Ethernet Switch

Command Line Reference Manual

V1.0.0

Foreword

Model

Gigabit Managed Switches.

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
⚠ TIPS	Provides methods to help you solve a problem or save you time.
📖 NOTE	Provides additional information as the emphasis and supplement to the text.

Command Line Format

The following symbols might appear in the manual.

Symbol	Description
< >	Command line parameter (it has to be replaced by the actual value in the command) adopts <> to represent.
[ ]	[ ] means optional during command configuration.
{x	y	…}	It means to select one from two or several options.
<x	y	…>	It means to select one or none from two or several options.
{x	y	…}*	It means to select several or at least one from two or several options; it is to select all the options at most.
( )	( ) means repetition for several times.
//	The line which starts with // means comment line.

Icon

Icon	Description
	The icon and related description mean layer 2 and 3 Ethernet switch and the devices which operate layer 2 protocol.

Port SN Example

The port SN which appears in the Manual is only used as an example, which doesn't mean the device is equipped with the port of the serial number. Refer to the actual port SN during application.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	April 2021

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

The manual helps you to use our product properly. To avoid danger and property damage, read the manual carefully before using the product, and we highly recommend you to keep it well for future reference.

Operating Requirements

- Do not expose the device directly to the sunlight, and keep it away from heat.
- Do not install the device in the damp environment, and avoid dust and soot.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Avoid liquid spattering on the device. Do not place object full of liquid on the device to avoid liquid flowing into the device.
- Install the device in the well-ventilated environment. Do not block the air vent of the device.
- Use the device at rated input and output voltage.
- Do not disassemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.
- When removing the cable, power off the device first to avoid personal injury.
- Voltage stabilizer and lightning protection device are optional according to power supply and surrounding environment.

Power Supply Requirements

- Use the battery properly to avoid fire, explosion, and other dangers.
- Replace the battery with battery of the same type.
- Use locally recommended power cord in the limit of rated specifications.
- Use the standard power adapter. We will assume no responsibility for any problems caused by nonstandard power adapter.
- The power supply shall meet the SELV requirement. Use the power supply that conforms to Limited Power Source, according to IEC 62368-1. Refer to the device label.
- Be sure to ground the device (cross section of copper wire: > 2.5 mm^2; resistance to ground: ≤ 4 Ω).
- The coupler is the disconnecting apparatus. Keep it at the angle for easy operation.

Table of Contents

1 Login

1.1 Login Methods

The switch supports two login methods including CLI (Command Line Interface) and web.

● You can directly enter the command line to configure and manage the switch after logging in the switch by CLI. The login methods can be different according to the login port and login interface under CLI method, including Console port, Telnet, and SSH. You can only log in by Console port for the first time login by CLI. And you can log in the switch by Telnet or SSH only when you log in the switch by Console port and set the corresponding configuration.

● You can visually manage and maintain the network devices in web interface after logging in the switch by web.

1.2 Login System

You can log in the switch by Console port when you need to configure the switch powered on for the first time.

Console port is a type of communication serial port on the main control panel of the switch. One main control panel provides one Console port. The user terminal serial port can be directly connected to the switch Console port to realize local configuration for the switch.

1.3 First Time Login via Console Port

Login by Console port is the most basic way to log in the switch, and it is also the method to configure other ways to log in the device.

To log in the device by Console port, do the following:

Step 1   Power off the PC.

Do not plug the serial port line into or out from PC when PC is powered on, because PC serial port does not support hot plug.

Step 2   Connect the PC and the switch with the default configuration port cable. First insert the DB-9 plug of configuration port cable into the 9-pin serial port of the PC, and then insert the RJ-45 plug into the device Console port. See Figure 1-1.

● Confirm the symbol on the port during connection in case that it plugs into other ports.

● When removing configuration port cable, first plug out RJ-45 and then DB-9.

● You need to prepare a USB line if there is no serial port on the PC.

Figure 1-1 Networking
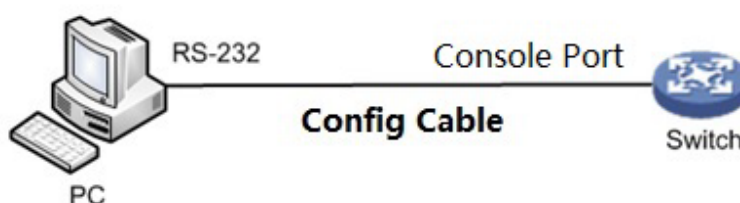
Step 3   Power on the PC.

Step 4   Operate the terminal simulation program on the PC, and then select the serial port connect to the switch to set the terminal communication parameters. The parameters should be in accordance with that of the switch. The default values are as follows:

- Baud rate: 115200
- Data bit: 8
- Stop bit: 1
- Parity: None
- Flow control: None

For the PC with Windows Server 2003 operating system, you need to add the super terminal program in the Windows and then log in and manage the switch according to the descriptions in the text. For the PC with Windows Server 2008, Windows Vista, Windows 7, or other operating system, you need to prepare third-party terminal control software, and refer to the guidance or online help of the software. SecureCRT is taken as an example.

Step 5   Power on the switch, and the self-check information is displayed on PC. There will be the prompt for you to press Enter key after switch self-check. And you can enter the user name and password.

Step 6   Enter the user name. It is admin by default. And press Enter key.

Step 7   Enter the password. It is admin by default. And press Enter key.
Prompt symbol of command line (SWITCH#) is displayed after you press Enter key, as shown in the following. And you login the device successfully.

Press ENTER to get started

Username: admin
Password:
SWITCH#

Step 8   Enter the command, and you can configure the device and view the device operating status. You can enter ? anytime if you need help.

1.4 (Optional) Login by Telnet

Telnet Server function of the switch is disabled by default. You need to log in the device by Console port first to enable Telnet server function, and then set the corresponding configuration for authentication method, user role, and public attribute to log in the device by Telnet.

Enable Telnet Server Function

aaa authentication login telnet local, to enable Telnet function.

no aaa authentication login telnet, to disable Telnet function.

Add New Telnet User

You can log in the switch with the default user name (admin) and password (admin), and you can also add a new Telnet user to log in the switch.

To add a new Telnet user, do the following:

// Add a new user. The user name is telnet, and the password is admin123456.

```
Username telnet privilege 15 password unencrypted admin123456
```

Display Result

After configuration is completed, and when you log in the switch by Telnet, the login interface will be displayed, as shown in the following.

```
Username:
```

Enter the user name and the password.

1.5 (Optional) Login by SSH

Secure Shell (SSH) can provide security guarantee and protect the device from being attacked by IP address fraud and cleartext password interception with encryption and powerful authentication function.

SSH Server function of the switch is disabled by default. You need to log in the device by Console port first to enable SSH server function, and then set the corresponding configuration for authentication method, user role, and public attribute to log in the device by SSH.

Enable Telnet Server Function

ip ssh, to enable SSH function.

no ip ssh, to disable SSH function. You cannot manage the switch by SSH.

See "8.1.2 IP SSH" for details.

Add New Telnet User

You can log in the switch with the default user name (admin) and password (admin), and you can also add a new SSH user to log in the switch.

To add a new SSH user, do the following:

// Add a new user. The user name is ssh, and the password is admin123456.

```
username ssh privilege 15 password unencrypted admin123456
```

Display Result

After configuration is completed, and when you log in the switch by SSH, the login interface will be displayed, as shown in the following.

```
SWITCH#
```

Enter the user name and the password.

1.6 (Optional) Login by Web

You can log in the switch by web. After you login the switch by web, see the web operation manual for detailed operation.

Step 1   Open web browser, enter the IP address of the switch in the address bar, and press Enter key.

Ⅲ

The IP address is 192.168.1.110 by default.

Figure 1-2 Login interface

Step 2 Enter the user name and the password.

Ⅲ

The user name and password are admin by default.

Step 3 Click **Login**.

Ⅲ

Change the password after first login. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

2 Command Line

2.1 Command Line Interface

Command Line (CLI) is a type of text command interactive interface between user and device.

You need to enter the text command, and press Enter key to submit the command for the switch to execute, and to configure and manage the switch. You can also view the configuration result by checking the output information.

The switch supports multiple methods to enter the command line interface. For example. You can log in the switch by Console port, Telnet, and SSH, and then enter the command line interface, as shown in the following.

```
Press ENTER to get started

Username: admin
Password:
SWITCH#
```

2.2 Command Mode

2.2.1 Command Mode Introduction

The switch provides various functions, and different functions are corresponding to different configuration and query commands. To make it convenient for you to use the commands, the commands are divided into different groups, which are corresponding to different command modes. When you need to configure a certain command of a certain function, you need to enter the function mode first. Every mode has its unique and clear prompt symbol. For example, the prompt symbol SWITCH (config) # means that the current command mode is global mode, and you can configure port/VLAN (Virtual Local Area Network) and other attributes.

The command mode adopts layered structure. See Figure 2-1.

Figure 2-1 Layered structure for command mode
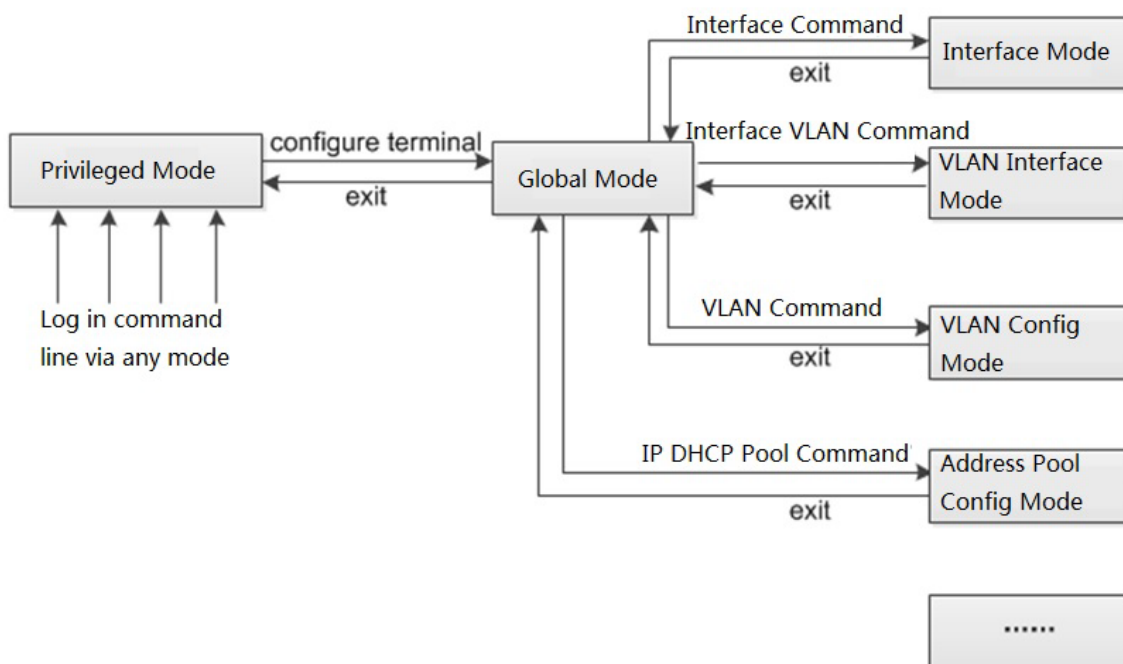
- You will enter the privileged mode directly after you log in the switch, and the prompt symbol displayed on the screen is device name #. In privileged mode, you can check, debug, manage the files, set the system time, reboot the switch, and operate FTP and Telnet.
- You can enter the global mode from privileged mode, and the prompt symbol displayed on the screen is device name *(config)* #. In global mode, you can configure the switch running parameters and some functions, including DST, welcome information, and shortcut key.
- Enter the specific command in the privileged mode to enter the corresponding function mode, and to configure the corresponding function. For example, enter the interface mode to configure the interface parameters, enter the VLAN interface mode to add the interface to VLAN.

If you want to know the commands supported in a certain mode, enter <?> after the prompt symbol.

"Device Name" means the name of the switch.

2.2.2 Entering Global Mode

Enter the global mode. See Table 2-1.

Table 2-1 Entering global Mode

Parameter	Command	Description
Enter global mode	configure terminal	The command is executed in privileged mode.

2.2.3 Returning to the Previous Mode

When the functions of the current mode are configured, you can exit the mode and return to the previous mode with this command. See Table 2-2 for details.

Table 2-2 Returning to the previous mode

Parameter	Command	Description
Return to the previous mode from the current mode.	exit	The command is executed in amy mode.

2.3 Command Line Online Help

You can enter <?> in any location of the command line for detailed online help when you are entering the command line. The following are the common online help applications for reference only.

● In any mode, you can enter <?> to acquire all the commands and their simple descriptions available in the mode. Example:

```
SWITCH#?
alarm            alarm
clear            Reset functions
configure        Enter configuration mode
……omit……
```

● Enter the key words of a command, a blank, and <?>. If <?> location is key word, all key words and their simple descriptions are listed. Example:

```
SWITCH(config)# ip ?
arp              Address Resolution Protocol
dhcp             Configure DHCP server parameters
dns              Domain Name System
domain           IP DNS Resolver
helper-address   DHCP relay server
http             Hypertext Transfer Protocol
igmp             Internet Group Management Protocol
name-server      Domain Name System
route            Add IP route
source           source command
ssh              Secure Shell
verify           verify command
```

● Enter the incomplete key word of the command and <?>, and all key words which start with the character string will be listed. Example:

```
SWITCH# con?
configure      Enter configuration mode
```

2.4 NO Form of the Command

The NO form of the command is generally used to restore default, forbid some function, or delete some settings. Most of the configuration commands have their corresponding NO forms.

For example, logging on command is used to enable log server mode, and no logging on command is used to forbid logging server mode.

2.5 Entering the Command Line

2.5.1 Editing Command Line

When you edit the command line, single key is supported. See Table 2-3 for details.

Table 2-3 Editing command line

Parameter	Description
Common key	If the editing buffer area is not full, insert to the current cursor location and move the cursor rightward (the command line will be temporarily cached in the editing buffer area before issuing, and the capacity of buffer area is 511 characters. the follow-up characters are invalid if the editing buffer area is full).
<Backspace>	Delete the previous character of the cursor location, and move the cursor forward.
Left cursor key<←>	The cursor moves one character leftward.
Right cursor key<→>	The cursor moves one character rightward.
Up cursor key<↑>	Visit previous history command.
Down cursor key<↓>	Visit the next history command.
<Tab> key	The system will automatically complement the key word after entering incomplete key word and pressing <Tab> key. ● If the matched key word is unique , the system will replace the original input with this complete key word and display with line feed. ● If the matched key word is not unique, press <Tab> key for several times, and the system will circularly display the entire key words which start with the entered character string. ● If there is not matched key word, the system will not make any modification, and the original input will be displayed with line feed again.

Press Enter key to execute the command after you enter the command line by keyboard.

Then total length of the command you entered cannot exceed 512 characters, including spacing, key word, and other special symbol.

2.5.2 Entering Command Line Quickly

The switch supports incomplete key word input, which means that in the current mode, you do not need to enter the complete key word when there are enough input characters to match the unique key word, and it provides a type of rapid input mode to enhance efficiency. For example, in global mode, the commands which start with c include configure terminal and clear.

You can directly enter con ter (do not enter c merely, because the matched key word is not unique) if you need to enter configure terminal.

Press <Tab> key and the system will automatically complement all the characters of the key word, and make sure that the key word is what you need to enter.

2.6 Common Input Error Information

Press Enter key to execute the command after entering all the command lines. The grammar of the command lines will be checked first during the executing process. If there is no error, the command will be executed normally. Otherwise, it will output error information. See Table 2-4.

Table 2-4 Common input error of command line

Error Information	Error Reason
%Incomplete command.	The entered command line is incomplete.
%Invalid word detected at '^' marker.	The entered command line is wrong.

2.7 History Command

The commands successfully executed on the switch will be saved in the history command buffering zone which is only for the user. See Table 2-5.

Table 2-5 History command buffer zone

History Command Buffer Zone	Whether it can be checked	Whether it can be called	Whether the history command will be saved after logging out
Exclusive history command buffer zone, and each user is corresponding to an exclusive history command buffer zone	Check by show history.	• Press up cursor key< ↑ > and Enter key to call the previous history command. • Press down cursor key< ↑ > and Enter key to call the next history command.	Not saved.

When saving the history commands, the switch conforms to the following principles:

- Format of the history command saved in the switch should be the same as that of the entered command. If you adopt the incomplete command format, format of the history command saved will also be incomplete. And if you adopt the alias format of command key word, the format of the history command saved will also be alias.
- The history command will only be saved for once if you execute the same command continuously for several times. If you enter the command in different formats, it will be saved as different commands.

⚠️

You can visit the history command with the cursor key in super terminal of Windows 200X and Windows XP and Telnet. As for the super terminal of Windows 9X, up cursor key< ↑ > and down cursor key< ↓ > are invalid, because there are different explanations for up cursor key< ↑ > and down cursor key< ↓ > in the super terminal of Windows 9X.

2.8 Checking Display Information Conveniently

Split Screen Display

The information will be displayed in split screen if there is too much display information covering more than one screen. And it will automatically pause between the screen for you to check the information conveniently.

You can select the next operation with the keyboard. See Table 2-6.

Table 2-6 Key for split screen display

Key	Function
Space	Continues to display the information of next screen.
Enter	Continues to display the information of next line.
<Ctrl+C>	Stops displaying and returns to the editing status of command line.
<PageUp>	Displays information of the previous page.
<PageDown>	Displays information of the next page.

3 System Status Command

3.1 Mode Description

Command Description

This chapter introduces how to enter and exit the different modes, including privileged mode, global mode, and interface mode. See Figure 2-1.

Parameter

None.

Command Mode

None.

Example

// Enter privileged mode, exit privileged mode.

```
username: admin
password: admin (hidden)
SWITCH#
SWITCH # exit
Press ENTER to get started
username:
```

// Enter global mode, exit global mode and return to privileged mode.

```
SWITCH # configure terminal
SWITCH (config) # exit
SWITCH#
```

// In global mode, enter G1/1 (Gigabit Ethernet 1/1) interface mode, exit interface mode and return to global mode.

```
SWITCH # configure terminal
SWITCH (config) # interface Gigabit Ethernet 1/1
SWITCH (config-if) # exit
SWITCH (config) #
```

// In global mode, enter VLAN 1 interface mode, exit VLAN 1 interface mode and return to global mode.

```
SWITCH (config) # interface vlan 1
SWITCH (config-if-vlan) #exit
SWITCH (config) #
```

3.2 System Information

3.2.1 Function Introduction

You can check the device name, software and hardware version, MAC address, compilation time, system operation time, and system current time in this module.

3.2.2 Show Version

Command Description

Show version is for checking version information including device name, software and hardware version, MAC address, compilation time, and system operation time.

Parameter

None.

Command Mode

Privileged mode.

Example

// Check version information.

Username: admin

Password: admin (The password is in the hidden status)

SWITCH # show version

3.2.3 Show Clock

Command Description

Show clock is for checking the current system time.

Parameter

None.

Command Mode

Privileged mode.

Example

// Check the current system time.

SWITCH# show clock
System Time: 2017-10-10T09:17:28+08:00

3.3 System Log

3.3.1 Function Introduction

You can check the system log information in this module, which is convenient for maintenance.

3.3.2 Show Logging

Command Description

Show logging <log_id> is for checking the log information of the exact serial number.

Show logging [informational] [notice] [warning] [error] is for checking the current log information of the switch.

Parameter

Table 3-1 Parameter

Parameter	Description
log_id	Check log information of the exact serial number. The value ranges from 1 through 4294967295.
informational	Check log information of informational.
notice	Check log information of notice.
warning	Check log information of warning.
error	Check log information of error

Command Mode

Privileged mode.

