume the **Default** size of the TCP window, run no ip tcp window-size.

ip tcp window-size *bytes*

no ip tcp window-size

Parameter

Parameter	Description
bytes	Size of the windowThe maximum window size is 65535 bytes. The Default window size is 2000 bytes.

Default

2000 bytes

Command Mode

Global configuration mode

Usage Description

Do not change the window size at will unless you have a definite purpose. To know the current value, you can run ip tcp synwait-time ?. The value in the square bracket is the current value.

Example

The following **Example** shows how to set the size of the TCP window to 6000 bytes.

Router_config#ip tcp window-size 6000 Router_config#ip tcp window-size ?

<1-65535>[6000] bytes -- Window size

40.7.18 ip unreachables

To enable the router to transmit the ICMP unreachable packet, run ip unreachable. To enable the router to stop transmitting this packet, run no ip unreachable.

ip unreachable

no ip unreachable

Parameter

The command has no **Parameter**s or keywords.

Default

The ICMP unreachable packet is transmitted.

Command Mode

Interface configuration mode

Usage Description

When the router forwards the IP packet, the packet may be dropped because there is no relative route in the routing table. In this case, the router can send the ICMP unreachable packet to the source host, notifying the source host and enabling it to detect the host timely and correct the fault rapidly.

Example

The following **Example** shows how to enable the ICMP unreachable packet to be transmitted on interface Ethernet 1/0:

```
interface ethernet 1/0
 ip unreachables
```

40.7.19 show ip cache

To display the route cache which is used for fast IP switching, run show ip cache [*prefix mask*] [*type number*].

```
show ip cache [prefix mask] [type number]
```

Parameter

Parameter	Description
prefix mask	Displays the items whose destination addresses match up the designated prefixes/masks users enter. It is optional.
type number	Displays the items whose transmitter interfaces match up the designated interface types/numbers users enter. It is optional.
rsvp	Displays RSVP-relative items. It is optional.

Command Mode

EXEC

Example

The following **Example** shows that the route cache is displayed:

```
 Router#show ip cache

Source                  Destination             Interface       Next Hop
192.168.20.125  2.0.0.124               Serial1/0       2.0.0.124
192.168.20.124  192.168.30.124          Serial1/0       2.0.0.124
2.0.0.124       192.168.20.125          Ethernet1/1     192.168.20.125
```

Domain	Description
Source	Source address
Destination	Destination address
Interface	Type and number of the transmitted interface
Next Hop	Gateway's address

The following **Example** shows the route cache whose destination address matches up the designated prefix/mask.

```
Router#show ip cache 192.168.20.0 255.255.255.0
Source      Destination Interface     Next Hop
2.0.0.124   192.168.20.125 Ethernet0/1   192.168.20.125
```

The following **Example** shows the route cache whose transmitter interface matches up the designated interface type/mask.

```
Router#show ip cache s1/0
```

Source	Destination	Interface	Next Hop
192.168.20.125	2.0.0.124	Serial1/0	2.0.0.124
192.168.20.124	192.168.30.124	Serial1/0	2.0.0.124

40.7.20 show ip irdp

To display the irdp protocol information, run show ip irdp.

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

xuhao_config_e1/0# show ip irdp

Async0/0 ICMP router discovery protocol(IRDP):OFF

Ethernet1/0 ICMP router discovery protocol (IRDP): ON Advertisements occur between every 450 and 600 seconds

Advertisements are sent as broadcasts Advertisements valid in 1800 seconds **Default** preference: 0

Ethernet1/1 ICMP router discovery protocol (IRDP): OFF

Null0 ICMP router discovery protocol (IRDP): OFF

Loopback7 ICMP router discovery protocol (IRDP): OFF

Loopback10 ICMP router discovery protocol (IRDP): OFF

40.7.21 show ip sockets

To display the socket information, run show ip sockets.

show ip sockets

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

Router#show ip sockets

Proto	Local	Port	Remote	Port	In	Out
17	0.0.0.0	0	0.0.0.0	0	161	0
6	0.0.0.0	0	0.0.0.0	0	513	0
17	0.0.0.0	0	0.0.0.0	0	1698	0
17	0.0.0.0	0	0.0.0.0	0	69	0
6	0.0.0.0	0	0.0.0.0	0	23	0
17	0.0.0.0	0	0.0.0.0	0	137	122590

Domain	Description
Proto	Number of the IP protocol If the value is 17, it means the UDP protocol; if the value is 6, it means the TCP protocol.
Remote	Remote address
Port	Remote port
Local	Local address
Port	Local port
In	Total number of the received bytes
Out	Total number of the transmitted bytes