Example

// Check current log information of switch.

SWITCH # show logging

3.4 Port Statistics

3.4.1 Function Introduction

In the module of port statistics, you can check the packet quantity, number of bytes and error message quantity sent and received by the global port. It means that the working status of the port is weak when the number of error message is too big, then it needs to check the connected cable or if there is something wrong with the opposite device.

3.4.2 Show Interface

Command Description

Show interface (<port_type> [<in_port_list>]) switchport [access | trunk | hybrid], check the modes of all the ports.

Show interface (<port_type> [<v_port_type_list>]) capabilities, display the function which is provided by all ports.

Show interface (<port_type> [<v_port_type_list>]) status, check the status of all the ports.

Show interface (<port_type> [<v_port_type_list>]) veriphy, diagnose circuit and display results.

Show interface vlan [<vlist>], check the info of some VLAN.

Show interface (<port_type> [<v_port_type_list>]) statistics, check the statistics info of port message.

Parameter

Table 3-2 Parameter

Parameter	Description
port_type	Port type, value Gigabit Ethernet
in_port_list	Port number, it supports 1/1-8, 1/1, 1/1-2, 3, 5-8 and other forms.
v_port_type_list	
vlist	VLAN number

Command Mode

Privileged mode.

Example

// Check message statistics info of port 1.

SWITCH# show interface GigabitEthernet 1/1 statistics			
Rx Packets:	0	Tx Packets:	0
Rx Octets:	0	Tx Octets:	0
Rx Unicast:	0	Tx Unicast:	0
Rx Multicast:	0	Tx Multicast:	0

Rx Broadcast:	0	Tx Broadcast:	0
Rx Pause:	0	Tx Pause:	0
Rx 64:	0	Tx 64:	0
Rx 65-127:	0	Tx 65-127:	0
Rx 128-255:	0	Tx 128-255:	0
Rx 256-511:	0	Tx 256-511:	0
Rx 512-1023:	0	Tx 512-1023:	0
Rx 1024-1526:	0	Tx 1024-1526:	0
Rx 1527-:	0	Tx 1527-:	0
Rx Priority 0:	0	Tx Priority 0:	0
Rx Priority 1:	0	Tx Priority 1:	0
Rx Priority 2:	0	Tx Priority 2:	0
Rx Priority 3:	0	Tx Priority 3:	0
Rx Priority 4:	0	Tx Priority 4:	0
Rx Priority 5:	0	Tx Priority 5:	0
Rx Priority 6:	0	Tx Priority 6:	0
Rx Priority 7:	0	Tx Priority 7:	0
Rx Drops:	0	Tx Drops:	0
Rx CRC/Alignment:	0	Tx Late/Exc. Coll.:	0
Rx Undersize:	0		
Rx Oversize:	0		
Rx Fragments:	0		
Rx Jabbers:	0		
Rx Filtered:	0		

The common output info description of show interface command, please refer to Table 3-3 for more details.

Table 3-3 Show interface command

Parameter	Description
Rx Packets	Received data packet quantity statistics
Tx Packets	Sent data packet quantity statistics
Rx Unicast	Received unicast data statistics
Tx Unicast	Sent unicast data statistics
Rx Multicast	Received multicast data statistics
Tx Multicast	Sent multicast data statistics
Rx Broadcast	Received broadcast data statistics
Tx Broadcast	Sent broadcast statistics

Parameter	Description
Rx <64, 65-127, 128-255, 256-511, 512-1023, 1024-1526, 1527->	Received length or length range is 64, 65-127, 128-255, 256-511, 512-1023, 1024-1526, 1527 data packet quantity statistics.
Tx <64, 65-127, 128-255, 256-511, 512-1023, 1024-1526, 1527->	Sent length or length range is 64, 65-127, 128-255, 256-511, 512-1023, 1024-1526, 1527 data packet quantity statistics.
Rx Priority	Received data packet priority
Tx Priority	Sent data packet priority

3.5 Detail Statistics

3.5.1 Function Introduction

In this function module, you can inquire detailed working condition of each port, including receive/send message quantity, broadcast packet, error packets (include discarded message by the port, CRC (Cyclic Redundancy Check) error message, extremely short frame message, jumbo frame message and filtered message) and so on, which is convenient for network management personnel to maintain network.

3.5.2 Show Interface

Command Description

Show interface (<port_type> [<v_port_type_list>]) statistics [{ packets | bytes | errors | discards | filtered | { priority [<priority_v_0_to_7>] } }] [{ up | down }], check detailed statistics info of port message.

Parameter

Table 3-4 Parameter

Parameter	Parameter sub item	Description
	begin	<64, 65-127, 128-255, 256-511, 512-1023, 1024-1526, 1527->	It is to display the data packet statistics of all the bytes after the byte which has the key word.
	exclude	<64, 65-127, 128-255, 256-511, 512-1023, 1024-1526, 1527->	It is to display the data packet statistics of the bytes except those bytes which have key word.
	include	<64, 65-127, 128-255, 256-511, 512-1023, 1024-1526, 1527->	It is to display the data packet statistics which has key word.
packages	—	Check port packet statistics.
bytes	—	Check port data byte statistics.
errors/filtered	—	Check port error frame/filtered frame.

Parameter	Parameter sub item	Description
discards	—	Check discarded message quantity of port.
priority	—	Check port priority.
down/up	—	It is to check port status which is down or up.

Command Mode

Privileged mode.

Example

// Display data packet statistics from key word 5 (the data packet range includes number 5).

SWITCH# show interface Gigabit Ethernet 1/1 statistics | begin 5

// Display the data packet statistics except those have key word 4.

SWITCH# show interface Gigabit Ethernet 1/1 statistics | exclude 4

// Display the data packet statistics result of all bytes which include key word 5.

SWITCH# show interface Gigabit Ethernet 1/1 statistics | include 5

// Error frame statistics of port 1.

SWITCH# show interface Gigabit Ethernet 1/1 statistics errors

// Data packet statistics of port 1.

SWITCH# show interface Gigabit Ethernet 1/1 statistics packets

3.6 ACL Statistics

3.6.1 Function Introduction

In this function module, it can check the statistics info of each function module under switch ACL (Access Control List).

3.6.2 Show Access-List ACE-Status

Command Description

show access-list ace-status [static] [loop-protect] [dhcp] [ptp] [upnp] [arp-inspection] [ipmc] [ip-source-guard] [conflicts], check ACL rule info.

Parameter

Table 3-5 Parameter

Parameter	Description
static	Check the config which is manually added by users.
loop-protect	Check config module of loop protection.

Parameter	Description
dhcp	Check the config with DHCP (Dynamic Host Configuration Protocol) module.
ptp	Check PTP (Picture Transfer Protocol) module configuration.
upnp	Check general and agreement module configuration.
arp-inspection	Check ARP (Address Resolution Protocol) detection module configuration.
ipmc	Check IPMC module configuration.
ip-source-guard	Check source address protection module configuration.
conflicts	Check conflict rule caused by hardware restriction.

Command Mode

Privileged mode.

Example

// Check ACL rule info.

SWITCH# show access-list ace-status

3.7 STP Status

3.7.1 Function Introduction

In this function module, it can check STP (Spanning Tree Protocol) network bridge and port info, STP dynamic port, STP message statistics, STP configuration and STP summary info etc.

3.7.2 Show Spanning Tree

Command Description

show spanning-tree [summary | active | { interface (<port_type> [<v_port_type_list>]) } | { detailed [interface (<port_type> [<v_port_type_list_1>])] } | { mst [configuration | { <instance> [interface (<port_type> [<v_port_type_list_2>])] }] }], check spanning tree bridge status.

Parameter

Table 3-6 Parameter

Parameter	Description
<cr>	Check STP network bridge and port info.
summary	Check STP summary info.
active	Check STP dynamic port.
interface	Check STP status of some port.
detailed	Check STP message statistics.
mst	Check MSTP configuration.

Command Mode

Privileged mode.

Example

// Check spanning tree bridge status.

SWITCH # show spanning-tree

// Check STP status of port 4.

SWITCH # show spanning-tree interface Gigabit Ethernet 1/4

3.8 LLDP Neighbor

3.8.1 Function Introduction

In this module, it can check neighbor info, including opposite terminal port, system name, port instruction, system performance, management address and so on, or it can check LLDP (Link Layer Discovery Protocol) message statistics info.

3.8.2 Show LLDP

Command Description

Show lldp neighbors [interface (<port_type> [<v_port_type_list>])], check LLDP neighbor info.

Show lldp statistics [interface (<port_type> [<v_port_type_list>])], check LLDP message statistics info.

Parameter

Table 3-7 Parameter

Parameter	Parameter sub item	Description
neighbors	<cr>	Check LLDP neighbor info.
	interface	Check the learned neighbor info under exact port.
statistics	<cr>	Check LLDP message statistics.
	interface	Check LLDP message statistics under exact port.

Command Mode

Privileged mode.

Example

// Check LLDP neighbor info.

SWITCH #show lldp neighbors

3.9 Layer Two Forwarding Table

3.9.1 Function Introduction

In this module, it can check all layer two MAC address forwarding tables, types, ports, MAC addresses, VLAN info of the switch.

3.9.2 Show MAC Address Table

Command Description

show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>]) | vlan <v_vlan_id_2>] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])], check layer two forwarding table.

Parameter

Table 3-8 Parameter

Parameter	Description
<cr>	Check layer two forwarding table.
conf	Check the info of static layer two forwarding table added by users.
static	Check all the static MAC addresses.
aging-time	Check aging time of layer two forwarding table.
learning	Check layer two forwarding table status of each port. Auto: Auto study MAC address join layer two forwarding table. Disabled: Forbid learning MAC address. Secure: It is allowed to add static MAC items, dynamic learning is not allowed.
count	Check item statistics of layer two forwarding table.
interface	Check layer two forwarding table item of the exact port.
vlan	Check layer two forwarding table of some VLAN.
address	Check forwarding table info of exact MAC address.

Command Mode

Privileged mode.

Example

// Check layer two forwarding table

SWITCH#show mac address-table

// Check all static MAC addresses

SWITCH#show mac address-table static

4 System Setting Command

4.1 IP Configuration

IP configuration commands:

<u>Show ip interface brief</u>

<u>IPaddress</u>

4.1.1 Function Introduction

IP configuration module can add, modify or check port IP info of the switch.

4.1.2 Show Up Interface Brief

Command Description

Show IP interface [brief], check the port IP configuration, it can display corresponding IP info of network port, also it can display IP info of corresponding VLAN.

Parameter

None

Command Mode

Privileged mode.

Example

// Check IP info of port or VLAN.

SWITCH#show mac address-table

4.1.3 IP Address

Command Description

IP address {<address> <netmask> | dhcp}, modify switch management IP.

The switch management IP is 192.168.1.110/24 by default.

Parameter

Table 4-1 Parameter

Parameter	Description
address	IP address of VLAN port

Parameter	Description
netmask	Subnet mask
dhcp	Acquire IP info automatically

Command Mode

VLAN port mode.

Example

// Modify switch management IP

SWITCH#show mac address-table

SWITCH (config-if-vlan) # ip address 192.168.1.1 255.255.255.0

// Save configuration after IP is modified

SWITCH# copy running-config startup-config

4.2 Log Configuration

Log configuration commands

logging on

logging host

logging level

4.2.1 Function Introduction

The function module can upload switch log info to remote log server.

4.2.2 Logging On

Command Description

Logging on, enable log server mode.

No logging on, disable logging server mode.

Parameter

None

Command Mode

Global mode

Example

// Enable log server mode.

```
SWITCH (config) #logging on
```

// Disable logging server mode.

```
SWITCH (config) #no logging on
```

4.2.3 Logging Host

Command Description

Logging host {<ipv4_addr> | <domain_name>}, configure the IP address of log server.

Parameter

Table 4-2 Parameter

Parameter	Description
ipv4_addr	IP address of log server
domain_name	Domain name of log server

Command Mode

Global mode.

Example

// Configure IP address of log server.

```
SWITCH (config) #logging host 192.168.0.1
```

4.2.4 Logging Level

Command Description

Logging level {informational | notice | warning | error}, it is to configure and upload log level of log server.

Parameter

Table 4-3 Parameter

Parameter	Description
information	Prompt
notice	Notice
warning	Warning
error	Error

Command Mode

Global mode.

Example

// Configure and upload log level to log server

SWITCH (config) # logging level error

4.3 User Configuration

User configuration command

username name

show users

4.3.1 Function Introduction

In this function module, it can check, modify or add user info, which is to protect the switch configuration.

4.3.2 Username name

Command Description

Username {default-administrator | <input username>} privilege <priv> password {unencrypted <unencry_password> | encrypted <encry_password> | none}, it is to add a new user or modify the password of an old user, or modify the administration authority of an old user, or modify the password and administration authority of an old user.

No username <username>, it means deleting a user.

Parameter

Table 4-4 Parameter

Parameter	Description
input_username	Username
password	User password, include the following: Encrypted, the password is encrypted Unencrypted, the password is not encrypted. 📖 The password can be set from 8 to 32 characters, which consists of at least two types of number, letter and special character (Except ""、 """、 ";"、 ":" and "&").
priv	User level, legal value is 0~15 (0 means lowest administration authority, 15 means highest administration authority).

Command Mode

Global mode.

Example

// Add new test user, password is test1234. It is the highest administration authority; password is not encrypted.

`SWITCH (config) # username test privilege 15 password unencrypted test1234`

// Delete test user.

`SWITCH (config) #no username test`

4.3.3 Show Users

Command Description

Show users, check current all user configuration info of the switch.

Parameter

None.

Command Mode

Privileged mode.

Example

// Check configuration info of all current users.

`SWITCH # show users`

4.4 NTP Configuration

User configuration command

[ntp](#)

[ntp server](#)

4.4.1 Function Introduction

It can auto synchronize network time after the function is enabled.

4.4.2 NTP

Command Description

NTP, enable NTP (Network Time Protocol) service.

No NTP, disable NTP service.

Parameter

None.

Command Mode

Global mode.

Example

// Enable NTP service.

SWITCH (config) # ntp

4.4.3 NTP Server

Command Description

NTP server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }, it is to add the IP address of NTP server.

Parameter

Table 4-5 Parameter

Parameter	Description
index_var	Value range 1–5
ipv4_var	IPv4 address
ipv6_var	IPv6 address
name_var	Domain name

Command Mode

Global mode.

Example

// Set IP address of NTP server.

SWITCH (config)# ntp server 1 ip-address 202.120.2.101

5 Port Configuration Command

5.1 Port Configuration

Port configuration commands:

[duplex](#)

[speed](#)

[flowcontrol](#)

[mtu](#)

[shutdown](#)

5.1.1 Function Introduction

In this module, it can configure related basic parameters of switch port. The port basic parameter will directly influence the working mode of the port.

5.1.2 Duplex

Command Description

Duplex {auto | full | half}, it is to set the duplex mode of the port. Several ports can be configured at the same time.

The duplex mode of port is auto by default.

⚠️

Please do not modify port rate mode randomly if there is no special requirements, mismatched negotiation will affect normal communication of the port.

Parameter

Table 5-1 Parameter

Parameter	Description
auto	Auto negotiation
full	Full duplex
half	Half duplex

Command Mode

Port mode.

Example

// Modify duplex mode of G1-G3 port.

SWITCH (config) # interface Gigabit Ethernet 1/1-3

SWITCH (config-if) # duplex full	

// Restore default duplex mode of G1-G3 port.

SWITCH (config-if) # no duplex	

// Modify duplex mode of G4 port.

SWITCH (config) # interface Gigabit Ethernet 1/4	
SWITCH (config-if) # duplex full	

// Restore default duplex mode of G4 port.

SWITCH (config-if) # no duplex	

5.1.3 Speed

Command Description

RJ-45 port: speed {10 | 100 | 1000 | auto}, it is to set the rate of RJ 45 port.

Optical port: speed {100 | 1000 | auto}, it is to set the rate of optical port.

The speed rate of RJ 45 port and optical port are both auto by default.

Parameter

Table 5-2 Parameter

Parameter		Description
RJ-45 port	10 | 100 | 1000	It is to set port speed rate 10 M, 100 M, 1000 M
	auto	It is to set port rate auto negotiation
Optical port	100 | 1000	It is to set optical port rate 100 M (full), 1000 M (full)
	auto	It is to set optical port rate auto negotiation

Command Mode

Port mode.

Example

// Set speed rate of G1 port as megabit.

SWITCH (config)# interface Gigabit Ethernet 1/1
SWITCH (config-if)# speed 100

5.1.4 Flow Control

Command Description

Flowcontrol {on | off}, enable, disable port flow control function.

Flow control function is enabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable the flow control function of port 1.

SWITCH (config) # interface Gigabit Ethernet 1/1

SWITCH (config-if) # flowcontrol on

// Disable the flow control function of port 1.

SWITCH (config-if) # flowcontrol off

5.1.5 MTU

Command Description

mtu <max_length>, set MTU (Maximum Transmission Unit) value, which is the max length frame allowed by port.

MTU value is 9600 by default.

Parameter

max_length, MTU value,   range 1518–9600.

Command Mode

Port mode.

Example

// Set MTU value.

SWITCH (config)# interface Gigabit Ethernet 1/1

SWITCH (config-if)# mtu 1518

5.1.6 Shutdown

Command Description

Shutdown, a command used to disable the port.

No shutdown, command used to enable the port.

The port is enabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable port 1.

SWITCH (config)# interface Gigabit Ethernet 1/1

SWITCH (config-if)# no shutdown

5.2 Port Mirror

Port mirror command:

monitor session destination

monitor session source

5.2.1 Function Introduction

Port mirror is called port monitoring as well. Port monitoring is a type of data packet acquisition technology, which can realize copying the data packet of one/several ports (mirror source port) to one specific port (mirror destination port) via configuring switch. The mirror destination port is connected with a host of data packet analysis software, which is to make analysis upon the collected data packet and it is to realize the purpose of network monitoring and excluding network failure.

5.2.2 Monitor Session Destination

Command Description

Monitor session <session_number> [destination interface (<port_type> [<di_list>])], it is to

Configure mirror destination interface.

no monitor session <session_number> [destination interface (<port_type> [<di_list>])], mirror destination interface is prohibited to use.

Parameter

Table 5-3 Parameter

Parameter	Description
session_number	Range 1–5
port_type	Mirror destination interface

Parameter	Description
di_list	Port number

Command Mode

Global mode.

Example

// Configure the mirror destination port as port 1.

SWITCH(config)# monitor session 1 destination interface Gigabit Ethernet 1/1

// Forbidden mirror destination port 1.

SWITCH(config)# no monitor session 1 destination interface Gigabit Ethernet 1/1

5.2.3 Monitor Session Source

Command Description

monitor session <session_number> [source { interface (<port_type> [<si_list>]) [both | rx | tx] | cpu [both | rx | tx] }], it is to configure mirror source port and mirror direction.

no monitor session <session_number> [source { interface (<port_type> [<si_list>]) [both | rx | tx] | cpu [both | rx | tx] }], forbidden mirror source port and mirror direction.

Parameter

Table 5-4 Parameter

Parameter	Description
session_number	Range 1–5
port_type	Mirror Source Port
si_list	Port Number
both	Mirror the data of source port enter and exit direction to the destination port.
rx	Mirror the data of source port enter direction to the destination port.
tx	Mirror the data of source port exit direction to destination port.

Command Mode

Global mode.

Example

// Configure the mirroring of source port 2 exit and entrance direction to destination port.

SWITCH(config)# monitor session 1 source interface GigabitEthernet 1/2 both

// Prohibited to mirror source port 2 exit and entrance direction to destination port.

SWITCH(config)# no monitor session 1 source interface GigabitEthernet 1/2 both

5.3 Bandwidth Strategy

Bandwidth strategy command:

access-list rate-limiter

5.3.1 Function Introduction

It can configure the speed limit strategy of the port, it can restrict the rate of all data packet entering and exiting the port.

5.3.2 Access-list rate-limiter

Command Description

Access-list rate-limiter [<rate_limiter_list>] {pps <pps_rate> | 100kbps <kpbs100_rate>}, it is to configure ACL bandwidth limit strategy, and set corresponding rate limit value of each ID (The command is matched with rate ID of the port).

Parameter

Table 5-5 Parameter

Parameter	Description
rate_limiter_list	Rate limit ID group, range 1–16
pps_rate	Rate value: <0–3276700>
kpbs100_rate	Rate value: <0–10000>

Command Mode

Global mode.

Example

// Configure the limit value of ID 4 which is 100000 pps.

SWITCH (config) # access-list rate-limiter 4 pps 100000

6 Advanced Configuration Command

6.1 Link Aggregation

Static aggregation configuration command:

[aggregation mode](#)

[aggregation group](#)

6.1.1 Function Introduction

Link aggregation is to form several physical ports of the switch to one logic port, several links which belong to the same convergence group can be considered as logic link with bigger bandwidth.

Link aggregation can realize communication flow can be distributed among each member port during the aggregation group, which is to increase bandwidth. Meanwhile, each member port makes dynamic backup mutually within the same aggregation group, which is to improve the link reliability.

The member port which belongs to the same aggregation group has to own the corresponding configuration, these configurations mainly includes STP, QoS, VLAN port attribute, MAC address learning, ERPS configuration, loop Protect configuration, mirror, 801.1x, IP filter, Mac filter and port segregation etc.

6.1.2 Aggregation Mode

Command Description

aggregation mode { [smac] [dmac] [ip] [port] }, it is to configure aggregation load balancing algorithm.

No aggregation mode, it is to cancel the configuration of aggregation load balancing algorithm.

Parameter

Table 6-1 Parameter

Parameter	Description
smac	Load balancing mode is based on source mac address.
dmac	Load balancing mode is based on destination mac address.
ip	Load balancing mode is based on IP address.
smac dmac	Load balancing mode is based on source & destination mac address.
port	Load balancing mode is based on tcp/udp port number.

Command Mode

Global mode.

Example

SWITCH(config)# aggregation mode smac dmac

6.1.3 Manual Aggregation

Command Description

Aggregation group <v_uint>, configuration port is added into convergence group.

No aggregation group, delete static convergence configuration of designated group.

Parameter

v_uint, aggregation group ID

Command Mode

Port mode.

Example

// Port 1–8 added to aggregation group 2.

SWITCH(config)# interface GigabitEthernet 1/1-8

SWITCH(config-if)# aggregation group 2 mode on

// Delete aggregation group.

SWITCH(config-if)# no aggregation group

6.1.4 Link Aggregation Example

Networking Requirement

Use link aggregation to increase device cascading port bandwidth and realize the load sharing which is based on source MAC.

As it is shown in Figure 6-1, switch SW1 G1 port and switch SW2 G1 port are connected, meanwhile the switch SW! G2 port is connected to SW2 G2 port. These two physical links are required to be aggregated as one logic link.

Figure 6-1 Networking
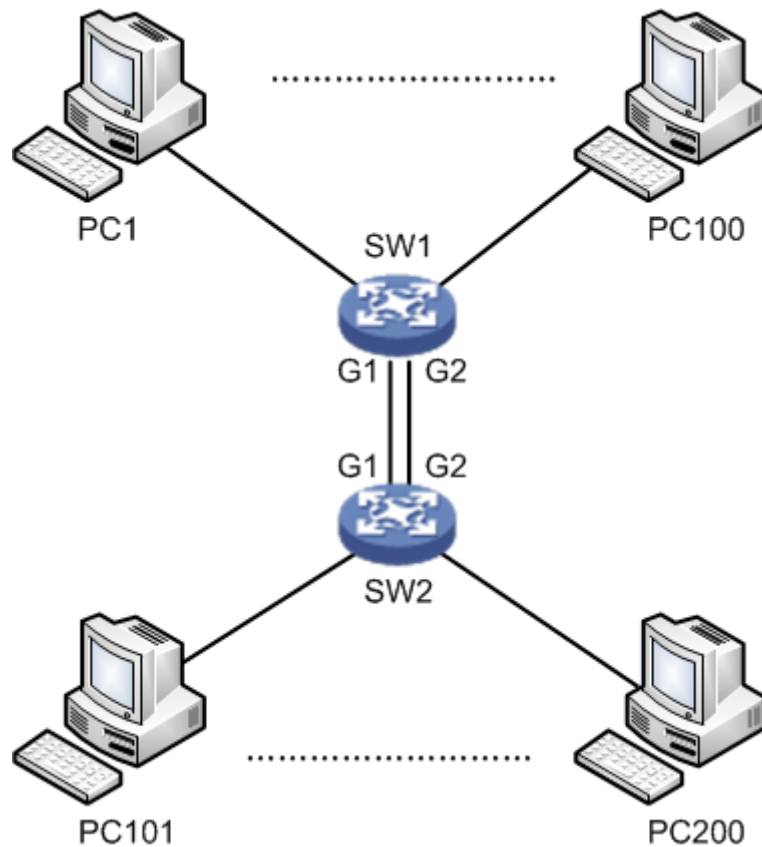
Configuration Example

SW1/SW2 configuration shown as follows.

```
SWITCH# configure terminal
SWITCH(config)# aggregation mode smac dmac
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# aggregation group 1
SWITCH(config-if)# exit
SWITCH(config)# interface GigabitEthernet 1/2
SWITCH(config-if)# aggregation group 1
```

Result Verification

Two links are formed as one logic link after aggregation, and bandwidth is doubled. Besides, it is to implement load sharing according to source or destination MAC. The data will take other links of the aggregation group when there is one link is cut off, which will not interrupt communication.

6.2 VLAN Management

VLAN configuration command:

vlan

name

6.2.1 Function Introduction

Ethernet is a type of shared communication media which is based on CSMA/CD. It adopts Ethernet technology to build LAN, which is not only a conflict area but also a broadcast area. It will cause serious conflict, broadcast overflow and performance decrease, even network failure when there are too many hosts in the network. It can solve conflict via deploying Network Bridge or layer-two switch in the Ethernet, however, it still fails to segregate broadcast packet. Then VLAN technology shows up, this technology is able to divide one physical LAN into several logical LAN-VLAN. The hosts which are in the same VLAN can be directly interacted while the hosts which are not in the different VLAN fail to be directly interacted. Thus, broadcast packet is restricted in the same VLAN, which means that each VLAN is a broadcast domain.

The advantages of VLAN are shown as follows:
- Improve network performance. The broadcast packet is restricted within the VLAN, which is to effectively control network broadcast storm, save network bandwidth and enhance network processing power.
- Enhance network security. Devices with different VLAN cannot be mutually accessed, hosts with different VLAN cannot be directly communicated, it needs to transmit layer-three packet via router or layer-three switch and some other network devices.
- Simplify network management. The hosts in the same virtual work group cannot be restricted in some certain physical range, it simplifies network management and makes it convenient for people in different areas to build work group.

6.2.2 VLAN

Command Description

vlan <vlist>, used to add new VLAN.

No vlan, used to delete VLAN.

All ports belong to VLAN 1 by default.

Parameter

<vlist>, VLAN ID, allowed range 1–4095, 4095 reserved, for actual configuration, it uses 1–4094.

Command Mode

Global mode.

Example

// Newly add 4 vlan, which is vlan 2, vlan 3, vlan 6, and vlan 9 respectively.

SWITCH(config)#vlan 2-3,6,9

// Delete vlan 6 and vlan 9.

SWITCH(config)#no vlan 6,9

6.2.3 Name

Command Description

name <vlan_name>, configure VLAN name.

Parameter

vlan_name, it is the name description of VLAN.

Command Mode

VLAN configuration mode.

Example

// Configure vlan 2 name as test123.

SWITCH(config)# vlan 2

SWITCH(config-vlan)# name test123

6.2.4 Switch Port Mode

Command Description

Switch port mode {access | trunk | hybrid}, it is to configure the switch port mode.

The switch port mode is access by default.

Parameter

Table 6-2 Parameter

Parameter	Description
access	Access mode, it means that the port only belongs to a VLAN, besides, it only sends and receive Ethernet frame without label.

Parameter	Description
trunk	Trunk mode, it means that the port is connected with other switches. And it can send and receive Ethernet frame with label.
hybrid	Hybrid mode, it means that the port can not only connect to computer, but also connect to switch and router (it is the collection of access mode and trunk mode).

Command Mode

Port mode.

Example

// Configure switch port 2, 3, 4 mode as access.

SWITCH(config)# interface GigabitEthernet 1/2-4

SWITCH(config-if)#switchport mode access

// Configure switch port 1 mode as trunk.

SWITCH(config)# interface GigabitEthernet 1/1

SWITCH(config-if)#switchport mode trunk

6.2.5 Switch Port Access VLAN

Command Description

Switch port access vlan <pvid>, add the port into VLAN.

The port is added into VLAN 1 by default.

Parameter

Pvid, VLAN number, value range is 1–4094.

Command Mode

Port mode.

Example

// Create vlan 2.

SWITCH(config)#vlan 2

// Port 5–8 added into vlan 2.

SWITCH(config)# interface GigabitEthernet 1/5-8

SWITCH(config-if)#switchport mode access

SWITCH(config-if)#switchport access vlan 2

6.2.6 Switch Port Forbidden VLAN

Command Description

Switch port forbidden vlan {add | remove} <vlan_list>, it is to configure the port forbidden VLAN number.

Parameter

Table 6-3 Parameter

Parameter	Description
add	It is to add port forbidden VLAN number
remove	It is to remove port forbidden VLAN number
vlan_list	VLAN number

Command Mode

Port mode.

Example

// Port one is forbidden to add into vlan 3.

SWITCH(config)# interface GigabitEthernet 1/1

SWITCH(config-if)# switchport forbidden vlan add 3

6.2.7 Switch port hybrid acceptable-frame-type

Command Description

Switch port hybrid acceptable-frame-type {all | tagged | untagged}, it is to configure

It is to configure frame type which is to be received by hybrid port.

The frame type which can be received by hybrid port is all by default.

Parameter

Table 6-4 Parameter

Parameter	Description
all	It means that the frame type which can be received by hybrid port is all frame.
tagged	It means that the frame type which can be received by hybrid port is tag frame.
untagged	It means that the frame type which can be received by hybrid port is untagged frame.

Command Mode

Port mode.

Example

// Hybrid port allows to receive all frames.

SWITCH(config)# interface GigabitEthernet 1/1

SWITCH(config-if)# switchport hybrid acceptable-frame-type all

6.2.8 Switch port hybrid egress-tag

Command Description

Switch port hybrid egress-tag {none | all}, it is to configure the tag attribute of egress port.

No switch port hybrid egress-tag, it is to restore data egress port tag attribute as default configuration.

Data egress port attribute is untag port VLAN by default.

Parameter

Table 6-5 Parameter

Parameter	Description
all	It means data egress port is tag attribute
none	It means data egress port is untag attribute

Command Mode

Port mode.

Example

// Configure data egress port 5 tag attribute.

SWITCH (config)# interface Gigabit Ethernet 1/5

SWITCH (config-if)# switch port hybrid egress-tag all

// Restore data egress port tag attribute as default configuration.

SWITCH (config-if)# no switch port hybrid egress-tag

6.2.9 Switch port hybrid native

Command Description

Switch port hybrid native vlan <pvid>, it is to configure the local VLAN of hybrid port.

Parameter

Pvid, VLAN number, value range 1–4094.

Command Mode

Port mode.

Example

// Configure local VLAN of hybrid port 5 as VLAN 2.

SWITCH(config)# interface Gigabit Ethernet 1/5

SWITCH(config-if)# switch port hybrid native vlan 2

6.2.10 Switch port trunk allowed

Command Description

Switch port trunk allowed vlan {all | none | [add | remove | except]<vlan_list>}, it is to configure VLAN number which is allowed to pass by trunk port.

Parameter

vlan_list, VLAN number, value range is 1–4094.

Command Mode

Port mode.

Example

// Configure that trunk port allows VLAN 3 to pass.

SWITCH(config)# interface GigabitEthernet 1/1

SWITCH(config-if)# switchport trunk allowed vlan 3

6.2.11 Show VLAN

Command Description

Show vlan [id <vlan_list> | name <name> | brief] [all], check corresponding VLAN configuration via VLAN ID or VLAN name, and check VLAN total configuration information.

Show vlan ip-subnet [<ipv4>], check VLAN item based on IP subnet.

Show vlan mac [address <mac_addr>], check VLAN item of MAC address.

show vlan protocol, check VLAN status based on each protocol.

show vlan status [interface (<port_type> [<plist>])] [admin | all | combined | conflicts | erps | evc | gvrp | mep | mstp | mvr | nas | rmirror | vcl | voice-vlan], check VLAN configuration of each port.

Parameter

Table 6-6 Parameter

Parameter	Description
vlan_list	VLAN number
name	VLAN name
ipv4	IP and subnet mask, format is "IP address/ subnet mask", for example, "172.8.4.1/255.255.0.0"
mac_addr	MAC address
port_type	Port type
plist	Port number

Command Mode

Privileged mode.

Example

// Check configuration information of vlan 2.

SWITCH# show vlan id 2

// Check VLAN total configuration information.

SWITCH# show vlan brief

// Check VLAN configuration of each port.

SWITCH# show vlan status

6.2.12 VLAN Management Example

Networking Requirement

As it is shown in Figure 6-2, it is to realize VLAN communication of switch, which is PC1 (192.168.222.107) and PC2 (192.168.222.94) can have access normally.

Figure 6-2 Networking

SW1 G1 — G1 SW2
G2 — trunk — G2
vlan2 — vlan2
PC1 192.168.222.107 — PC2 192.168.222.94
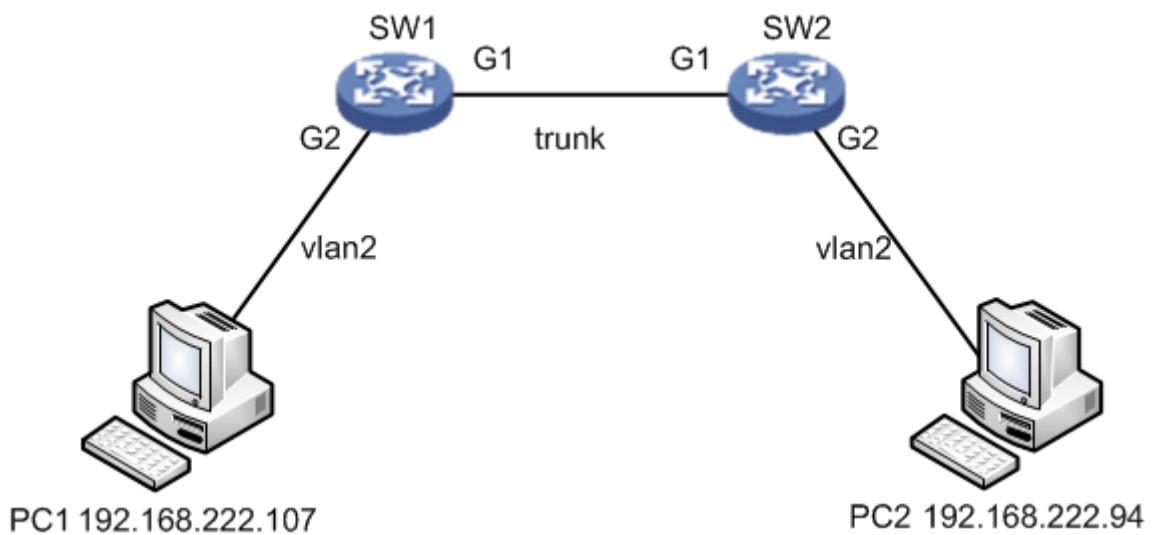
Configuration Example

// Configure SW1 port 1 and port 2 mode.

```
SWITCH# configure terminal
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# switchport mode trunk
SWITCH(config-if)# switchport trunk allowed vlan 1-2
SWITCH(config-if)# exit
SWITCH(config)# interface GigabitEthernet 1/2
SWITCH(config-if)# switchport mode access
SWITCH(config-if)# switchport access vlan 2
```

// Configure SW2 port 1 and port 2 mode.

As it is similar to SW1, so the description is omitted here.

Result Verification

pc1 (192.168.222.107) and pc2 (192.168.222.94) can ping mutually.

6.2.13 Link Aggregation Unvarnished Transmission VLAN Management Example

Networking Requirement

As it is shown in Figure 6-3, it is to realize VLAN communication of switch, which means that PC1 (192.168.222.107) and PC2 (192.168.222.94) can have access normally, PC 3(192.168.222.5) and PC4 (192.168.222.6) can have access normally. Besides, the G1 port of switch SW1 is connected to G1 port of switch SW2, meanwhile G2 port of switch SW1 is connected to G2 port of SW2. It is required to aggregate these two physical links as one logic link.

Figure 6-3 Networking
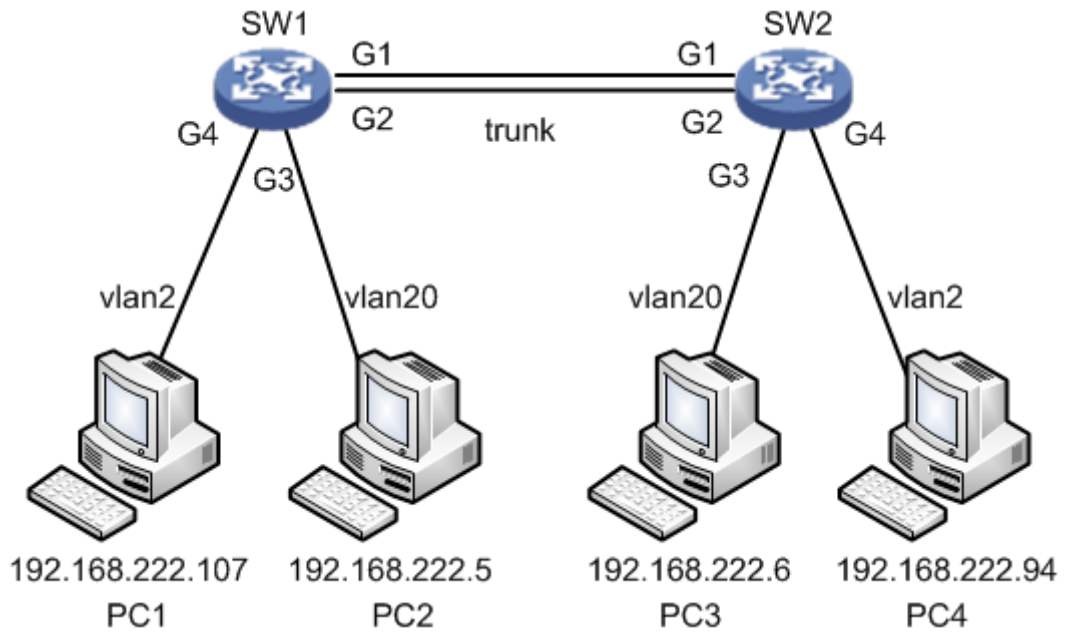
Configuration Example

// Configure SW1 port 1, port 3, and port 4 mode.

```
SWITCH# configure terminal
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# switchport mode trunk
SWITCH(config-if)# switchport trunk allowed vlan 1,2,20
SWITCH(config-if)# exit
SWITCH(config)# interface GigabitEthernet 1/2
SWITCH(config-if)# switchport mode trunk
SWITCH(config-if)# switchport trunk allowed vlan 1,2,20
SWITCH(config-if)# exit
SWITCH(config)# interface GigabitEthernet 1/3
SWITCH(config-if)# switchport mode access
SWITCH(config-if)# switchport access vlan 20
SWITCH(config-if)# exit
SWITCH(config)# interface GigabitEthernet 1/4
SWITCH(config-if)# switchport mode access
SWITCH(config-if)# switchport access vlan 2
```

// Configure SW1 link aggregation.

```
SWITCH# configure terminal
SWITCH(config)# aggregation mode smac dmac
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# aggregation group 1 mode
SWITCH(config-if)# exit
```

```
SWITCH(config)# interface GigabitEthernet 1/2
SWITCH(config-if)# aggregation group 1 mode
```

// Configure SW2 port 1 and port 2 mode.