40.7.22 show ip traffic

To display the flow statistics information, run the following command:

show ip traffic

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

```
Router#show ip traffic
IP statistics:
Rcvd: 0 total, 0 local destination, 0 delivered
        0 format errors, 0 checksum errors, 0 bad ttl count
        0 bad destination address, 0 unknown protocol, 0 discarded
        0 filtered , 0 bad options, 0 with options

Opts: 0 loose source route, 0 record route, 0 strict source route
        0 timestamp, 0 router alert, 0 others

Frags: 0 fragments, 0 reassembled, 0 dropped
        0 fragmented, 0 fragments, 0 couldn't fragment
Bcast: 0 received, 0 sent
Mcast: 0 received, 0 sent
Sent: 230 generated, 0 forwarded
        0 filtered, 0 no route, 0 discarded
```

```
ICMP statistics:
Rcvd: 0 total, 0 format errors, 0 checksum errors
0 redirect, 0 unreachable, 0 source quench
0 echos, 0 echo replies, 0 mask requests, 0 mask replies
0 Parameter problem, 0 timestamps, 0 timestampreplies
0 time exceeded, 0 router solicitations, 0 routeradvertisements
Sent: 0 total, 0 errors
0 redirects, 0 unreachable, 0 source quench
0 echos, 0 echo replies, 0 mask requests, 0 mask replies
0 Parameter problem, 0 timestamps, 0 timestamp replies
0 time exceeded, 0 router solicitations, 0 router advertisements

UDP statistics:
Rcvd: 28 total, 0 checksum errors, 22 no port, 0 full sock
Sent: 0 total

TCP statistics:
Rcvd: 0 total, 0 checksum errors, 0 no port
Sent: 3 total

IGMP statistics:
Rcvd: 0 total, 0 format errors, 0 checksum errors
0 host queries, 0 host reports Sent: 0 host reports

ARP statistics:
Rcvd: 8 total, 7 requests, 1 replies, 0 reverse, 0 other
Sent: 5 total, 5 requests, 0 replies (0 proxy), 0 reverse
```

Domain	Description
format errors	Error of the packet's format, such as incorrect IP header length
bad hop count	If the router finds that the TTL value of the packet decreases to zero when it forwards the packet, the packet will be dropped.
no route	Means that the router has no corresponding route.

40.7.23 show tcp

To display the states of all TCP connections, run the following command:

show tcp

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

```
Router#show tcp

TCB 0xE9ADC8
Connection state is ESTABLISHED, unread input bytes: 934
Local host: 192.168.20.22, Local port: 1023
Foreign host: 192.168.20.124, Foreign port: 513

Enqueued bytes for transmit: 0, input: 934         mis-ordered: 0 (0 packets)

Timer Starts Wakeups    Next(ms)
Retrans      33    1      0
TimeWait     0     0      0
SendWnd      0     0      0
KeepAlive    102   0      7199500

iss:      29139463      snduna:      29139525    sndnxt:      29139525    sndwnd:     17520
irs: 709124039 rcvnxt:709205436  rcvwnd:       4380


SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):
Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396
Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61
```

Domain	Description
TCB 0xE77FC8	Internal identifier of the control block for the TCP connection
Connection state is ESTABLISHED	Current state of the TCP connection The TCP connection may be in one of the following states: LISTEN---Means the TCP connection request from any remote host is being waited. SYN_SENT---Means that the response from the peer is being waited after the connection request is transmitted to the peer. SYN_RCVD---Means that the connection request acknowledgement from the peer is being waited after the local machine receives the peer's connection request, transmits its acknowledgement and also its own connection request. ESTABLISHED---Means that the connection has been established and is now in the data transmission phase in which the upper-layer application can be received or

	transmitted.
Domain	**Description**
Connection state is ESTABLISHED	FIN_WAIT_1---Means that the peer's acknowledgement and connection termination request is being waited after the local machine transmits the connection termination request to the peer. FIN_WAIT_2---Means that the peer's connection termination request is being waited after the local machine transmits connection termination request to the peer and receives the peer's acknowledgement. CLOSE_WAIT—Means the connection termination request of the peer is received and the local response has been sent out, and now the local user is being waited to close the connection. Once the user requires to close the connection, the system will send the connection termination request. CLOSING—Means the connection termination request has been sent to the peer and the peer's connection termination request is also received and the corresponding response is also sent out, and now is waiting for the peer to acknowledge the local connection termination request. LAST_ACK—Means that the connection termination request from the peer is received and acknowledged, and now the connection termination request is transmitted and the response is waited. Means that a sufficient time is needed to ensure that the peer has already received the local acknowledgement of its connection termination request. CLOSED—Means that there is no connection or the connection has been completely shut down. For more detailed information, see RFC 793, TRANSMISSION CONTROL PROTOCOL.
unread input bytes:	Data that is submitted to but not yet received by the upper-layer application after the lower-layer TCP handles
Local host:	Local IP address
Local port:	Local TCP port
Foreign host:	Remote IP address
Foreign port:	Remote TCP port
Enqueued bytes for transmit:	Bytes in the transmission queue, including the transmitted but unacknowledged data bytes and not-yet-transmitted data bytes
input:	Data in the receiver queue which is waiting for being received by the upper-layer application after sorting
mis-ordered:	Number of bytes and number of packets in the mis-ordered queue These data can enter the receiver queue in order and be received by the upper-layer application after other data is received. For Example, if packets 1, 2, 3, 4, 5 and 6 are received, packets 1 and 2 can enter the receiver queue, while packets 4, 5 and 6 have to enter the mis-ordered queue to wait for the arrival of packet 3.

The information about the currently-displayed timer will then be displayed, including start-up times, timeout times and next timeout time. Each connection has its independent timers. The timeout times of the timer are generally less than the start-up times of the timer because the timer may be reset when it is running. For **Example**, if the system receives the peer's acknowledgement of all transmitted data when the re-sending timer runs, the re-sending timer will stop running.