It is similar to SW1, so the description is omitted.

// Configure SW2 link aggregation.

It is similar to SW1, so the description is omitted here.

Result Verification

pc1 (192.168.222.107) and pc4 (192.168.222.94) can ping mutually. Besides, two links are formed into one logic link after aggregation, double the bandwidth and it makes load distribution according to source or destination MAC. The data will be transmitted via other links of the aggregation group when one link in the aggregation group is cut off, besides it will not cause communication interruption.

6.3 VCL Configuration

VCL configuration commands:

[switchport vlan mac](#)

[switchport vlan ip-subnet](#)

[switchport vlan protocol](#)

[vlan protocol](#)

6.3.1 Function Introduction

The module can divide VLAN based on MAC address, divide VLAN based on subnet mask and divide VLAN based on protocol. It can use different technologies according to different network work requirement.

📖

- VCL needs to use together with VLAN based on port.
- VCL priority: VLAN based on MAC > VLAN based on subnet mask > VLAN based on protocol.

6.3.2 Switch Port VLAN MAC

Command Description

Switch port vlan mac <mac_addr> vlan <vid>, configure VLAN division based on MAC.

No switchport vlan mac <mac_addr> vlan <vid>, cancel the configuration of VLAN division based on MAC.

Parameter

Table 6-7 Parameter

Parameter	Description
mac_addr	48 bit MAC address, format is xx:xx:xx:xx:xx:xx
vid	VLAN number

Command Mode

Port mode.

Example

// Configure G1/3 port which belongs to vlan2.

SWITCH(config)# interface GigabitEthernet 1/3

SWITCH(config-if)# switchport mode access

SWITCH(config-if)# switchport access vlan 2

// Label the data frame with vlan 2, which is to enter G1/3 port with the MAC address of

00:00:00:00:00:01.

SWITCH(config)# interface GigabitEthernet 1/3

SWITCH(config-if)# switchport vlan mac 00:00:00:00:00:01 vlan 2

// Cancel the configuration of division based on MAC.

SWITCH(config-if)# no switchport vlan mac 00:00:00:00:00:01 vlan 2

6.3.3 Switch Port VLAN IP-Subnet

Command Description

switchport vlan ip-subnet [id <1-128>] <ipv4> vlan <vid>, configure VLAN based on subnet mask.

no switchport vlan ip-subnet [id <1-128>] <ipv4> vlan <vid>, delete the config of VLAN based on ip-subnet.

Parameter

Table 6-8 Parameter

Parameter	Description
ipv4	IP address and subnet mask
vid	VLAN number

Command Mode

Port mode.

Example

// Configure port 4 belongs to vlan 2.

SWITCH(config)# interface GigabitEthernet 1/4

SWITCH(config-if)# switchport mode access

SWITCH(config-if)# switchport access vlan 2

// Place label on IP of 192.168.4.0/24 network segment which is to enter port 4.

SWITCH(config)# interface GigabitEthernet 1/4

SWITCH(config-if)# switchport vlan ip-subnet id 1 192.168.4.0/255.255.255.0 vlan 2

// Delete config of VLAN based on ip-subnet.

SWITCH(config-if)# no switchport vlan ip-subnet 192.168.4.0/255.255.255.0

6.3.4 Switch Port VLAN Protocol

Command Description

Switchport vlan protocol group <grp_id> vlan <vid>, configure group name and map to VLAN.

No switchport vlan protocol group <grp_id> vlan <vid>, cancel group name mapping to VLAN.

Parameter

Table 6-9 Parameter

Parameter	Description
grp_id	Group Name
vid	VLAN Number

Command Mode

Port mode.

Example

// Config port 6 belongs to vlan 2

SWITCH(config)# interface GigabitEthernet 1/6

SWITCH(config-if)# switchport mode access

SWITCH(config-if)# switchport access vlan 2

// Place the label of VLAN 2 on the data frame of protocol group from port 6

SWITCH(config)# interface GigabitEthernet 1/6

SWITCH(config-if)# switchport vlan protocol group test vlan 2

// Cancel placing label VLAN 2 on the data frame from protocol group test

SWITCH(config-if)# no switchport vlan protocol group test vlan 2

6.3.5 VLAN Protocol

Command Description

vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } |

{ llc <dsap> <ssap> } } group <grp_id>, configure protocol to group mapping

no vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>, cancel config of mapping from protocol to group.

Parameter

Table 6-10 Parameter

Parameter	Description
etype	Value range 0x600–0xFFFF
oui	Value range 0x000000–0XFFFFFF
pid	Value range 0x0–0xFFFF
dsap	Value range 0x00–0xFF
ssap	Value range 0x00–0xFF
grp_id	Protocol group name

Command Mode

Global mode.

Example

// Add protocol snap 0xE02B 0x1 data frame to protocol group test.

SWITCH(config)# vlan protocol snap 0xE02B 0x1 group test

// Cancel adding protocol snap 0xE02B 0x1 data frame to protocol group test.

SWITCH(config)# no vlan protocol snap 0xE02B 0x1 group test

6.3.6 VCL Configuration Example

6.3.6.1 VLAN Partition Based on MAC

Networking Requirement

It is to realize mutual communication between PC1 (192.168.1.1) and PC2 (192.168.1.2) in VLAN 2 via VLAN configuration based on MAC address. But it fails to communicate in other VLAN.

Add MAC addresses of both PC1 and PC2 to VLAN 2, in the VLAN based on port, add port 1 and port 2 to VLAN 2, which is shown in Figure 6-4.

Figure 6-4 Networking
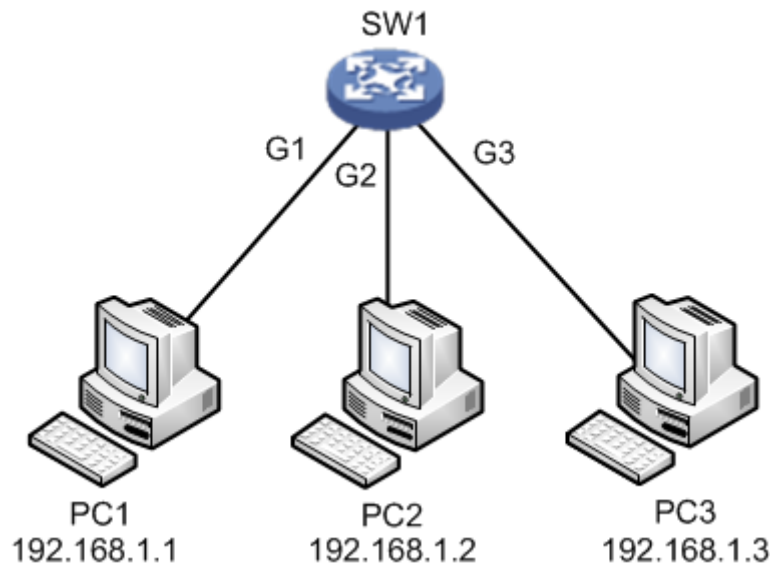
Configuration Example

```
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# switchport mode access
SWITCH(config-if)# switchport access vlan 2
SWITCH(config-if)# switchport vlan mac 00-00-00-00-00-01 vlan 2
SWITCH(config-if)# switchport vlan mac 00-00-00-00-00-02 vlan 2
SWITCH(config-if)#exit
SWITCH(config)# interface GigabitEthernet 1/2
SWITCH(config-if)# switchport mode access
SWITCH(config-if)# switchport access vlan 2
SWITCH(config-if)# switchport vlan mac 00-00-00-00-00-01 vlan 2
SWITCH(config-if)# switchport vlan mac 00-00-00-00-00-02 vlan 2
```

Result Verification

PC1 (192.168.1.1) ping PC2 (192.168.1.2) normal communication.

PC1 (192.168.1.1) ping PC3 (192.168.1.3) fails to communicate.

6.3.6.2 VLAN Partition Based on Subnet Mask

Networking Requirement

As it is shown in Figure 6-5, PC1 (192.168.222.64), PC2 (192.168.222.128) and PC3 (192.168.222.2) are the PC which connects to the port of G1, G2 and G3. These three ports all belong to vlan 2 in the VLAN based on port. It is to realize mutual ping between PC1 and PC2 via VLAN based on subnet mask, PC3 ping fails to ping PC1 or PC2.

Figure 6-5 Networking
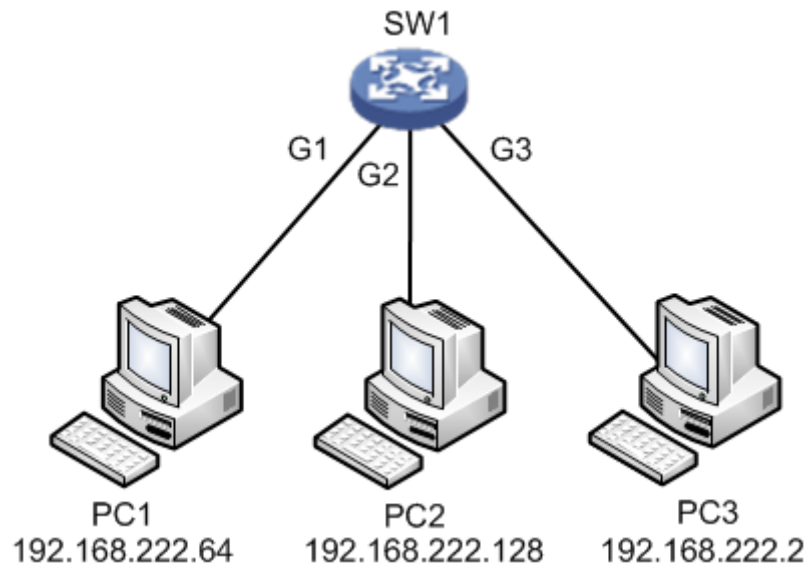
Configuration Example

```
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# switchport mode access
SWITCH(config-if)# switchport access vlan 2
SWITCH(config-if)#switchport vlan ip-subnet id 1 192.168.222.1/255.255.255.192 vlan 2
SWITCH(config-if)#exit
SWITCH(config)# interface GigabitEthernet 1/2
SWITCH(config-if)# switchport mode access
SWITCH(config-if)# switchport access vlan 2
SWITCH(config-if)#switchport vlan ip-subnet id 1 192.168.222.1/255.255.255.192 vlan 2
```

Result Verification

PC1 (192.168.222.64) ping PC2 (192.168.222.128) normal communication.

PC1 (192.168.222.64) ping PC3 (192.168.222.2) fails to communicate.

6.3.6.3 Protocol Maps Group Name and Then Maps to VLAN

Networking Requirement

As it is shown in Figure 6-6, PC1 is the PC which connects to the G1 port of switch. It is to make IP protocol transmits in vlan 2 via VLAN configuration based on protocol, and it fails to transmit in other VLAN.

Figure 6-6 Networking
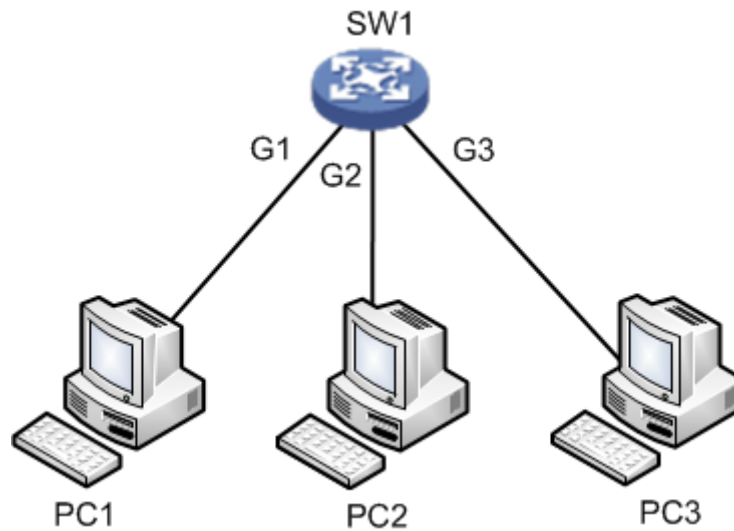
Configuration Example

// Configure G1 port belong to vlan 2 in the VLAN based on port.

// Configure protocol map to group name.

// Configure group name map to VLAN.

```
SWITCH(config)#vlan protocol eth2 ip group ip
SWITCH(config) #interface GigabitEthernet 1/1
SWITCH(config-if) #switchport mode access
SWITCH(config-if) #switchport access vlan 2
SWITCH(config-if) #switchport vlan protocol group ip vlan 2
```

Result Verification

After configuration is completed, PC1 uses vlan2 port IP to visit switch WEB interface; if make G1 port belong to vlan1 in the vlan based on port, then PC1 fails to use vlan1 port IP to visit switch WEB interface.

6.4 DHCP Snooping

DHCP Snooping configuration commands:

ip igmp snooping

ip dhcp snooping trust

show ip dhcp snooping table

show ip dhcp snooping interface

6.4.1 Function Introduction

DHCP Snooping is a kind of security feature; it guarantees that client can acquire IP address from legal server, if an illegal DHCP server is installed in the network, it may cause the DHCP client to obtain wrong IP address and network configuration parameters, and thus it is unable to

communicate properly. In order to enable DHCP client to obtain IP address via legal DHCP server, DHCP Snooping security mechanism allows ports to be set as trust port and untrusted port.

- Trusted ports normally transmit the received DHCP packets.
- After untrusted ports receiving DHCP-ACK and DHCP-OFFER packets responded from DHCP server, then discard the packets.

6.4.2 IP DHCP Snooping

Command Description

IP dhcp snooping, enable DHCP snooping configuration mode.

No ip dhcp snooping, disable DHCP snooping configuration mode.

DHCP snooping configuration mode is in the disabled status by default.

Parameter

None.

Command Mode

Global mode.

Example

// Enable DHCP snooping configuration mode.

SWITCH(config)# ip dhcp snooping

// Disable DHCP snooping configuration mode.

SWITCH(config)# no ip dhcp snooping

6.4.3 IP DHCP Snooping Trust

Command Description

IP dhcp snooping trust, enable port DHCP snooping trust mode.

No IP dhcp snooping trust, disable port DHCP snooping trust mode.

Port DHCP snooping trust mode is in the enable status by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable port DHCP snooping trust mode.

SWITCH(config)# interface Gigabit Ethernet 1/1

SWITCH(config-if)# ip dhcp snooping trust

// Disable port DHCP snooping trust mode.

SWITCH(config-if)# no ip dhcp snooping trust

6.4.4 Show IP DHCP Snooping Table

Command Description

Show IP dhcp snooping table, check DHCP dynamic snooping information table.

Parameter

None.

Command Mode

Privileged mode.

Example

// Check DHCP dynamic snooping information table.

SWITCH# show ip dhcp snooping table

6.4.5 Show IP DHCP Snooping Interface

Command Description

Show ip dhcp snooping [interface (<port_type> [<in_port_list>])], check port DHCP snooping trust mode.

Parameter

Table 6-11 Parameter

Parameter	Description
port_type	Port type
in_port_list	Port No.

Command Mode

Privileged mode.

Example

// Check DHCP snooping trust mode of port 1.

SWITCH# show ip dhcp snooping interface Gigabit Ethernet 1/1

6.4.6 Snooping Example

Networking Requirement

It only allows the client to acquire IP info from DHCP server which is connected to G1 port; it is not allowed to acquire info from other server which is connected to G2 port, which is shown in Figure 6-7.

Figure 6-7 Networking
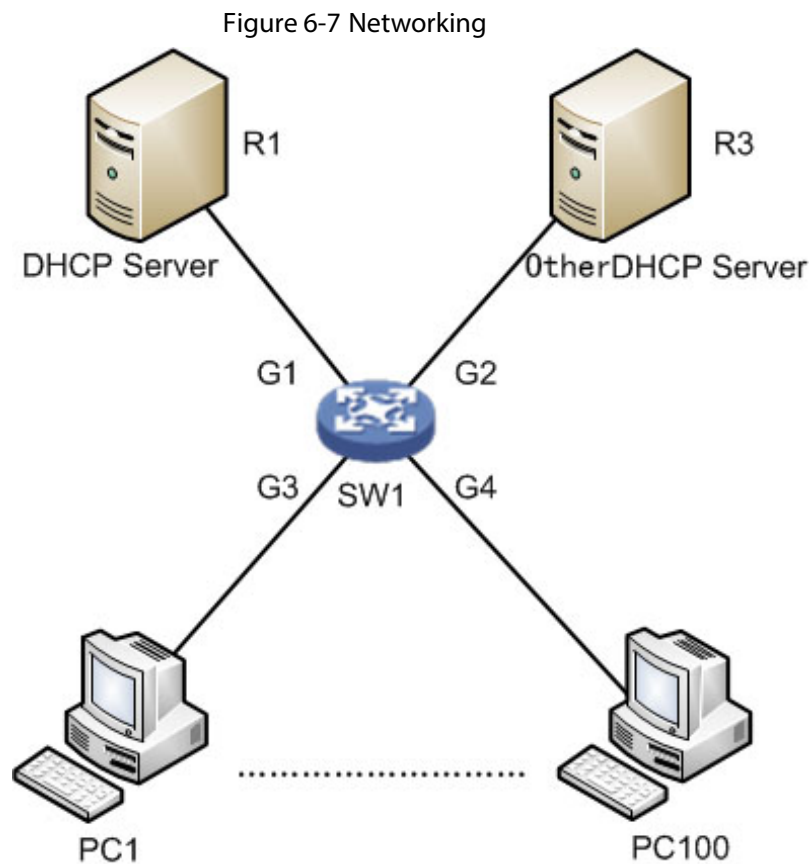
Configuration Example

SWITCH#config terminal

SWITCH(config)# ip dhcp snooping

SWITCH(config)# interface GigabitEthernet 1/1

SWITCH(config-if)# ip dhcp snooping trust

SWITCH(config)# interface GigabitEthernet 1/2

SWITCH(config-if)#no ip dhcp snooping trust

Result Verification

PC1–PC100 can acquire IP info from DHCP server under G1 port, it fails to acquire IP info from DHCP server under G2 port.

6.5 DHCP Server

DHCP Server configuration commands:

ip dhcp server

ip dhcp pool

host/network

ip dhcp excluded-address

lease time

dns

default-router

show ip dhcp

6.5.1 Function Introduction

DHCP Server is a computer which manages DHCP standard in a particular network. DHCP Server is to distribute IP address when workstation logs in, and make sure each IP address is different for each workstation, DHCP Server has greatly simplify network management tasks which used to be completed manually.

Generally it uses DHCP Server to complete IP address distribution in the following occasions.

- Network scale is quite big, it needs a lot of workforce to configure manually and it is hard to make centralized management upon the whole network.
- Number of hosts is bigger than that of IP addresses in the network; it fails to distribute a fixed IP address to each host. For example, Internet access service provider restricts user number of network access; users must acquire their own IP address dynamically.
- There are only a few hosts need fixed IP address in the network; most hosts have no requirement of fixed IP address. The configuration of DHCP Server can be divided into three parts: mode configuration, IP exclusion, address pool configuration.

6.5.2 IP DHCP Server

Command Description

IP dhcp server, enable DHCP service.

No ip dhcp server, disable DHCP service.

DHCP service is in the disabled status by default.

Parameter

None.

Command Mode

Global mode/VLAN port mode.

Example

// Enables DHCP Server globally. The corresponding VLAN ports which belong to address pool can acquire IP info after it is enabled.

SWITCH (config) # ip dhcp server

// Configure DHCP Server allows to distribute IP in vlan 2.

SWITCH (config) # interface vlan 2

SWITCH (config-if-vlan) # ip dhcp server

// Configure DHCP Server doesn't allow to distribute IP in vlan 2

SWITCH (config-if-vlan) # no ip dhcp server

6.5.3 IP DHCP Pool

Command Description

IP dhcp pool <pool_name>, newly add DHCP address pool name.

No ip dhcp pool <pool_name>, delete the DHCP address pool of designated name.

Parameter

Pool_name, it is the address pool name.

Command Mode

Global mode.

Example

// Add a new DHCP address pool whose name is vlan2_test.

SWITCH (config) # ip dhcp pool vlan2_test1

// Delete the DHCP address pool whose name is vlan2_test.

SWITCH (config) # no ip dhcp pool vlan2_test1

6.5.4 Host/Network

Command Description

Host <ip> <subnet_mask>,

It is to configure the host address of address pool.

Network <ip> <subnet_mask>, it is to configure IP network segment of address pool. It supports max distribution of 1K Ip and it can be extended to 4K.

No host <ip> <subnet_mask>, it means deleting the host address of address pool.

No network <ip> <subnet_mask>, it means deleting IP network segment of address pool.

Parameter

Table 6-12 Parameter

Parameter	Description
ip	IP address
subnet_mask	Subnet mask

Command Mode

Address pool configuration mode.

Example

// Configure the host address and IP network segment of address pool.

SWITCH (config) # ip dhcp pool test_pool

SWITCH (config-dhcp-pool) # host 3.0.0.1 255.0.0.0

SWITCH (config-dhcp-pool) # network 1.0.0.1 255.0.0.0

6.5.5 IP DHCP Excluded-address

Command Description

IP dhcp excluded-address <low_ip> [<high_ip>], it is to configure DHCP server address and exclude IP or IP segment.

No ip dhcp excluded-address <low_ip> [<high_ip>], it is to delete the designated excluded IP or IP segment in the DHCP server address pool. Excluded IP will not be distributed to the client of corresponding port.

Parameter

Table 6-13 Parameter

Parameter	Description
low_ip	Start IP of IP segment, it only needs to configure low_ip when it is to configure IP address rather than Ip segment.
high_ip	End IP of IP segment.

Command Mode

Global mode.

Example

// Configure IP segment exclusion of DHCP server address pool.

SWITCH (config) # ip dhcp excluded-address 1.0.0.1 1.0.0.2

// Delete designated excluded IP segment in the DHCP server address pool.

SWITCH (config) #no ip dhcp excluded-address 1.0.0.1 1.0.0.2

6.5.6 Lease Time

Command Description

Lease {<day> [<hour> [<min>]] | infinite }, it is to configure address pool IP lease.

The lease of address pool IP is infinite by default.

Parameter

Table 6-14 Parameter

Parameter	Description
day	Day
hour	Hour
min	Minute
infinite	Infinite

Command Mode

Address pool configuration mode.

Example

// Configure the lease of address pool as infinite.

SWITCH(config)#ip dhcp pool 1

SWITCH(config-dhcp-pool)# lease infinite

// Configure the lease of address pool as 1 day.

SWITCH(config-dhcp-pool)# lease 1 0 0

6.5.7 DNS

Command Description

DNS-server <ip>, configure DNS（Domain Name System）server address.

Parameter

IP, DNS server address.

Command Mode

Address pool configuration mode.

Example

// Configure DNS server address as 8.8.8.8.

SWITCH (config) #ip dhcp pool 1

SWITCH (config-dhcp-pool) # dns-server 8.8.8.8

6.5.8 Default-router

Command Description

Default-router <ip>, it is to configure default gateway of address pool.

Parameter

IP, gateway IP address.

Command Mode

Address pool configuration mode.

Example

// Configure default gateway of address pool as 1.0.0.100.

SWITCH (config) #ip dhcp pool 1

SWITCH (config-dhcp-pool) # default-router 1.0.0.100

6.5.9 Show IP DHCP

Command Description

Show ip dhcp pool [<pool_name>], check address pool configuration.

Show ip dhcp server, check server configuration.

Parameter

pool_name, address pool name.

Command Mode

Privileged mode.

Example

// Check address pool configuration.

SWITCH# show ip dhcp pool

// Check server configuration.

SWITCH# show ip dhcp server

6.5.10 DHCP Server Example

Networking Requirement

It is to configure switch as DHCP server, client IP info is distributed by server, which is shown in Figure 6-8.

Figure 6-8 Networking
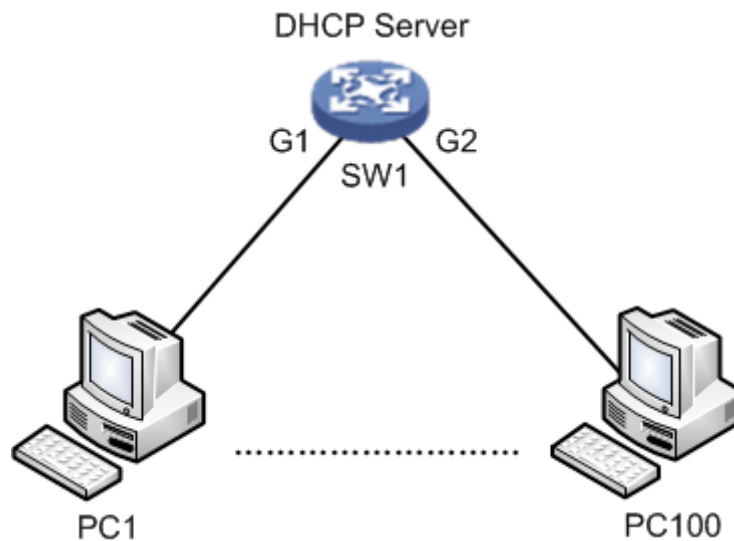
Configuration Example

SWITCH# config terminal

SWITCH(config)# ip dhcp server

SWITCH(config)# interface vlan 1

SWITCH(config-if-vlan)# ip dhcp server

SWITCH(config-if-vlan)# exit

SWITCH(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10

SWITCH(config)# ip dhcp pool a

SWITCH(config-dhcp-pool)# network 192.168.1.0 255.255.255.0

SWITCH(config-dhcp-pool)#default-router 192.168.1.1

SWITCH(config-dhcp-pool)#lease 1 0 0

SWITCH(config-dhcp-pool)#dns-server 8.8.8.8

Result Verification

PC1–PC100 can acquire IP info from DHCP server under G1 port, it fails to acquire IP info from DHCP server under G2 port.

It needs to configure layer three port of the same VLAN when configuring the DHCP Server of VLAN; therefore, DHCP Server can send IP info to the client of corresponding VLAN.

6.6 DHCP Client

Only supported by aggregation switches.

DHCP client configuration command: ip address dhcp.

6.6.1 Function Introduction

To facilitate configuration and management, you can specify the interface of the device as a DHCP client, and use the DHCP protocol to dynamically obtain parameters such as IP addresses from the DHCP server. Currently only VLAN interfaces can be configured.

6.6.2 IP Address DHCP

Command Description

Obtain IP address of the VLAN interface by DHCP.

Parameter

None.

Command Mode

VLAN configuration mode.

Example

// Obtain IP address of the VLAN interface by DHCP

SWITCH(config)# interface vlan 1

SWITCH(config-if-vlan)# ip address dhcp

6.7 DHCP Relay

📖

Only supported by optical aggregation switches.

DHCP relay configuration command:
- ip dhcp relay
- ip helper-address

6.7.1 Function Introduction

During dynamically acquiring an IP address, the request packet is sent by broadcast. So DHCP is only applicable when the DHCP client and server are in the same subnet. For dynamic host configuration, it is necessary to set up a DHCP server on all network segments, which is obviously uneconomical.

The DHCP relay function can solve this problem, and the DHCP client can communicate with the DHCP server of other network segments through the DHCP relay and obtain the IP address. That is, DHCP clients on multiple networks can use the same DHCP server, which saves costs and facilitates centralized management.

6.7.2 IP DHCP Relay

Command Description

Enable DHCP Relay function.

Parameter

None.

Command Mode

Global mode.

Example

// Enable DHCP Relay function.
SWITCH(config)# ip dhcp relay

6.7.3 IP Helper-address

Command Description

ip helper-address <v_ipv4_ucast>, set the server address of DHCP Relay.

Parameter

v_ipv4_ucast, server address of DHCP Relay.

Command Mode

Global mode.

Example

// Set the server address of DHCP Relay to 9.9.9.9.

SWITCH(config)# ip helper-address 9.9.9.9

6.8 IGMP Snooping

IGMP Snooping configuration commands:

ip igmp snooping

ip igmp snooping vlan

ip igmp unknown-flooding

ip igmp-snooping immediate-leave

6.8.1 Function Introduction

IGMP Snooping (Internet Group Management Protocol Snooping) is a type of multicast restriction mechanism which is operated on the layer two device. It is to operate IGMP Snooping layer two device and establish mapping for port and MAC multicast address via analysis upon the received IGMP packet, and then it is to transmit multicast data according to the mapping.

6.8.2 IP IGMP Snooping

Command Description

IP igmp snooping, enable IGMP Snooping function.

No ip igmp snooping, disable IGMP Snooping function.

IGMP Snooping function is in the enabled status by default.

Parameter

None.

Command Mode

Global mode, VLAN port mode or port mode

Example

// Enable IGMP Snooping function.

SWITCH (config) # ip igmp snooping

6.8.3 IP IGMP Snooping VLAN

Command Description

IP igmp snooping vlan <v_vlan_list>, enable IGMP Snooping function of some certain VLAN.

No ip igmp snooping vlan <v_vlan_list>, disable IGMP Snooping function of some certain VLAN.

IGMP Snooping function is in the enabled status by default.

Parameter

v_vlan_list, VLAN number.

Command Mode

Interface mode.

Example

// Enable IGMP Snooping function of vlan 1.

SWITCH (config)# interface vlan 1

SWITCH(config-if-vlan)# ip igmp snooping

6.8.4 IP IGMP Unknown-flooding

Command Description

IP igmp unknow-flooding, it is to enable unknown multicast flooding.

No ip igmp unknow-flooding, it is to disable unknown multicast flooding.

The unknown multicast flooding is in the enabled status by default.

Parameter

None.

Command Mode

Global mode.

Example

// Enable unknown multicast flooding.

```
SWITCH (config)#ip igmp unknown-flooding
```

6.8.5 IP IGMP-Snooping Immediate-leave

Command Description

IP igmp-snooping immediate-leave, it is to enable the function of port immediate leave.

No ip igmp-snooping immediate-leave, it is to disable the function of port immediate leave.

The function of port immediate leave is in the disabled status by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable the function of immediate leave for port 1.

```
SWITCH (config)# interface GigabitEthernet 1/1
SWITCH (config-if)# ip igmp snooping immediate-leave
```

6.8.6 IGMP Snooping Example

Networking Requirement

The member port which requires to join multicast group can receive the multicast info, the non-member port which fails to require to join multicast group cannot receive multicast info. For example, PC2 and PC3 require to join dynamic multicast group, PC4 fails to require, which is shown in Figure 6-9.

Figure 6-9 Networking
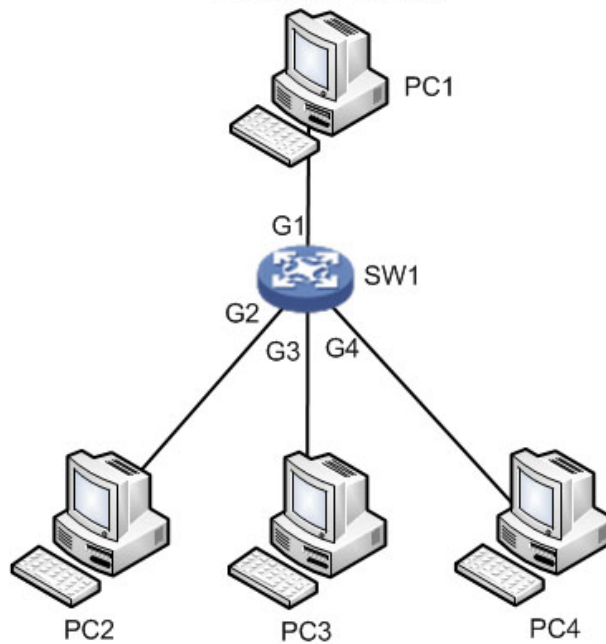
Configuration Example

// Enable IGMP Snooping in vlan 1.

```
SWITCH# conf terminal
SWITCH(config)# ip igmp snooping
SWITCH(config)# interface vlan 1
SWITCH(config-if-vlan)# ip igmp snooping
```

Result Verification

Both PC2 and PC3 can receive the video stream from multicast source while PC4 fails to receive the video stream from multicast source.

6.9 PoE

PoE (Power over Ethernet) configuration commands are:

poe management mode

poe supply

poe system-power-reserve

poe mode

show poe interface

6.9.1 Function Introduction

PoE means providing remote power supply upon the external PD (Powered Device) via Ethernet port and twisted pair. PoE function realizes centralized power supply, convenient backup. It makes network terminal needs no external power; it only needs a network cable. It conforms to IEEE 802.3af

and IEEE 802.3at standards, using global power port. It can be applied to IP phone, wireless AP (Access Point), portable device charger, POS, network camera and data acquisition etc.

6.9.2 PoE Mode

Command Description

PoE mode {on| off}, it is to enable the PoE function of the port.

No PoE mode, it is to disable the PoE function of the port.

The PoE function of port is in the status of enabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Configure port 3 as general PoE port.

```
SWITCH (config) #interface Gigabit Ethernet 1/3
SWITCH(config-if)# poe mode on
```

6.9.3 Show PoE Interface

Command Description

Show PoE [interface (<port_type> [<v_port_type_list>])], it is used to check the device info which supports PoE function.

Parameter

Table 6-15 Parameter

Parameter	Description
port_type	Port type
v_port_type_list	Port number

Command Mode

Privileged mode.

Example

// Configure PoE info of all ports.

SWITCH# show poe

// Configure PoE info of port 1.

SWITCH# show poe interface GigabitEthernet 1/1

6.10 Static Routing

Only supported by aggregation switches.

Static routing configuration command:

ip route xxx.xxx.xxx.xxx   xxx.xxx.xxx.xxx   xxx.xxx.xxx.xxx

Function Introduction

The static routing is a special routing, which is manually configured by the administrator. When the network structure is simple, you only need to configure the static routing to make the network work.

Static routing cannot automatically adapt to changes in the network topology. When the network fails or the topology changes, the network administrator must manually modify the configuration.

Command Description

Configure static routing:

ip route xxx.xxx.xxx.xxx (target network segment) xxx.xxx.xxx.xxx (subnet mask) xxx.xxx.xxx.xxx (Next hop address)

Parameter

None.

Command Mode

Global mode.

Example

// Configure static routing.

SWITCH(config)# ip route 192.168.1.1 255.255.255.0 192.168.2.1

7 Network Security Command

7.1 MAC Address Table

MAC address table commands are:

mac address-table learning

mac address-table static

mac address-table aging-time

show mac address-table

7.1.1 Function Introduction

MAC (Media Access Control) address table records the corresponding relationship between MAC address and port, and VLAN info which belongs to port. It is to search MAC address table according to the destination MAC address of packet when the device transmits packet. If MAC address table contains the corresponding table items of the packet destination MAC address, then it will transmit the packet via the port of the table item; if the MAC address table doesn't contain corresponding table item of packet destination MAC address, the device will adopt multicast mode to transmit the packet via all the ports except the receiver port in the corresponding VLAN.

The module can configure learning mode and aging time of dynamic MAC, it can configure static MAC as well.

7.1.2 MAC Address-table Learning

Command Description

Mac address-table learning [secure], it is to select MAC address table learning mode of the port.

Parameter

Secure, it allows adding static binding but it doesn't allow dynamic learning MAC.

Command Mode

Port mode.

Example

// It allows port 1 adding static binding; it doesn't allow dynamic learning MAC.

SWITCH (config) # interface Gigabit Ethernet 1/1

SWITCH (config-if) # mac address-table learning secure

7.1.3 MAC Address-table Static

Command Description

mac address-table static <v_mac_addr> vlan <v_vlan_id> [interface (<port_type> [<v_port_type_list>])], add static MAC address.

no mac address-table static <v_mac_addr> vlan <v_vlan_id> [interface (<port_type> [<v_port_type_list>])], cancel adding static MAC address.

Parameter

Table 7-1 Parameter

Parameter	Description
v_mac_addr	MAC address
v_vlan_id	The MAC address belongs to VLAN, the value range is 1–4094
port_type	Port type
v_port_type_list	Port number

Command Mode

Global mode.

Example

// Configure MAC address 00-00-00-00-00-01 to bind to port 8 which belongs to VLAN2.

SWITCH(config)# mac address-table static 00-00-00-00-00-01 vlan 2 interface Gigabit Ethernet 1/8

7.1.4 MAC Address-table Aging-time

Command Description

mac address-table aging-time <v_0_10_to_1000000>, it is to set MAC address aging time.

no mac address-table aging-time <v_0_10_to_1000000>, it is to restore the default value of aging time.

Parameter

v_0_10_to_1000000, aging time, when it is configured as 0, it means disabling auto aging; the default value is 300; the value range is <0, 10-1000000>, the unit is "s".

Command Mode

Global mode.

Example

// The aging time of configuring MAC address table is 200s.

SWITCH (config)# mac address-table aging-time 200

7.1.5 Show MAC Address-table

Command Description

show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>]) | vlan <v_vlan_id_2>] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])], it is to display the content of switch MAC address.

Parameter

Table 7-2 Parameter

Parameter	Description
conf	Static MAC address added by users
static	Static MAC address table
aging-time	MAC address table aging time
learning	MAC learning status
count	MAC address amount
port_type	Port type
v_port_type_list	Port number
v_vlan_id_2	VLAN number, value range 1–4094
address	Inquire MAC address

Command Mode

Privileged mode.

Example

// Display all MAC address tables.

SWITCH# show mac address-table

7.2 Port Isolation

Port isolation command is:

[Pvlan isolation](#)

7.2.1 Function Introduction

Port isolation function, it can realize isolation among ports within one VLAN. Users only need to add the port into the isolation group, and then it can realize the isolation of layer two data communication between ports within isolation group. Port isolation function is to provide safer, more flexible and more convenient networking scheme for users.

7.2.2 PVLAN Isolation

Command Description

PVLAN isolation, port members in the isolation group fail to communicate mutually after port is added into isolation group, the ports in the isolation group can communicate with the ports out of the isolation group.

The ports are not added into isolation group by default.

Parameter

None.

Command Mode

Port mode.

Example

// Add G1–5 ports into isolation port, and make them fails to communicate mutually.

SWITCH (config) # interface GigabitEthernet 1/1-5

SWITCH (config-if) # pvlan isolation

7.3 Strom Restrain

Storm restrain command is:

qos storm

7.3.1 Function Introduction

Storm restrain means that the ports can restrict the broadcast stream size allowed by port. The system will discard the data frame which exceeds stream limit after this type of stream exceeds the threshold set by users, which is to prevent storm and guarantee normal operation of the network.