Timer	Starts	Wakeups	Next(ms)
Retrans	33	1	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	102	0	7199500

Domain	Description
Timer	Name of the timer
Starts	Start-up times of the timer
Wakeups	Timeout times of the timer
Next(ms)	Time before next timeout occurs (unit: millisecond) 0 means that the timer is not running.
Retrans	Retransmission timer which is used to retransmit the data The timer is restarted after the data is transmitted. If the data is not acknowledged by the peer during the timeout time, the data will be resent.
TimeWait	Time-wait timer which is used to ensure that the peer receives the acknowledgement of the connection termination request.
SendWnd	Timer of the transmission timer, used to ensure that the receiver window resumes the normal size after the TCP acknowledgement is lost.
KeepAlive	KeepAlive timer used to ensure that the communication link is normal and the peer is still in the connection state It will trigger the transmission of the test packet to detect the state of the communication link and the peer's state.

The sequence number of the TCP connection will then be displayed. The reliable and ordered data transmission is guaranteed through the sequence number. The local/remote host conducts flow control and transmission acknowledgement through the sequence number.
iss: 29139463 snduna: 29139525 sndnxt: 29139525 sndwnd: 17520
irs: 709124039 rcvnxt: 709205436 rcvwnd: 4380

Domain	Description
iss:	Initial transmission sequence number
snduna:	Transmission sequence number of the first byte in the data which has been transmitted but the peer's acknowledgement is not received
sndnxt:	Transmission sequence number of the first byte in the data which will be transmitted next time
sndwnd:	Size of the TCP window of the remote host
irs:	Initial reception sequence number, that is, initial transmission sequence number of the remote host
rcvnxt:	Recently-acknowledged acceptation sequence number
rcvwnd:	Size of the TCP window of the local host

The transmission time recorded by the local host is then displayed. The system can adapt to different networks according to the data.

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms

minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Domain	Description
SRTT:	Round-trip time after smooth handlement
RXT:	Retransmission timeout time
RTV:	Change value of the round-trip time
MinRXT:	Allowable minimum retransmission timeout
MaxRXT:	Allowable maximum retransmission timeout
ACK hold:	Maximum latency time for delaying the acknowledgement and enabling it to be transmitted together with the data

Datagrams (max data segment is 1460 bytes):

Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396

Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61

Domain	Description
max data segment is	Maximum data-segment length allowed by a connection
Rcvd:	Number of packets received by the local host through the connection and the number of mis-ordered packets
with data:	Number of packets which contains valid data
total data bytes:	Total data bytes contained in the packet
Sent:	Total number of packets transmitted by the local host during the connection and the number of resent packets

Related command

show tcp brief

show tcp tcb

40.7.24 show tcp brief

To display the brief information about the TCP connection, run the following command:

show tcp brief [all]

Parameter

Parameter	Description
all	(optional) Displays all ports. If the keyword is not entered, the system will not display the port in listening mode.

Command Mode

EXEC

Example

```
Router#show tcp brief

TCB    Local Address      Foreign Address   State
0xE9ADC8   192.168.20.22:1023       192.168.20.124:513       ESTABLISHED
0xEA34C8   192.168.20.22:23  192.168.20.125:1472      ESTABLISHED
```

Domain	Description
TCB	Internal identifier of the TCP connection
Local Address	Local address and local TCP port
Foreign Address	Remote address and remote TCP port
State	State of the connection For details, see the show tcp command.

Related command

show tcp

show tcp tcb

40.7.25 show tcp statistics

To display the statistics data about TCP, run the following command:

show tcp statistics

Parameter

The command has no **Parameter**s or keywords.

Command Mode

EXEC

Example

```
Router#show tcp statistics
Rcvd: 148 Total, 0 no port
0 checksum error, 0 bad offset, 0 too short
131 packets (6974 bytes) in sequence
0 dup packets (0 bytes)
0 partially dup packets (0bytes)
0 out-of-order packets (0bytes)
0 packets (0 bytes) with data after window
0 packets after close
0 window probe packets, 0 window update packets
 0 dup ack packets, 0 ack packets with unsenddata
127 ack packets (247 bytes)
Sent: 239 Total, 0 urgent packets
6 control packets
123 data packets (245 bytes)
0 data packets (0 bytes) retransmitted
110 ack only packets (101 delayed)
0 window probe packets, 0 window update packets
 4 Connections initiated, 0 connections accepted, 2 connections established
3 Connections closed (including 0 dropped, 1 embryonicdropped)
5 Total rxmt timeout, 0 connections dropped in rxmt timeout
1 Keepalive timeout, 0 keepalive probe, 1 Connections dropped in keepalive
```

Domain	Description
Rcvd:	Statistics data of the packets received by the router
Total	Total number of the received packets
no port	Number of received packets which have no destination ports
checksum error	Number of received packets which have checksum error
bad offset	Number of received packets which have offset error
too short	Number of received packets whose length is less than the valid effective length
packets in sequence	Number of packets received in order
dup packets	Number of received duplicate packets
partially dup packets	Number of some duplicate packets received
out-of-order packets	Number of packets received out of order

packets with data after window	Number of received packets whose data exceeds the received window of the router