7.3.2 QoS Storm

Command Description

qos storm { unicast | multicast | broadcast } <rate> [fps | kfps | kbps | mbps], it is to enable storm restrain function.

No qos storm { unicast | multicast | broadcast } <rate> [fps | kfps | kbps | mbps],

It is to disable the function of storm restrain.

The storm restrain function is in the disabled status by default.

Parameter

Table 7-3 Parameter

Parameter	Description
unicast	Unicast packet, value range 1–1024000
multicast	Multicast packet, value range 1–1024000
broadcast	Broadcast packet, value range 1–1024000

Command Mode

Global mode.

Example

// Configure broadcast packet storm restrain as 500kbps.

SWITCH (config) #qos storm broadcast 500

7.4 IP Source Protection

IP source protection commands are:

ip verify source

ip verify source translate

ip verify source limit

ip source binding interface

show ip verify source

7.4.1 Function Introduction

It can make filter control upon the packet transmitted by port via IP source protection function, it can prevent illegal packet passing through port and then it can restrict illegal use upon network resource (for example, illegal host counterfeits legal user IP to get access to network), which is finally to improved port security.

If the switch port is configured with IP source protection, then when the packet arrives at the port, the device will check the table item of IP source protection, the packet which conforms to table item

can transmit or enter the following process, the packet which fails to conform to table item will be discarded. Binding function is for ports, after one port is bound, then only this port is restricted, other ports will not be affected by the binding.

7.4.2 IP Verify Source

Command Description

IP verify source, it is to enable IP source protection function.

No ip verify source, it is to disable the function of IP source protection.

IP source protection function is in the disabled status by default.

Parameter

None.

Command Mode

Global mode.

Example

// Enable IP source protection function.

SWITCH (config)# ip verify source

// Enable IP source protection function of port 8.

SWITCH (config)#interface Gigabit Ethernet 1/8

SWITCH (config-if)# ip verify source

7.4.3 IP Verify Source Translate

Command Description

IP verify source translate, it is to translate dynamic entry into static entry

No IP verify source translate, it is to cancel translating dynamic entry into static entry.

Parameter

None.

Command Mode

Global mode.

Example

// Translate dynamic entry into static entry.

SWITCH (config)# ip verify source translate

7.4.4 IP Verify Source Limit

Command Description

IP verify source limit <cnt_var>, it is to restrict port max dynamic client amount.

No ip verify source limit <cnt_var>, it is to restore default value.

It doesn't restrict port max dynamic client amount by default.

Parameter

cnt_var, dynamic client amount, value range 0–2.

Command Mode

Port mode.

Example

// Restrict the Max. dynamic client amount of port 1 no more than 2.

SWITCH (config)# interface GigabitEthernet 1/1

SWITCH (config-if)# ip verify source limit 2

7.4.5 IP Source Binding Interface

Command Description

IP source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var>, add static entry.

No ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var>, delete static entry.

Parameter

Table 7-4 Parameter

Parameter	Description
port_type	Port type
in_port_type_id	Port number
vlan_var	VLAN number
ipv4_var	IP address

Parameter	Description
mac_var	MAC address

Command Mode

Global mode.

Example

// Add one static item that its port number is 1, VLAN number is 1, IP address and subnet mask is 192.168.2.66/255.255.255.0.

SWITCH (config)#ip source binding interface Gigabit Ethernet 1/1 1 192.168.2.66 00-00-00-00-00-01

7.4.6 Show IP Verify Source

Command Description

Show IP verify source, check the config status of IP source protection.

Parameter

None.

Command Mode

Privileged mode.

Example

// Check IP source protection configuration status.

SWITCH# show IP verify source

7.5 ARP Detection Configuration

ARP detection configuration commands are:

ip arp inspection

ip arp inspection trust

ip arp inspection logging

ip arp inspection entry interface

ip arp inspection translate

show ip arp inspection

7.5.1 Function Introduction

ARP protocol is simple and easy to use; however, it is easy to be used by attacker because it is not equipped with any security mechanism. The attacker can counterfeit user and gateway to send false ARP packet, making the ARP table item of gateway or host incorrect, and then it attacks the network. The attacker sends plenty of IP packets which can't be resolved by destination IP address to device, making the device try to resolve destination IP address repeatedly, causing CPU overload and network flow overload. The attacker sends plenty of ARP packets to device and forms impact upon device CPU. Currently ARP attack and ARP virus have become a big threat to LAN security. In order to avoid danger caused by various attacks, the device provides ARP detection technology which is to prevent, detect and solve attacks.

7.5.2 IP ARP Inspection

Command Description

IP arp inspection, it is to enable ARP detection function.

No ip arp inspection, disable ARP detection function.

ARP detection function is disabled by default.

Parameter

None.

Command Mode

Global mode.

Example

// Enable ARP detection function.

SWITCH(config)# ip arp inspection

7.5.3 IP ARP Inspection Trust

Command Description

IP arp inspection trust, it is to enable ARP detection function of the port.

No ip arp inspection trust, it is to disable the ARP detection function of the port.

The port ARP detection function is disabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable the ARP detection function of port 8.

SWITCH (config)#interface Gigabit Ethernet 1/8

SWITCH (config-if)#ip arp inspection trust

// Disable ARP detection function of port 8.

SWITCH (config-if)# no ip arp inspection trust

7.5.4 IP ARP Inspection Logging

Command Description

IP arp inspection logging {deny | permit | all}, the system generates log when illegal ARP appears.

Parameter

None.

Command Mode

Port mode.

Example

// Enable illegal ARP report function of port 8.

SWITCH (config)#interface GigabitEthernet 1/8

SWITCH (config-if)#ip arp inspection logging permit

7.5.5 IP ARP Inspection Entry Interface

Command Description

ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>, add static entry.

no ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>, delete static entry.

Parameter

Table 7-5 Parameter

Parameter	Description
port_type	Port type
in_port_type_id	Port number
vlan_var	VLAN number
mac_var	MAC address
ipv4_var	IP address

Command Mode

Global mode.

Example

// Add one static entry.

SWITCH (config)# ip arp inspection entry interface Gigabit Ethernet 1/1 1 00:00:00:00:00:08 192.168.2.3

7.5.6 IP ARP Inspection Translate

Command Description

ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>], translate dynamic entry into static entry.

no ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>], it is cancelled to translate dynamic entry into static entry.

Parameter

Table 7-6 Parameter

Parameter	Description
port_type	Port type
port_type_id	Port number
vlan_var	VLAN number
mac_var	MAC address
ipv4_var	IP address

Command Mode

Global mode.

Example

// Translate all dynamic entries into static entries.

SWITCH (config)# ip arp inspection translate

7.5.7 Show IP ARP Inspection

Command Description

Show ip arp inspection, check relevant configuration info of ARP detection.

Parameter

None.

Command Mode

Privileged mode.

Example

// Check configuration info of ARP detection.

SWITCH# show ip arp inspection

7.6 ACL Configuration

ACL configuration commands are:

access-list ace

show access-list

7.6.1 Function Introduction

ACL (Access Control List) is to realize packet filtering via configuring packet matching rule and treatment. The applied ACL rule on the port makes analysis upon packet field, after it recognizes specific packet, it will make corresponding treatment according to preset operations (allow/forbid pass, speed limit, redirection, disable port etc.)

ACL configuration is related to port security (port ACL strategy configuration) and bandwidth strategy (port ACL bandwidth strategy), ACE (Access Control Entry) entry calls ACL strategy ID and bandwidth strategy ID according to requirements.

7.6.2 Access-list ACE

Command Description

access-list ace [update] <ace_id> [next { <ace_id_next> | last }] [ingress { interface { <port_type> <ingress_port_id> | (<port_type> [<ingress_port_list>]) } | any }] [policy <policy> [policy-bitmask <policy_bitmask>]] [tag { tagged | untagged | any }] [vid { <vid> | any }] [tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any }] [dmac-type { unicast | multicast | broadcast | any }] [frame-type { any | etype [etype-value { <etype_value> | any }] [smac { <etype_smac> | any }……omit......, configure ACL entry.

no access-list ace, delete ACL ACE entry.

Parameter

Table 7-7 Parameter

Parameter	Description
ace_id	ACE entry ID, allowed range is 1–256
next	Add new ACE entry in the current ACE entry
ingress interface	Ingress port
policy	Strategy configuration item
vid	VID filter domain configuration item
tag-priority	vlanTag priority configuration option
dmac-type	Destination MAC type
action	Access control action
rate-limiter	Rate limit, it will call the rate-limiter in the bandwidth strategy
logging	Log frame info
shutdown	Shut down port configuration option
redirect	Port redirection configuration option
frame-type	Frame type

Command Mode

Global mode.

Example

// Configure ACL entry.
SWITCH(config)# $GigabitEthernet 1/1 rule-type ip ipv4 action deny
SWITCH(config)# access-list rate-limiter 1 25kbps 10000

// Delete ACL ACE entry.
SWITCH (config) # no access-list ace 1

7.6.3 Show Access-list

Command Description

Show access-list ace statistics, check configuration info of ACE.

Parameter

None.

Command Mode

Privileged mode.

Example

7.7 STP Configuration

STP configuration commands are:

spanning-tree

spanning-tree mode

spanning-tree mst 0 priority

spanning-tree mst forward-time

spanning-tree mst hello-time

spanning-tree auto-edge

spanning-tree bpdu-guard

spanning-tree edge

spanning-tree link-type

spanning-tree mst

spanning-tree restricted-role

spanning-tree restricted-tcn

show spanning-tree

7.7.1 Function Introduction

STP (Spanning Tree Protocol) is established according to IEEE 802.1D standard, which is used to remove physical loop of DLL (Data Link Layer) in the LAN. The device which operates the protocol can discover network loop via mutual information, and optionally block some ports, finally trim the loop network structure into tree-shaped network structure without loop, in this way it can prevent packet from continuous proliferation and infinite loop in the loop network, besides, it can avoid the problem of decrease of packet treatment capability due to repeatedly receiving same packet.

The protocol packet adopted by STP is BPDU (Bridge Protocol Data Unit), which is called configuration information as well. BPDU contains enough information to guarantee that the device completes the calculation process of spanning tree. STP is to confirm network topology structure via transmitting BPDU between devices.

7.7.2 Spanning –tree

Command Description

Spanning-tree, enable STP function.

No spanning-tree, disable STP function.

STP function is enabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable STP function of port 8.

SWITCH(config)#interface GigabitEthernet 1/8

SWITCH (config-if) #spanning-tree

// Enable STP function of aggregation port.

SWITCH (config) # spanning-tree aggregation

SWITCH (config-stp-aggr) # spanning-tree

7.7.3 Spanning-tree Mode

Command Description

Spanning-tree mode { stp | rstp | mstp }, set STP protocol version

STP protocol version is STP by default.

Parameter

None.

Command Mode

Global mode.

Example

// Set STP protocol version as RSTP.

SWITCH (config) #spanning-tree mode rstp

7.7.4 Spanning-tree MST 0 Priority

Command Description

Spanning-tree mst <instance> priority <prio>, modify STP, RSTP network bridge priority. The smaller the value is, the higher the priority becomes, and the value after priority has to be the multiple of 4096.

The network bridge priority is 32768 by default.

Parameter

Table 7-8 Parameter

Parameter	Description
instance	Value range 0–7
prio	Network bridge priority

Command Mode

Global mode.

Example

// Modify the current device network bridge priority as 4096.

SWITCH (config) #spanning-tree mst 0 priority 4096

7.7.5 Spanning-tree MST Forward-time

Command Description

Spanning-tree mst forward-time <fwdtime>, it is to configure forward time.

The forward time is 15s by default.

Parameter

Fwdtime, value range is 4s–30s.

Command Mode

Global mode.

Example

// Configure forward time.

SWITCH (config) #spanning-tree mst forward-time 16

7.7.6 Spanning-tree MST Hello-time

Command Description

spanning-tree mst hello-time <hellotime>, configure hellotime。

Hello time is 2s by default.

Parameter

Hello time, value range is 1s–10s.

Command Mode

Global mode.

Example

// Configure hellotime.

SWITCH (config) #spanning-tree mst hello-time 3

7.7.7 Spanning-tree Auto-edge

Command Description

Spanning-tree auto-edge, enable auto-edge function.

No spanning-tree auto-edge, disable auto-edge function.

Auto-edge function is enabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable auto-edge function of port 8.

SWITCH (config)#interface Gigabit Ethernet 1/8

SWITCH (config-if) #spanning-tree auto-edge

7.7.8 Spanning-tree BPDU-guard

Command Description

Spanning-tree bpdu-guard, enable BPDU guard function.

No spanning-tree bpdu-guard, disable BPDU guard function.

BPDU guard function is disabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable BPDU guard function of port 8.

```
SWITCH(config)#interface GigabitEthernet 1/8
SWITCH (config-if) #spanning-tree bpdu-guard
```

// Enable BPDU guard function of aggregation port.

```
SWITCH(config)# spanning-tree aggregation
SWITCH (config-stp-aggr)# spanning-tree bpdu-guard
```

7.7.9 Spanning-tree Edge

Command Description

Spanning-tree edge, enable management edge function.

No spanning-tree edge, disable management edge function.

Management edge function is disabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable management edge function of port 8.

```
SWITCH(config)#interface Gigabit Ethernet 1/8
SWITCH (config-if) #spanning-tree edge
```

7.7.10 Spanning-tree Link-type

Command Description

Spanning-tree link-type { point-to-point | shared | auto }, configure point-to-point type.

No spanning-tree link-type, restore default value.

The point-to-point type is auto by default.

Parameter

Table 7-9 Parameter

Parameter	Description
point-to-point	Point-to-point
shared	Shared
auto	Auto detection

Command Mode

Port mode.

Example

// Configure port 8 type as point-to-point

SWITCH (config)#interface Gigabit Ethernet 1/8

SWITCH (config-if) # spanning-tree link-type point-to-point

// Configure aggregation port type as point-to-point.

SWITCH (config-stp-aggr)# spanning-tree link-type point-to-point

7.7.11 Spanning-tree MST

Command Description

spanning-tree mst <instance> cost { <cost> | auto }, set path cost.

No spanning-tree mst <instance> cost { <cost> | auto }, restore default value

Spanning-tree mst <instance> port-priority <prio>, set port priority.

no spanning-tree mst <instance> port-priority <prio>, restore default value.

Parameter

Table 7-10 Parameter

Parameter	Description
instance	Value range 0–7
cost	Value range 1–200000000
prio	Value range 0–240

Command Mode

Port mode.

Example

// Configure path cost of port 8.

SWITCH (config)#interface Gigabit Ethernet 1/8

SWITCH (config-if) # spanning-tree mst 1 cost 144

// Configure path cost of aggregation port.

SWITCH (config-stp-aggr)# spanning-tree mst 1 cost 144

7.7.12 Spanning-tree Restricted-role

Command Description

Spanning-tree restricted-role, enable root guard mechanism, the designated port cannot be root port after enabling the function.

No spanning-tree restricted-role, disable root guard mechanism.

Root guard mechanism is disabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable root guard mechanism of port 8.

SWITCH (config)#interface GigabitEthernet 1/8

SWITCH (config-if) # spanning-tree restricted-role

// Enable root guard mechanism of aggregation port.

SWITCH (config-stp-aggr)# spanning-tree restricted-role

7.7.13 Spanning-tree Restricted-tcn

Command Description

Spanning-tree restricted-tcn, enable TCN (Topology Change Notification) guard mechanism, after the function is enabled, the topology notification of designated port is restricted, which is to prevent TCN packet attack.

No spanning-tree restricted-tcn, disable TCN guard mechanism.

TCN guard mechanism is disabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable TCN guard mechanism of port 8.

switch(config)#interface Gigabit Ethernet 1/8

switch (config-if) # spanning-tree restricted-tcn

// Enable TCN guard mechanism of aggregation port.

switch (config-stp-aggr)# spanning-tree restricted-tcn

7.7.14 Show Spanning-tree

Command Description

show spanning-tree [summary | active | { interface (<port_type> [<v_port_type_list>]) } | { detailed [interface (<port_type> [<v_port_type_list_1>])] } | { mst [configuration | { <instance> [interface (<port_type> [<v_port_type_list_2>])] }] }], check STP relevant configuration.

Parameter

Table 7-11 Parameter

Parameter	Description
port_type	Port type
v_port_type_list	Port number
instance	Value range 0–7

Command Mode

Privileged mode.

Example

// Check STP configuration status.

SWITCH # show spanning-tree

7.7.15 STP Configuration Example

Networking Requirement

As it is shown in Figure 7-1, three devices SW1 (192.168.1.1), SW2 (192.168.1.2) and SW3 (192.168.1.3) form STP loop, SW1 is selected as root network bridge.

STP can realize faster switch when other links of the blocked port malfunctions.

Figure 7-1 Networking
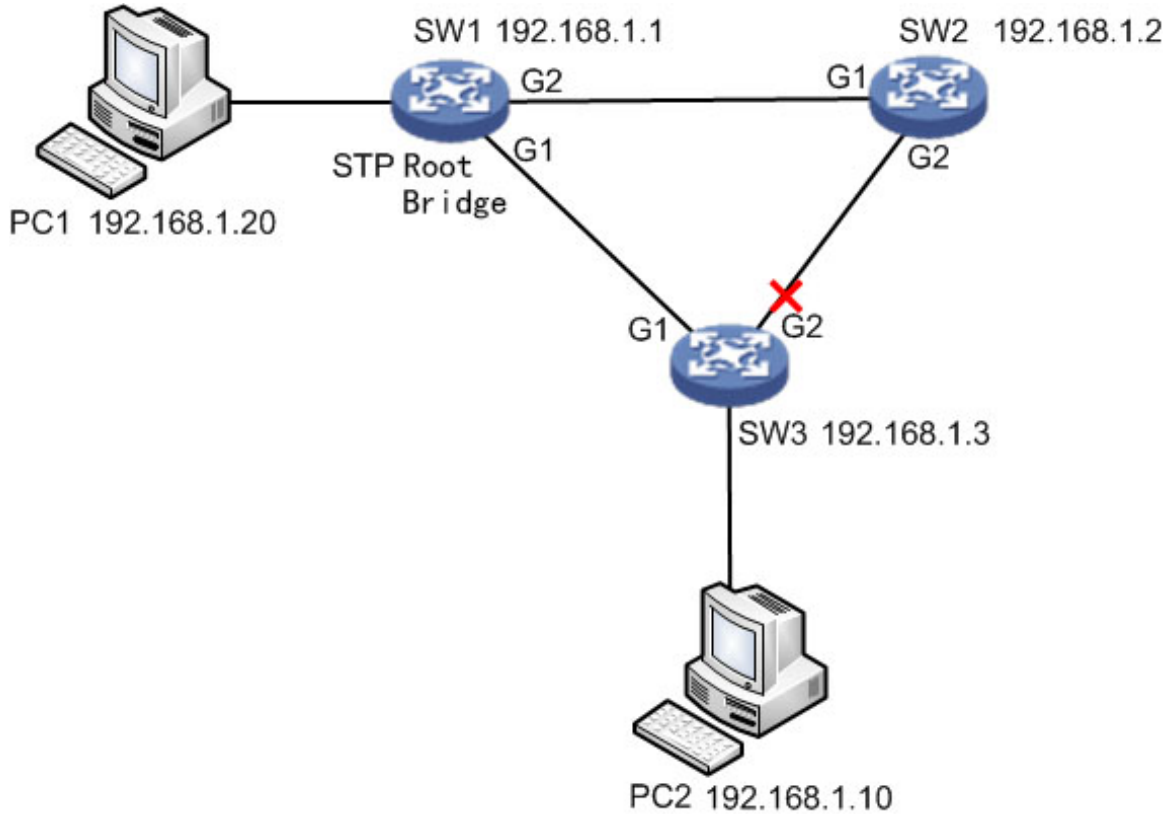
Configuration Example

SW1:

```
SWITCH# configure terminal
SWITCH(config)# spanning-tree mode stp
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# spanning-tree
SWITCH(config-if)#exit
SWITCH(config)# interface GigabitEthernet 1/2
SWITCH(config-if)# spanning-tree
SWITCH(config-if)#exit
SWITCH(config)# spanning-tree mst 0 priority 0
```

SW2:

```
SWITCH# configure terminal
SWITCH(config)# spanning-tree mode stp
```

```
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# spanning-tree
SWITCH(config-if)#exit
SWITCH(config)# interface GigabitEthernet 1/2
SWITCH(config-if)# spanning-tree
SWITCH(config-if)#exit
SWITCH(config)# spanning-tree mst 0 priority 4096
```

SW3:

```
SWITCH# configure terminal
SWITCH(config)# spanning-tree mode stp
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# spanning-tree
SWITCH(config-if)#exit
SWITCH(config)# interface GigabitEthernet 1/2
SWITCH(config-if)# spanning-tree
SWITCH(config-if)#exit
SWITCH(config)# spanning-tree mst 0 priority 8192
```

Result Verification

PC1 (192.168.1.20) ping PC2 (192.168.1.10) normal communication

Cut off G1 port of SW1 manually: it will cause short-period non communication during switch, communication is recovered normally after a period of time (about 30s–45s).