Domain	Description
packets after close	Number of packets received after the connection is closed
window probe packets	Number of received packets about window detection
window update packets	Number of received packets about window update
dup ack packets	Number of packets which are re-acknowledged after received
ack packets with unsent data	Number of packets which are received but not sent
ack packets	Number of acknowledgement packets
Sent	Statistics data of the packets transmitted by the router
Total	Total number of the transmitted packets
urgent packets	Number of transmitted urgent packets
control packets	Total number of control packets (SYN, FIN or RST) which have been transmitted
data packets	Number of transmitted urgent packets
data packets retransmitted	Number of resent data packets
ack only packets	Number of transmitted acknowledgement packets
window probe packets	Number of transmitted packets about window detection
window update packets	Number of transmitted packets about window update
Connections initiated	Number of locally-initiated connections
connections accepted	Number of locally-accepted connections
connections established	Number of locally-established connections
Connections closed	Number of locally-closed connections
Total rxmt timeout	Total number of re-transmission timeouts
Connections dropped in rxmit timeout	Number of disconnected connections because of re-transmission timeout
Keepalive timeout	Number of keepalive timeouts
keepalive probe	Number of transmitted packets about keepalive detection
Connections dropped in keepalive	Number of connections which are disconnected because of Keepalive

Related command

clear tcp statistics

40.7.26 show tcp tcb

To display the state of a TCP connection, run the following command:

show tcp tcb *address*

Parameter

Parameter	Description
address	Address of the transmission control block (TCB) for the to-be-displayed TCP connection TCB is an internal identifier of the TCP connection, which can be obtained through the show tcp brief command.

Command Mode

EXEC

Example

The following information is displayed after the show tcp command is run:

```
Router_config#show tcp tcb 0xea38c8

TCB 0xEA38C8
Connection state is ESTABLISHED, unread input bytes: 0 Local host: 192.168.20.22, Local port: 23
Foreign host: 192.168.20.125, Foreign port: 1583


Enqueued bytes for transmit: 0, input: 0 mis-ordered: 0 (0 packets)

Timer Starts Wakeups Next(ms)
Retrans 4 0 0
TimeWait 0 0 0
SendWnd 0 0 0
KeepAlive +5 0 6633000

iss: 10431492 snduna: 10431573 sndnxt: 10431573 sndwnd: 17440
irs: 915717885 rcvnxt:915717889 rcvwnd: 4380


SRTT: 2812 ms, RXT: 18500 ms, RTV: 4000 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):
Rcvd: 5 (out of order: 0), with data: 1, total data bytes: 3
Sent: 4 (retransmit: 0), with data: 3, total data bytes: 80
```

Related command

show tcp

show tcp brief

40.8 ACL Configuration Commands

ACL configuration commands include:

- deny
- ip access-group
- ip access-list
- show ip access-list
- permit

40.8.1 deny

To configure the deny rules in IP ACL configuration mode, run deny *source* [*source-mask*] [log]; to remote the deny rules from the IP access control list, run no deny *source* [*source-mask*] [log].

deny *source* [*source-mask*] [log]

no deny *source* [*source-mask*] [log]

deny src_range source-begin source-end [log]

no deny src_range source-begin source-end [log]

deny *protocol source source-mask destination destination-mask* [precedence *precedence*] [tos *tos*] [log]

no deny *protocol source source-mask destination destination-mask* [precedence *precedence*] [tos *tos*] [log]

deny protocol src_range source-begin source-end dst_range destination-begin destination-end [precedence *precedence*] [tos *tos*] [log]

no deny protocol src_range source-begin source-end dst_range destination-begin destination-end [precedence *precedence*] [tos *tos*] [log]

The following **Syntax** can also be applied to ICMP:

deny icmp *source source-mask destination destination-mask* [*icmp-type*] [precedence *precedence*] [tos *tos*] [log]

deny icmp src_range source-begin source-end dst_range destination-begin destination-end [*icmp-type*] [precedence *precedence*] [tos *tos*] [log]

The following **Syntax** can be used for IGMP:

deny igmp *source source-mask destination destination-mask* [*igmp-type*] [precedence *precedence*] [tos *tos*] [log]

deny igmp src_range source-begin source-end dst_range destination-begin destination-end [*igmp-type*] [precedence *precedence*] [tos *tos*] [log]

For TCP, you can use the following **Syntax**:

deny tcp *source source-mask* [*operator port*] *destination destination-mask*
[*operator port*] [established] [precedence *precedence*] [tos *tos]* [log]

deny tcp src_range source-begin source-end [*src_portrange port-begin port-end*] dst_range destination-begin destination-end [*dst_portrange port-begin port-end*] [established] [precedence *precedence*] [tos *tos*] [log]

For UDP, you can use the following **Syntax**:

deny udp *source source-mask* [*operator port*] *destination destination-mask*
[*operator port*] [precedence *precedence*] [tos *tos*] [log]

deny udp src_range source-begin source-end [*src_portrange port-begin port-end*] dst_range destination-begin destination-end [*dst_portrange port-begin port-end*] [precedence *precedence*] [tos *tos*] [log]

Parameter

Parameter	Description
protocol	Protocol name or IP protocol number It can be icmp, igmp, igrp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the ip keyword. Some protocol can be further limited, which can be further described.
source	Source network or host numberTwo methods can be used to designate the source: 32-byte binary-system numbers and decimal-system numbers which are separated by four points. The any keyword can be the abbreviation of the source and the source's mask of host0.0.0.0.0.0.0.0.
source-mask	Mask of the source address The any keyword can be the abbreviation of the source and the source's mask of host 0.0.0.0.0.0.0.0.
destination	Source network or host number, which can designated by the decimal numbers or the binary numbers The any keyword can be the abbreviation of the destination and the destination's mask of host 0.0.0.0.0.0.0.0.
destination-mask	Mask of the destination network The any keyword can be the abbreviation of the destination and the destination's mask of host 0.0.0.0.0.0.0.0.

Parameter	Description
precedence precedence	Filters the packets based on the precedence. The precedence of the packet can be designated by an integer from 0 to 7. This Parameter is optional.
tos tos	An optional Parameter, meaning that the packets can be filtered at the service layer It is designated by any number between 0 and 15.
icmp-type	An optional Parameter, which means that the ICMP packet can be filtered based on the type of the ICMP packetThe type of the ICMP packet can be designated by a number between 0 and 255.
igmp-type	An optional Parameter, which means that the IGMP packets can be filtered based on the type and name of the IGMP packet The type of the IGMP packet can be designated by a number between 0 and 15.
operator	Compares the source or destination ports. It is an optional Parameter. The operations include lt, gt, eq and neq. If the operator symbol is behind source and source-mask, it must match up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
ISDN(BRI) interface	Decimal number or name of the TCP/UDP port, which is optional The port number ranges between 0 and 65535. The name of the TCP port is listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. The names of the UDP ports are also listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. When the UDP is filtered, only the name of the UDP port can be used.
established	An optional Parameter for the TCP protocol, representing an established connection If the TCP data reports that the ACK or RST is configured, the match-up appears. For the unmatched case, the TCP packet is initialized to establish a connection.
log	An optional Parameter, meaning the logs can be recorded
Source-begin	Enables the source address.
Source-end	Terminates the source address.
Destination-begin	Starts the destination address.
Destination-end	Terminates the destination address.
Port-begin	Starts the port.
Port-end	Terminates the port.

Command Mode

ARP Access List Configuration

Usage Description

You can control the packet transmission on an interface, virtual terminal line access and routing choice update through the access control list. After the match-up is conducted, you shall stop checking the expanded access control list.The segmented IP

packet, not the initial segment, will be immediately accepted by any expanded IP access control list. The expanded ACL is used to control the access of the virtual terminal line or limit the content of the routing choice update without matching up the source TCP port, the type of the service value or the packet's priority.

NOTE: After an access control list is initially created, any content added later (or entered through the terminal) will be placed at the end of the list.

The following are the names of the TCP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

- bgp
- ftp
- ftp-data
- login
- pop2
- pop3
- smtp
- telnet
- www

The following are the names of the UDP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

- domain
- snmp
- syslog
- tftp

Example

The following **Example** shows that network segment 192.168.5.0 is being forbidden.

```
ip access-list standard filter
deny 192.168.5.0 255.255.255.0
```

NOTE: The IP access control list ends with an implicit deny rule.

Related command

```
ip access-group ip access-list permit
show ip access-list
```

40.8.2 ip access-group

To control and access an interface, run ip access-group {*access-list-name*}{in | out}. To delete the designated access group, run no ip access-group {*access-list-name*}{in | out}.

ip access-group {*access-list-name*}{in | out}

no ip access-group {*access-list-name*}{in | out}

Parameter

Parameter	Description
access-list-name	Name of the access control list, which is a string with up to 20 characters
in	Uses the access control list on the incoming interface.
out	Uses the access control list on the outgoing interface.

Command Mode

Interface configuration mode

Usage Description

The access control list can be used on the incoming or outgoing interface. For the standard incoming access control list, the source address of the packet will be checked according to the access control list after the packet is received. For the expanded access control list, the router will check the destination address. If the access is the address, the software continues to handle the packet. If the access control list forbids the address, the software drops the packet and returns an ICMP unreachable packet.

For the standard access control list, after a packet is received and routed to a control interface, the software checks the source address of the packet according to the access control list. For the expanded access control list, the router will also check the access control list at the receiver terminal. If the access control list at the receiver terminal permits the packet, the software will then forward the packet. If the access control list forbids the address, the software drops the packet and returns an ICMP unreachable packet.

If the designated access control list does not exist, all packets will be allowed.

Example

The following **Example** shows how to apply the filter application list on interface Ethernet 0.

```
interface ethernet 0
ip access-group filter out
```

Related command

```
ip access-list
show ip access-list
```

40.8.3 ip access-list

To add the IP access control list, run ip access-list {standard | extended} *name*.
To delete an IP access control list, run no ip access-list {standard | extended} *name*.
ip access-list {standard | extended} *name*
no ip access-list {standard | extended} *name*

Parameter

Parameter	Description
standard	Specifies the standard access control list.
extended	Specifies the expanded access control list.
name	Name of the access control list, which is a string with up to 20 characters

Default

No IP access control list is defined.