7.8 Loop Protection

Loop protection configuration commands are:

loop-protect

loop-protect tx-mode

loop-protect shutdown-time

loop-protect transmit-time

show loop-protect interface

show loop-protect

7.8.1 Function Introduction

The loop protection function is similar to STP, but loop protection is not equipped with IEEE standard, it belongs to private protocol, it is easy to configure and use. As for simple loop topology and general network business, it displays obvious advantages in cable backup.

7.8.2 Loop-protect

Command Description

Loop-protect, it is to enable global or port loop protection function.

no loop-protect, disable global or port loop protection function.

The global or port loop protection function is disabled by default.

Parameter

None.

Command Mode

Global mode/port mode.

Example

// Enable global loop protection function.

SWITCH# configure terminal

SWITCH (config) # loop-protect

// Enable port loop protection function.

SWITCH# configure terminal

SWITCH (config)# interface GigabitEthernet 1/1

SWITCH (config-if)#loop-protect

7.8.3 Loop-protect tx-mode

Command Description

Loop-protect tx-mode, it is to enable port master detection mode.

No loop-protect tx-mode; it is to disable port master detection mode.

The port master detection mode is disabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Enable master detection mode of port 1.

```
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)#loop-protect tx-mode
```

7.8.4 Loop-protect shutdown-time

Command Description

Loop-protect shutdown-time <t>, it is to set loop protection function, the shutdown time of the port.

The port shutdown time is 180s under loop protection function by default.

Parameter

t, under loop protection function, the shutdown time of the port. Value range is 0s–604800s.

Command Mode

Global mode.

Example

// Set the loop protection function, and the port shutdown time is 6s.

```
SWITCH (config)#loop-protect shutdown-time 6
```

7.8.5 Loop-protect Transmit-time

Command Description

Loop-protect transmit-time <t>, it is to set interval time of loop detection.

The interval time of loop detection is 5s by default.

Parameter

T, interval time of loop detection, value range is 1s–10s.

Command Mode

Global mode.

Example

// Set the time of loop detection, once per 6s.

```
SWITCH (config)#loop-protect transmit-time 6
```

7.8.6 Show Loop-protect Interface

Command Description

Show loop-protect [interface (<port_type> [<plist>])], check loop protection status of the port.

Parameter

Table 7-12 Parameter

Parameter	Description
port_type	Port type
plist	Port number

Command Mode

Privileged mode.

Example

// Check loop protection status of port 1.

```
SWITCH# show loop-protect interface Gigabit Ethernet 1/1
```

7.8.7 Show Loop-protect

Command Description

Show loop-protect, it is to check global loop protection status.

Parameter

None.

Command Mode

Privileged mode.

Example

// Check global loop protection status.

```
SWITCH# show loop-protect
```

7.8.8 Loop Protection Example

Networking Requirement

As it is shown in Figure 7-2, three devices form loop (SW3 is non-managed switch), PC1 and PC2 can access normally.

Figure 7-2 Networking
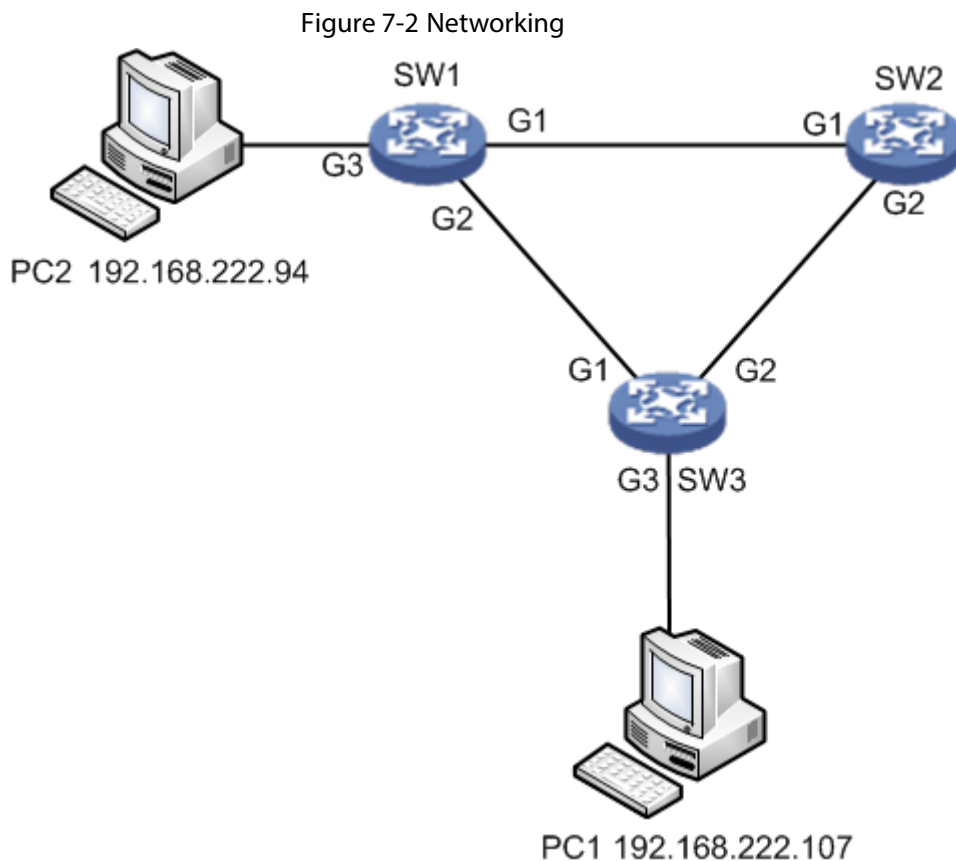
Configuration Example

SW1:

// Enable global loop protection and configure detection interval.

SWITCH#configure terminal

SWITCH(config)# loop-protect

SWITCH(config)# loop-protect transmit-time 6

// Enable G1 port loop protection and master detection mode.

SWITCH(config)# interface GigabitEthernet 1/1

SWITCH(config-if)# loop-protect

SWITCH(config-if)# loop-protect tx-mode

SWITCH(config-if)#exit

// Enable G2 port loop protection and master detection mode.

SWITCH(config)# interface GigabitEthernet 1/2

SWITCH(config-if)# loop-protect

SWITCH(config-if)# loop-protect tx-mode

SW2:

It is the same as SW1, it is omitted here no more description.

Result Verification

PC1 (192.168.222.107) ping PC2 (192.168.222.94).

It will cause communication interruption for a short period to the link when cutting off the link of the blocked port; it will take 6s to recover communication.

- It needs at least one port which enables master detection mode for those which form group loop.
- The blocked port exists in the device which has enabled the function of loop protection after group loop is successfully formed.

7.9 ERPS

Only supported by industrial switches.

ERPS configuration commands:

erps erps-group-number vlan vlan-id

erps erps-group-number major port0 interface port-number port1 interface port-number

erps erps-group-number rpl [owner][neighbor] port0

erps erps-group-number mep port0 sf 1 aps 1 port1 sf 2 aps 2

mep mep-instance-number vid vlan-id

mep mep-instance-number domain port flow 2 level 5 interface port-number

mep mep-instance-number mep-id mep-id

mep mep-instance-number peer-mep-id mep-id

7.9.1 Function Introduction

ERPS (Ethernet Ring Protection Switching) is a two-layer ring-breaking protocol standard defined by ITU-T. The standard number is ITU-T G.8032/Y1344, so it is also called G.8032. It defines RAPS (Ring Auto Protection Switching) protocol messages and protection switching mechanisms.

ERPS currently supports two versions, v1 and v2, v1 is the version released by the ITU-T organization in June 2008, and v2 is the version released by the ITU-T in August 2010. The v2 version is fully compatible with the v1 version, and the following functional extensions have been made based on the v1 version:

- Multi-ring networking, such as intersecting rings.
- The virtual channel or non-virtual channel is used to transmit RAPS messages on the sub-ring.
- Manually switch the blocking point, including forced switching and manual switching.
- The switchback mode of ERPS ring can be configured.

7.9.2 erps erps-group-number vlan vlan-id

Command Description

Configure ERPS group and data VLAN at the same time.

Parameter

None.

Command Mode

Global mode.

Example

// Set ERPS group to 1 and data VLAN to 1.

switch1(config-if)# erps 1 vlan 1

7.9.3 erps erps-group-number major port0 interface port-number port1 interface port-number

Command Description

Configure ERPS port0 and port1.

Parameter

None.

Command Mode

Global mode.

Example

// Configure ERPS port0 and port1.

switch2(config-if)# erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet 1/4

7.9.4 erps erps-group-number rpl [owner][neighbor] port0

Command Description

Configure ERPS RPL port and role.

Parameter

None.

Command Mode

Global mode.

Example

// Configure ERPS RPL port and role.

switch1(config-if)# erps 1 rpl neighbor port0

7.9.5 erps erps-group-number mep port0 sf 1 aps 1 port1 sf 2 aps 2

Command Description

Configure correlation between ERPS and MEP (Maintenance Association End Point).

Parameter

None.

Command Mode

Global mode.

Example

// Configure correlation between ERPS and MEP.

switch1(config-if)# erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2

7.9.6 mep mep-instance-number vid vlan-id

Command Description

Configure the control VLAN of ERPS.

Parameter

None.

Command Mode

Global mode.

Example

// Configure the control VLAN of ERPS.

`switch1(config-if)# mep 1 vid 10`

7.9.7 mep mep-instance-number domain port flow 2 level 5 interface port-number

Command Description

Configure MEP port.

Parameter

None.

Command Mode

Global mode.

Example

// Configure MEP port.

`switch1(config-if)# mep 2 down domain port flow 2 level 5 interface GigabitEthernet 1/2`

7.9.8 mep mep-instance-number mep-id mep-id

Command Description

Configure MEP ID.

Parameter

None.

Command Mode

Global mode.

Example

// Configure mep-id.

switch1(config-if)# mep 2 mep-id 2

7.9.9 mep mep-instance-number peer-mep-id mep-id

Command Description

Configure peer MEP ID.

Parameter

None.

Command Mode

Global mode.

Example

// Configure peer mep-id.

switch1(config-if)# mep 1 peer-mep-id 3

7.9.10 ERPS Networking Example

Figure 7-3 ERPS Networking
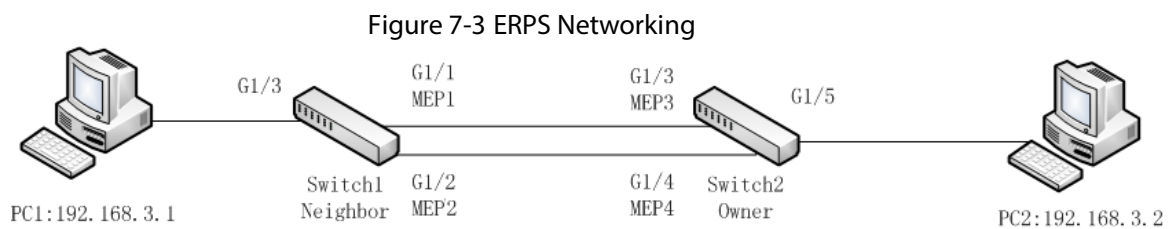
Switch1 and Switch2 form a ring network. Set Switch2 as the Owner node and Switch1 as the Neighbor node, and all ports are in the same vlan1.

Initial configuration:

Disable the STP protocol of the G1/1, G1/2, and G1/3 ports of Switch1 and configure these ports as trunk ports to allow vlan1 to pass. Configure Switch2 in the same way as Switch1.

switch1# configure   terminal

switch1(config)# interface   GigabitEthernet   1/1

switch1(config-if)# no spanning-tree

switch1(config-if)# switchport   mode   trunk

```
switch1(config-if)# switchport    trunk allowed    vlan    1

switch1(config-if)# exit
switch1(config)# mep 1 down domain port flow 1 level 5 interface GigabitEthernet 1/1
switch1(config)# mep 1 vid 10
switch1(config)# mep 1 peer-mep-id 3
switch1(config)# mep 1 cc 0
switch1(config)# mep 1 aps 0 raps
switch1(config)# mep 2 down domain port flow 2 level 5 interface GigabitEthernet 1/2
switch1(config)# mep 2 mep-id 2
switch1(config)# mep 2 vid 10
switch1(config)# mep 2 peer-mep-id 4
switch1(config)# mep 2 cc 0
switch1(config)# mep 2 aps 0 raps
switch1(config)# erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet
1/2
switch1(config)# erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
switch1(config)# erps 1 rpl neighbor port0
switch1(config)# erps 1 vlan 1

// Configure owner node and MEP of Switch2
switch2(config)# mep 1 down domain port flow 3 level 5 interface GigabitEthernet 1/3
switch2(config)# mep 1 mep-id 3
switch2(config)# mep 1 vid 10
switch2(config)# mep 1 peer-mep-id 1
switch2(config)# mep 1 cc 0
switch2(config)# mep 1 aps 0 raps
switch2(config)# mep 2 down domain port flow 4 level 5 interface GigabitEthernet 1/4
switch2(config)# mep 2 mep-id 4
switch2(config)# mep 2 vid 10
switch2(config)# mep 2 peer-mep-id 2
switch2(config)# mep 2 cc 0
switch2(config)# mep 2 aps 0 raps
switch2(config)# erps 1 major port0 interface GigabitEthernet 1/3 port1 interface GigabitEthernet
1/4
switch2(config)# erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
switch2(config)# erps 1 rpl owner port0
switch2(config)# erps 1 vlan 1
```

8 Network Management Command

8.1 SSH Configuration

SSH configuration command is:

ip ssh

8.1.1 Function Introduction

SSH (Secure Shell) is formulated by network working group of IETF. SSH is a type of security protocol which is established on the basis of application layer and transmission layer. Currently SSH is a quite reliable protocol which provides security for remote login session and other network service.

8.1.2 IP SSH

Command Description

ip ssh, it is to enable SSH function.

No ip ssh, disable SSH function, at this moment it cannot use SSH mode to manage switch.

SSH function is disabled by default.

Parameter

None.

Command Mode

Global mode.

Example

// Enable SSH function.

SWITCH (config)# ip ssh

8.2 HTTPS Configuration

HTTPS configuration commands are:

ip http secure-server

ip http secure-redirect

ip http secure-certificate

8.2.1 Function Introduction

HTTP (Hyper Text Transfer Protocol) defines how the browser request WWW file from WWW server and how the server transmits file to the browser. From the angle of layer, HTTP is transaction-oriented application layer protocol, it is the important basis for reliable file exchange on the WWW (including text, audio, image and various multimedia files).

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) is a HTTP channel with the goal of security, SSL layer/TLS layer is added to HTTP, the security basis of HTTPS is SSL/TLS, therefore, and the encrypted details need SSL/TLS. It is a URL scheme whose syntax is similar to http system. It is used for transmitting safe HTTP data. The system is built in browser Netscape Navigator, which provides identity authentication and encrypted communication. Currently it is widely used for secure and sensitive communication on World Wide Web, for example, it can be used for protecting account security and user information.

8.2.2 IP HTTP Secure-server

Command Description

ip http secure-server, it is to enable switch HTTPS service.

No ip http secure-server, it is to disable HTTPS service, at this moment it is unable to use HTTPS mode to manage switch.

Switch HTTPS service is disabled by default.

Parameter

None.

Command Mode

Global mode.

Example

// Enable switch HTTPS service.
```
SWITCH (config)# ip http secure-server
```

8.2.3 IP HTTP Secure-redirect

Command Description

ip http secure-redirect, it is to configure switch auto redirect to HTTPS service.

No ip http secure-redirect, it is to disable configuring switch auto redirect to HTTPS service.

Switch auto redirect to HTTPS service is disabled by default.

Parameter

None.

Command Mode

Global mode.

Example

// Enable switch HTTPS auto redirect service.

SWITCH (config)# ip http secure-redirect

8.2.4 IP HTTP Secure-certificate

Command Description

ip http secure-certificate { upload <url_file> [pass-phrase <pass_phrase>] | delete | generate },
configure secure certificate.

Parameter

Table 8-1 Parameter

Parameter	Description
url_file	It needs to upload the url address of certificate file
pass_phrase	The password when certificate is enabled

Command Mode

Global mode.

Example

// Generate secure certificate.

SWITCH (config)# ip http secure-certificate generate

8.3 LLDP Configuration

8.3.1 Function Introduction

LLDP is a type of standard link layer discovery mode; it can organize main capability, management address, device identification, port identification and other info of the local device into different TLV (Type Length Value), and encapsulate it in LLDPDU (Link Layer Discovery Protocol Data Unit) and release it to its neighbor, the neighbor will save it in the form of standard MIB (Management

Information Base), which is used to inquire and judge link communication status of network management system.

8.3.2 IIDP

Command Description

lldp receive, configure port LLDP frame receiver mode

lldp transmit, configure port LLDP frame transmit mode

no lldp receive, disable port LLDP frame receive mode

no lldp transmit, disable port LLDP frame transmit mode

Port LLDP frame receive and transmit mode are both enabled by default.

Parameter

None.

Command Mode

Port mode.

Example

// Configure port LLDP frame receiver mode.

SWITCH(config)#interface GigabitEthernet 1/8

SWITCH(config-if)# lldp receive

// Configure port LLDP frame transmit mode.

SWITCH(config-if)# lldp transmit

// Disable port LLDP frame receiver mode.

SWITCH(config-if)# no lldp receive

// Disable port LLDP frame transmit mode.

SWITCH(config-if)# no lldp transmit

8.3.3 LLDP Holdtime

Command Description

lldp holdtime <val>, configure LLDP   transmitting holdtime time value.

No lldp holdtime, it is to recover LLDP transmitting holdtime time default.

The time value of LLDP transmitting holdtime is 4s by default.

Parameter

Val, value range is 2s–10s.

Command Mode

Global mode.

Example

// Configure LLDP transmitting holdtime time value.

SWITCH(config)# lldp holdtime 3

// Recover LLDP transmitting holdtime time default value.

SWITCH(config)# no lldp holdtime

8.3.4 LLDP Transmission-delay

Command Description

lldp transmission-delay <val>, configure LLDP frame transmission delay.

No lldp transmission-delay, cancel configuring LLDP frame transmission delay.