Command Mode

Global configuration mode

Usage Description

After the command is run, the system enters the IP access control list mode. You then can run permit or deny to configure the access rules.

Example

The following **Example** shows that a standard access control list is configured.

```
ip access-list standard filter
deny 192.168.1.0 255.255.255.0
permit any
```

Related command

deny
ip access-group permit
show ip access-list

40.8.4 permit

To configure the permit rules in IP ACL configuration mode, run permit *source* [*source-mask*] [log]; to remote the permit rules from the IP access control list, run no permit *source* [*source-mask*] [log].

permit *source* [*source-mask*] [log] no permit *source* [*source-mask*] [log]
permit src_range source-begin source-end [log]

no permit src_range source-begin source-end [log]

permit *protocol source source-mask destination destination-mask* [precedence *precedence*] [tos *tos*] [log]

no permit protocol source source-mask destination destination-mask [precedence *precedence*] [tos *tos*] [log]

permit protocol src_range source-begin source-end dst_range destination-begin destination-end [precedence *precedence*] [tos *tos*] [log]

no permit protocol src_range source-begin source-end dst_range destination-begin destination-end [precedence *precedence*] [tos *tos*] [log]

The following **Syntax** can also be applied to ICMP:

permit icmp *source source-mask destination destination-mask* [*icmp-type*] [precedence *precedence*] [tos *tos*] [log]

permit icmp src_range source-begin source-end dst_range destination-begin destination-end [*icmp-type*] [precedence *precedence*] [tos *tos*] [log]

The following **Syntax** can be used for IGMP:

permit igmp *source source-mask destination destination-mask* [*igmp-type*] [precedence *precedence*] [tos *tos*] [log]

permit igmp src_range source-begin source-end dst_range destination-begin destination-end [*igmp-type*] [precedence *precedence*] [tos *tos*] [log]

For TCP, you can use the following **Syntax**:

permit tcp source source-mask *[*operator port*]* destination destination-mask [*operator port*] [established] [precedence *precedence*] [tos *tos*] [log]

permit tcp src_range source-begin source-end [*src_portrange port-begin port-end*] dst_range destination-begin destination-end [*dst_portrange port-begin port-end*] [established] [precedence *precedence*] [tos *tos*] [log]

For UDP, you can use the following **Syntax**:

permit udp *source source-mask* [*operator port* [*port*]] *destination destination-mask* [*operator port*] [precedence *precedence*] [tos *tos*] [log]

permit udp src_range source-begin source-end [*src_portrange port-begin port-end*] dst_range destination-begin destination-end [*dst_portrange port-begin port-end*] [precedence *precedence*] [tos *tos*] [log]

Parameter

Parameter	Description
protocol	Protocol name or IP protocol number It can be icmp, igmp, igrp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the ip keyword. Some protocol can be further limited, which can be further described.
source	Source network or host number Two methods can be used to designate the source: 32-byte binary-system numbers and decimal-system numbers which are separated by four points. The any keyword can be the abbreviation of the source and the source's mask of host 0.0.0.0.0.0.0.0.
source-mask	Mask of the source address The any keyword can be the abbreviation of the source and the source's mask of host 0.0.0.0.0.0.0.0.
destination	Source network or host number, which can designated by the decimal numbers or the binary numbers There are two methods to express the destination network or the host's number: the binary system and decimal system The any keyword can be the abbreviation of the destination and the destination's mask of host 0.0.0.0.0.0.0.0.
destination-mask	Mask of the destination network The any keyword can be the abbreviation of the destination and the destination's mask of host 0.0.0.0.0.0.0.0.
precedence precedence	Filters the packets based on the precedence. The precedence of the packet can be designated by an integer from 0 to 7. This Parameter is optional.
tos tos	An optional Parameter, meaning that the packets can be filter at the service layer It is designated by any number between 0 and 15.
icmp-type	An optional packet, which means that the ICMP packet can be filtered based on the type of the ICMP packetThe type of the ICMP packet can be designated by a number between 0 and 255.
igmp-type	An optional Parameter, which means that the IGMP packets can be filtered based on the type and name of the IGMP packet The type of the IGMP packet can be designated by a number between 0 and 15.
operator	Compares the source or destination ports. It is an optional Parameter. The operations include lt, gt, eq and neq. If the operator is behind source and source-mask, it must match up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
ISDN(BRI)	Decimal number or name of the TCP/UDP port, which is optional The port number ranges between 0 and 65535. The name of the TCP port is listed in the Usage Guide part. When the TCP is filtered, only the name of the TCP port can be used. The names of the UDP ports are also listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. When the UDP is filtered, only the name of the UDP port can be used.

Parameter	Description
established	An optional Parameter for the TCP protocol, representing an established connection If the TCP data reports that the ACK or RST is configured, the match-up appears. For the unmatched case, the TCP packet is initialized to establish a connection.
log	An optional Parameter, meaning the logs can be recorded
Source-begin	Enables the source address.
Source-end	Terminates the source address.
Destination-begin	Start the destination address.
Destination-end	Terminates the destination address.
Port-begin	Starts the port.
Port-end	Terminates the port.

Command Mode

IP access list configuration mode

Usage Description

You can control the packet transmission on an interface, virtual terminal line access and routing choice update through the access control list. After the match-up is conducted, you shall stop checking the expanded access control list.

The segmented IP packet, not the initial segment, will be immediately accepted by any expanded IP access control list. The expanded ACL is used to control the access of the virtual terminal line or limit the content of the routing choice update without matching up the source TCP port, the type of the service value or the packet'spriority.

NOTE: After an access control list is initially created, any content added later (or entered through the terminal) will be placed at the end of the list.

The following are the names of the TCP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the command.

- bgp
- ftp
- ftp-data
- login
- pop2
- pop3
- smtp
- telnet
- www

The following are the names of the UDP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the command.

- domain
- snmp
- syslog
- tftp

Example

The following **Example** shows that network segment 192.168.5.0 is allowed.

ip access-list standard filter permit 192.168.5.0 255.255.255.0

NOTE: The IP access control list ends with an implicit deny rule.

Related command

deny
ip access-group
ip access-list
show ip access-list

40.8.5 show ip access-list

To display the content of the current IP access control list, run the following command:

show ip access-list[*access-list-name*]

Parameter

Parameter	Description
access-list-name	Name of the access control list, which is a string with up to 20 characters

Default

All standard/expanded IP access control lists will be displayed.

Command Mode

EXEC

Usage Description

The show ip access-list command enables you to specify an access control list.

Example

The following information is displayed after the show ip access-list command is run while an access control list is not specified:

Router# show ip access-list i
p access-list standard aaa
permit 192.2.2.1
permit 192.3.3.0 255.255.255.0

```
ip access-list extended bbb
permit tcp any any eq www
permit ip any any
```

The following information is displayed after you run the show ip access-list command with an access control specified:

ip access-list extended bbb permit tcp any any eq www

Chapter 41 Fast Ethernet Protection ERPS Configuration Command

41.1 Global Configuration Command

41.1.1 Erps

configure the ring network instance to enter node configuration mode.

erps id

Delete node instances:

no erps id

Parameters

Parameters	Parameter description
id	Node instance number.

Default

By default, the ring network node instance is not configured.

Command mode

Global configuration mode.

Use instructions

None.

Example

Switch_config#erps 1
Switch_config_ring1#

Related Orders

None.

41.1.2 control-vlan

Configure the control vlan value of the local node.

control-vlan value

Delete the control vlan value of the local node.

no control-vlan

Parameters

Parameters	Parameter description
value	Range 1-4094.

Default

no control-vlan. by default

Command mode

ring network node configuration mode.

Use instructions

Node configuration must be optional, node after normal operation can not be changed.

Example

Switch_config#erps 1
Switch_config_ring1#
Switch_config_ring1#control-vlan 2

Related Orders

None.

41.1.3 interconnection-node

configure the local node as an interconnected node.

interconnection-node

Configuring local nodes is not an interconnected node.

no interconnection-node

Parameters

None.

Default

default is local node not interconnected node.

Command mode

ring network node configuration mode.

Use instructions

Node configuration must be optional, node after normal operation can not be changed. At the same time, although it is a required command item, it has an default configuration, so you can omit these commands when you create a local node without modifying the default value.

Example

```
Switch_config#erps 1
Switch_config_ring1#
Switch_config_ring1#interconnection-node
```

Related Orders

None.

41.1. 4 raps -virtual-channel

Configure local nodes to use R-APS virtual channels.

raps -virtual-channel

Configure the local node without using R-APS virtual channels.

no raps -virtual-channel

Parameters

None.

Default

Default uses R-APS virtual channels for local nodes.

Command mode

ring network node configuration mode.

Use instructions

Node configuration must be optional, node after normal operation can not be changed. At the same time, although it is a required command item, it has an default configuration, so you can omit these commands when you create a local node without modifying the default value.

Example

Switch_config#erps 1
Switch_config_ring1#
Switch_config_ring1#raps -virtual-channel

Related Orders

None.

41.1.5 revertive-mode

configure the return mode of the local node as return mode.

revertive-mode

Configure the return mode of the local node as non-return mode.

no revertive-mode

Parameters

None.

Default

Default is local node for return mode.

Command mode

ring network node configuration mode.

Use instructions

Node configuration must be optional, node after normal operation can not be changed. At the same time, although it is a required command item, it has an default configuration, so you can omit these commands when you create a local node without modifying the default value.

Example

```
Switch_config#erps 1
Switch_config_ring1#
Switch_config_ring1#revertive-mode
```

Related Orders

None.

41.1.6 Version

Configure version. of local nodes

version value

The configuration version is value.

no version

Parameters

Parameters	Parameter description
value	Default 1, range 0-2.

Default

Default, version 1.

Command mode

ring network node configuration mode.

Use instructions

None.

Example

```
Switch_config#erps 1
Switch_config_ring1#
Switch_config_ring1#version 1
```

Related Orders

None.

41.1.7 wtr-time

configure the switching recovery timer WTR timeout.

wtr-time value

no wtr-time

Parameters

Parameters	Parameter description
value	Timer timeout, default 20 seconds, range 10-720 seconds.

Default

By default, WTR timer timeout is 300 seconds.

Command mode

ring network node configuration mode.

Use instructions

None.

Example

```
Switch_config#erps 1
Switch_config_ring1#
Switch_config_ring1#wtr-time 15
```

Related Orders

None.

41.1.8 guard-time

configure Guard timer timeout time.

guard-time value

no guard-time

Parameters

Parameters	Parameter description
value	Timer timeout, unit 10 milliseconds, default 50, range 1-200.

Default

By default, Guard timer timeout is 500 milliseconds.

Command mode

ring network node configuration mode.

Use instructions

As a port recovers from the failure state, the Guard timer for a short period of time forbids processing the received protocol message to avoid the wrong protocol action due to receiving the expired message.

Example

```
Switch_config#erps 1
Switch_config_ring1#guard-time 60
```

Related Orders

None.

41.1.9 send-time

configure protocol message sending cycle.

send-time value

no send-time

Parameters

Parameters	Parameter description
value	Timer timeout, default 5 seconds, range 1-10 seconds.

Default

By default, the ERPS PDU transmission interval is 5 seconds.

Command mode

ring network node configuration mode.

Use instructions

None.

Example

```
Switch_config_ring1#wtr-time 15
Switch_config_ring1#send-time 5
```

Related Orders

None.

41.2 Port Configuration Command

41.2.1 erps ring-port

The configuration port is a normal ring network port.

erps id ring-port

Delete loop configuration for normal or RPL ports:

no erps id ring-port

Parameters

Parameters	Parameter description
id	Node instance number.

Default

No default configuration.

Command mode

Switch port configuration mode (physical port or aggregate port).

Use instructions

ERPS protocol supports configuring physical or aggregate ports as ring network ports. physical ports that have been configured for link aggregation ,802.1 X authentication, or port security are not configurable as ERPS ring network ports.

The default VLAN of all ring ports need to be configured consistently to ensure that ERPS messages are forwarded properly.

Example

```
Switch_config#interface f0/1
Switch_config_f0/1#erps 1ring-port
```

Related Orders

None.

41.2.2 erps rpl

the configuration port is ERPS ring network protection link (Ring Protection Link).

erps id rpl

Delete the RPL port configuration but retain the normal ring network port role of the port:

no erps id rpl

Parameters

Parameters	Parameter description
id	Node instance number.

Default

No default configuration.

Command mode

Switch port configuration mode (physical port or aggregate port).

Use instructions

For automatic discovery of enabling, the function of the erps rpl command is equivalent to modifying the priority value to 0.

To remove the ring configuration of the port, use the command:

no erps id ring-port

Example

```
Switch_config_f0/1#interface f0/3
Switch_config_f0/3#erps 1rpl
```

Related Orders

None.

41.2.3 erps neighbour

Configuration port is ERPS RPL neighbour.

erps id neighbour

Delete RPL neighbour port configuration:

no erps id neighbour

Parameters

Parameters	Parameter description
id	Node instance number.

Default

No default configuration.

Command mode

Switch port configuration mode (physical port or aggregate port).

Use instructions

the port is configured as the RPL neighbor port of the specified node, and the port must be connected to the RPL port and must be configured as the RPL neighbor port.

Example

```
Switch_config_f0/1#interface f0/3
Switch_config_f0/3#erps 1neighbour
```

Related Orders

None.

41.2.4 erps mep

bind ERPS port to MEP port.

erps id mep [up1|up2|down]md md-WORD ma ma-WORD level level-id local local-id remote remote-id

unbind ERPS port to MEP port.

no erps id mep [up1|up2|down]

Parameters

Parameters	Parameter description
id	ring network instance number.
md-WORD	MEP maintenance domain information.
ma-WORD	MEP maintenance link information.
level-id	MEP rating information.
local-id	MEP local id information.
remote-id	MEP distal id information.

Default

No default configuration.

Command mode

Switch port configuration mode (physical port or aggregate port).

Use instructions

CFM ports need to be configured before binding.

Example

```
Switch_config_f0/1#interface f0/3
Switch_config_f0/3#erps 1mep down md d ma d level 4local 4remote 1
```

Related Orders

None.

41.3 Control Orders

41.3.1 erps [ForcedSwitch |ManualSwitch |Clear]

Forced switching of nodes to port int er f ace-type interface -number：

erps id ForcedSwitch interface int er f ace-type interface -number

Change nodes manually to port int er f ace-type interface -number：

erps id M anualSwitch interface int er f ace-type interface -number

Clear node switching command:

erps id Clear

Parameters

Parameters	Parameter description
id	Node instance number.
int er f ace-type	Port type.
interface -number	Port number.

Default

None.

Command mode

Monitoring mode.

Use instructions

None.

Example

None.

Related Orders

None.

41.4 Display Command

41.4.1 show erps

Display summary information ERPS ring protection:

show erps [id]

Display ring node details:

show erps id detail

Display ring network port information:

show erps interface intf-name

Parameters

Parameters	Parameter description
id	Node instance number.
intf-name	Port name.

Default

None.

Command mode

monitoring mode, global configuration mode, node configuration mode, or port configuration mode.

Use instructions

None.

Example

None.

Related Orders

None.

https://www.fs.com

The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.