LLDP frame transmission delay is 2s by default.

Parameter

Val, the value range is 1s–8192s.

Command Mode

Global mode.

Example

// Configure LLDP frame transmission delay.

SWITCH(config)# lldp transmission-delay 4

// Cancel configuring LLDP frame transmission delay.

SWITCH(config)# no lldp transmission-delay

8.3.5 LLDP Timer

Command Description

lldp timer <val>, it is to configure LLDP transmitting packet TTL value

No lldp timer, it is to recover the default value of LLDP transmitting packet TTL.

The TTL value of LLDP transmitting packet is 30s by default.

Parameter

Val, value range is 5s–32768s.

Command Mode

Global mode.

Example

// Configure TTL value of LLDP transmitting packet.

SWITCH (config)# lldp timer 20

8.3.6 LLDP Reinit

Command Description

lldp reinit <val>, configure the delay time of LLDP continuously transmitting packet.

No lldp Reinit, it is to recover the default delay time of LLDP continuously transmitting packet.

The delay time of LLDP continuously transmitting packet is 2s by default.

Parameter

Val, value range is 1s–10s.

Command Mode

Global mode.

Example

// Configure delay time of LLDP continuously transmitting packet.

SWITCH (config)# lldp reinit 2

8.3.7 Show LLDP Neighbors

Command Description

Show lldp neighbors, it is to display brief info of neighbor.

Parameter

None.

Command Mode

Privileged mode.

Example

// Display brief info of neighbor.

SWITCH# show lldp neighbors

8.4 802.1x Configuration

802.1x configuration commands are:

dot1x system-auth-control

radius-server host

dot1x port-control

dot1x re-authentication

dot1x authentication timer re-authenticate

show dot1x statistics

📖

Enable STP port, and then it needs compulsory certification pass mode when configuring 802.1x certification.

8.4.1 Function Introduction

802.1x protocol is issued by IEEE802 LAN/WAN committee in order to solve network security problem of WLAN. Later the protocol is applied into Ethernet as a general access control mechanism of LAN port, which is mainly used to solve Ethernet authentication and security. It will make authentication and control upon the accessed device in the port layer of LAN accessed device.

The switch can make authentication upon network computer as an authentication system. The user device which is connected to port can have access to LAN resources via switch authentication; it fails to have access to LAN resources if it fails to pass switch authentication.

8.4.2 dot1x system-auth-control

Command Description

Dot1x system-auth-control, enable 802.1x NAS function.

No dot1x system-auth-control, disable 802.1x NAS function.

802.1x NAS function is disabled by default.

Parameter

None.

Command Mode

Global mode.

Example

// Enable 802.1x NAS.

SWITCH (config)# dot1x system-auth-control

// Disable 802.1x NAS.

SWITCH (config)# no dot1x system-auth-control

8.4.3 Radius-Server Host

Command Description

radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>] [key { [unencrypted] <unencrypted_key> | encrypted <encrypted_key> }], it is to configure the RADIUS server host name or IP address, designated authentication and recorded destination port number, switch and shared key among RADIUS servers.

The authentication port number and record port number is 1812 and 1813 respectively.

Parameter

Table 8-2 Parameter

Parameter	Description
host_name	Host name or IP address
auth_port	Authentication port number, value range 0–65535
acct_port	Record port number, value range 0–65535
unencrypted_key	Unencrypted
encrypted_key	Encrypted

Command Mode

Port mode.

Example

// Configure RADIUS server info.

SWITCH (config)#radius-server host 192.168.1.100 acct-port 0 key 123

8.4.4 dot1x port-control

Command Description

Dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-based }, it is to configure port authentication mode

No dot1x port-control, port authentication mode is restored to default.

The port authentication mode is force-authorized by default.

Parameter

Table 8-3 Parameter

Parameter	Description
force-authorized	Port authentication mode is force-authorize.
force-unauthorized	Port authentication mode is force-unauthorized.
auto	Port authentication mode is based on port 802.1x.
single	Port authentication mode is single host mode.
multi	Port authentication mode is multi host mode.
mac-based	Port authentication mode is based on MAC 802.1x.

Command Mode

Port mode.

Example

// Configure port authentication mode as force-unauthorized.

SWITCH (config)#interface GigabitEthernet 1/8

SWITCH (config-if)# dot1x port-control force-unauthorized

8.4.5 dot1x re-authentication

Command Description

dot1x re-authentication, enable port re-authentication function.

no dot1x re-authentication, disable port re-authentication function.

The port re-authentication function is disabled by default.

Parameter

None.

Command Mode

Global mode.

Example

// Enable port re-authentication function.

SWITCH(config)# dot1x re-authentication

// Disable port re-authentication function.

SWITCH(config)# no dot1x re-authentication

8.4.6 dot1x authentication timer re-authenticate

Command Description

dot1x authentication timer re-authenticate <v_1_to_3600>, configure port re-authentication timer

No dot1x authentication timer re-authenticate, port re-authentication timer is restored to default.

Port re-authentication timer is 3600s by default.

Parameter

v_1_to_3600, value range is 1s–3600s.

Command Mode

Global mode.

Example

// Configure port re-authentication timer.

SWITCH(config)# dot1x authentication timer re-authenticate 1000

// Port re-authentication timer is restored to default.

SWITCH(config)# no dot1x authentication timer re-authenticate

8.4.7 show dot1x statistics

Command Description

Show dot1x statistics { eapol | radius | all } [interface (<port_type> [<v_port_type_list>])], it is to check port authentication statistics.

Parameter

Table 8-4 Parameter

Parameter	Description
all	Check all ports authentication statistics.
eapol	Check request authentication statistics.
radius	Check server authentication statistics.
port_type	Port type.
v_port_type_list	Port number.

Command Mode

Privileged mode.

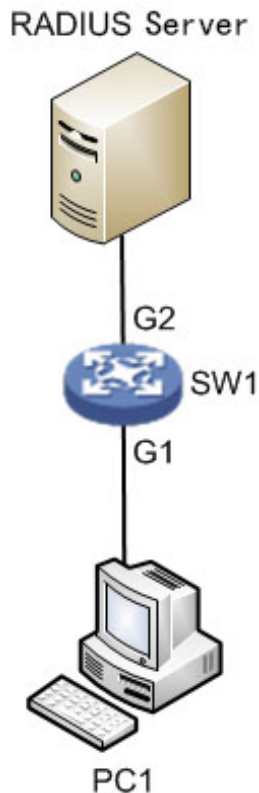## Example

// Check all ports authentication statistics.

SWITCH# show dot1x statistics all

8.4.8 802.1x Configuration Example

Networking Requirement

As it is shown in Figure 8-1, the device connected to G1 port needs authentication to get access the network.

Figure 8-1 Networking

Config Example

// Enable global 802.1x authentication.

SWITCH(config)# dot1x system-auth-control

// Add RADIUS server IP, set shared key.

SWITCH(config)#radius-server host 192.168.1.100 acct-port 0 key 123

// Enable port G1 based on 802.1x auto authentication.

📖

Please disable the STP protocol first when enabling 802.1x authentication under the port.

SWITCH(config)# interface GigabitEthernet 1/1

SWITCH(config-if)# dot1x port-control auto

// Configure RADIUS server end, add authentication account for authentication clients, set NAS key is in accordance with switch key value.

8.5 SNMP Configuration

SNMP configuration commands are:

snmp-server

snmp-server trap

snmp-server community

snmp-server host

host

8.5.1 Function Introduction

SNMP (Simple Network Management Protocol) is made up of a group of network management standards, which includes an application layer protocol (Application Layer Protocol), database schema and a group of materials. The protocol can support network management system, which is used to monitor if the devices which are connected to network are caused any attention about management. The protocol is a part of Internet protocol stack defined by IETF (Internet Engineering Task Force)

8.5.2 SNMP-Server

Command Description

snmp-server, enable SNMP function.

No snmp-server, disable SNMP function.

SNMP function is disabled by default.

Parameter

None.

Command Mode

Global mode.

Example

// Enable switch SNMP function.

SWITCH (config)# snmp-server

8.5.3 SNMP-Server Trap

Command Description

snmp-server trap <source_name>, add Trap source event.

No snmp-server trap <source_name>, delete Trap source event.

Parameter

Table 8-5 Parameter

Parameter	Description
source_name	Function name, include following options: ● alarmTrapStatus ● authenticationFailure ● coldStart ● entConfigChange ● fallingAlarm ● ipTrapInterfacesLink ● linkDown ● linkUp ● lldpRemTablesChange ● newRoot ● psecTrapGlobalsMain ● psecTrapInterfaces ● risingAlarm ● topologyChange ● warmStart

Command Mode

Global mode.

Example

// Add linkup event.

SWITCH(config)# snmp-server trap linkup

8.5.4 SNMP-Server Host

Command Description

snmp-server host <conf_name>, configure the host name of Trap destination address.

Parameter

conf_name, configuration name.

Command Mode

Global mode.

Example

// Config host name of trap is 1111.

SWITCH(config)# snmp-server host 1111

8.5.5 Host

Command Description

Host<domain_name>, configure host name.

host <v_ipv4_ucast>, configure the IP of Trap destination address.

Parameter

Table 8-6 Parameter

Parameter	Description
domain_name	Host name
v_ipv4_ucast	Host address

Command Mode

Host of trap configuration mode.

Example
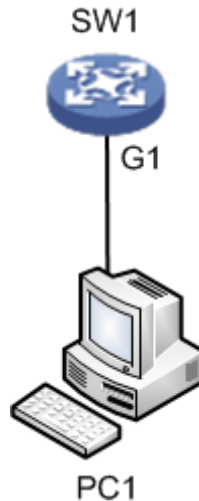
// Configure host name as 1111

SWITCH(config)#snmp-server host 1111

// Configure host address

SWITCH(config-snmps-host)# host 192.168.1 11.111 162 traps

8.5.6 SNMP Configuration Example

Networking Requirement

As it is shown in Figure 8-2, switch enables SNMP; PC1 is installed with MIB Browser, which is used to acquire switch node info.

Figure 8-2 Networking

Configuration Example

SW1:

// Configure SNMP read write community

SWITCH(config)#snmp-server
SWITCH(config)# snmp-server security-to-group model v2c name public group default_ro_group
SWITCH(config)# snmp-server security-to-group model v2c name private group default_rw_group

// Configure SNMP Trap info

SWITCH(config)# snmp-server host aa

SWITCH(config-snmps-host)# no shutdown

SWITCH(config-snmps-host)# host 192.168.222.107
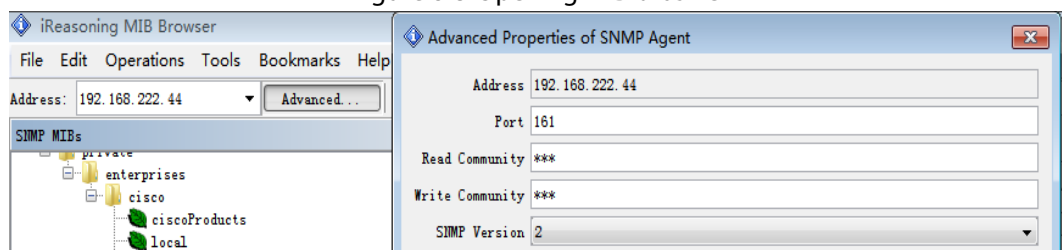
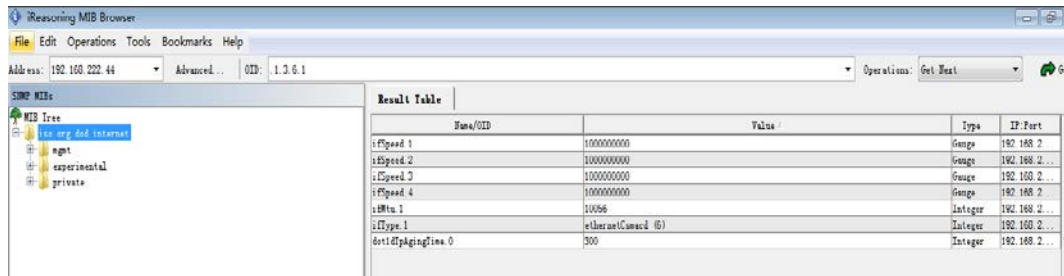192.168.222.107 is the IP address of PC1.

PC1:

Step 1   Open MIB Browser on PC, add switch IP and corresponding community name, which is shown in Figure 8-3.
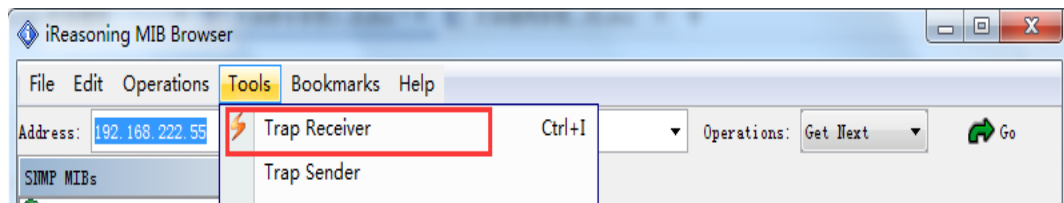
Figure 8-3 Opening MIB broswer

Step 2 Right click iso.org.dod.internet, click "work". It will display relevant info on the info page, which is shown in Figure 8-4.

Figure 8-4 Clicking "work"

Step 3 Select "Tools>Trap Receive", you can check uploaded Trap info, which is shown in

Figure 8-5 Checking upload trap info

8.6 RMON Configuration

RMON CLI configuration commands are:

rmon event

rmon collection history

rmon alarm

rmon collection stats

8.6.1 Function Introduction

RMON (Remote Networking Monitoring) is a standard monitoring specification, which makes it exchange network monitoring data between various network control monitor and console system. RMON helps network administrator to select console and network monitoring detector which conform to special network requirements with more freedom. First RMON has realized consistent remote management upon heterogeneous environment; it provides solution for remote monitoring via port. It mainly realized data flow monitoring function upon one segment or the entire network, currently it has become one of the successful network management standards.

RMON standard makes SNMP monitor remote devices more efficiently and actively, network administrator is able to follow network, segment or device fault more rapidly. RMON MIB is realized to record some network events, it can record network performance data and fault history, it can visit fault history anytime in order to make efficient fault diagnosis. It has reduced data flow between management station and agent by using this method, and made it possible to manage large-sized network simply and powerfully.

It needs to enable SNMP function at the same time when it needs to report server by using RMON function.

8.6.2 RMON Event

Command Description

rmon event <id> [log] [trap [<community>]] { [description <description>] }, it provides table of all events caused by RMON agent.

Parameter

Table 8-7 Parameter

Parameter	Description
id	Event entry ID
log	It generates RMON log when event is generated.
trap	It generates RMON Trap when event is generated.
community	The used community when event is generated.
description	Description of designated event

Command Mode

Global mode.

Example

// Set event number as 111, it is described as 111.

SWITCH(config)# rmon event 111 description 111

// Set event type as trap, community name is public.

SWITCH(config)#rmon event 111 trap public

8.6.3 RMON Collection History

Command Description

rmon collection history <id> [buckets <buckets>] [interval <interval>], it collects the record of network value, and it saves statistics for following treatment.

Parameter

Table 8-8 Parameter

Parameter	Description
id	History entry ID
buckets	Request interval. It is 50buckets by default
interval	Interval. It is 1800s by default.

Command Mode

Port mode.

Example

// Configure the entry whose number is 33, interval is 200s.

SWITCH(config)# interface GigabitEthernet 1/1

SWITCH(config-if)# rmon collection history 33 interval 200

8.6.4 RMON Alarm

Command Description

rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <ifIndex> <Sample interval> {absolute | delta} rising-threshold <rising_threshold> falling-threshold <falling_threshold> { [rising | falling | both] }, it monitors designated alarm variable regularly, it will trigger alarm once the counter exceeds the threshold.

Parameter

Table 8-9 Parameter

Parameter	Description
id	Alarm entry ID
ifInOctets	Number of bytes input into the port
ifInUcastpkts	Unicast packets transmitted to subnet via upper layer protocol
ifInNucastpkts	Non unicast packets transmitted to upper layer protocol
ifInDiscards	Discarded input packets, and these packets will not be transmitted to upper layer network protocol.
ifInErrors	Error packets, these packets will not be transmitted to upper layer network protocol.
ifInUnknownProtos	Discarded input packets due to unknown or unsupported network protocol.
ifOutOctets	Number of byte output by port
ifOutUcastpkts	Number of packets that upper layer protocol (such as IP) needs to send to a network unicast address, the quantity includes discarded or unsent packets.
ifOutNucastpkts	Number of packets that upper layer protocol (such as IP) needs to send to a network non-unicast address, the quantity includes discarded or unsent packets due to some reason.
ifOutDiscards	The packets which cannot be set due to some reason or a reason unrelated to error condition. For example, It may be caused due to packet TTL overtime
ifOutErrors	Number of packets which cannot be sent due to error

Parameter	Description
ifIndex	Corresponding port of bridging port
rising_threshold	Threshold upper limit
falling_threshold	Threshold lower limit
rising	It will trigger alarm when the first value is bigger than threshold upper limit.
falling	It will trigger alarm when the first value is smaller than the threshold lower limit
both	It will trigger alarm when the first value is smaller than threshold lower limit or when the first value is bigger than threshold upper limit.

Command Mode

Global mode.

Example

// Configure the entry whose number is 12.

SWITCH(config)#rmon alarm 12 ifoutErrors 1 1 delta rising-threshold 10 10 falling-threshold 1 1 both

8.6.5 RMON Collection Stats

Command Description

rmon collection stats <id>, Basic statistics info of the monitored Ethernet port.

Parameter

ID, value range is 1–65535.

Command Mode

Port mode.

Example

// Statistics entry of number 22 under port 1.

SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# rmon collection stats 22

9 System Maintenance Command

9.1 Device Reboot

9.1.1 Function Introduction

The module can restart the device.

9.1.2 Reload Cold

Command Description

Reload cold, restart the device.

Parameter

None.

Command Mode

Privileged mode.

Example

// Restarts the device after saving the configuration.
SWITCH# copy running-config startup-config
Do you want to continue? [y/n]: y
SWITCH# reload cold
Reboot system. Do you want to continue? [y/n]: y

9.2 Factory Default

9.2.1 Function Introduction

The module can be used to restore operation upon switch.

9.2.2 Reload Defaults

Command Description

Reload defaults [keep-ip], restore factory default operation, the device will reboot after using the command, it will restore successfully after reboot.

Parameter

Keep-IP, make device management IP address unchanged when restoring factory default settings.

📖

If the keep-in parameter is not added, all parameters will be restored to the factory default configuration.

Command Mode

Privileged mode.

Example

// Restore factory default configuration, it will be valid after the device reboots.
SWITCH# reload defaults
Reboot system. Do you want to continue? [y/n]: y

9.3 Save Configuration

9.3.1 Function Introduction

The module can be used to save configuration.

9.3.2 Copy Running-Config Startup-config

Command Description

copy running-config startup-config, used to save configuration.

Parameter

None.

Command Mode

Privileged mode.

Example

// Save configuration.
SWITCH# copy running-config startup-config
Do you want to continue? [y/n]: y

9.4 Ping Test

9.4.1 Function Introduction

It is used to check if network is connected.

9.4.2 Ping IP

Command Description

ping ip <v_ip_addr>, it is to test the reachability of switch and host.

Parameter

Table 9-1 Parameter

Parameter	Description
v_ip_addr	IP address, address format X.X.X.X

Command Mode

Privileged mode.

Example

// It is to test the reachability of switch and host.

SWITCH# ping ip 192.168.255.3

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

    Please refer to the following suggestions to set passwords:
    *   The length should not be less than 8 characters;
    *   Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
    *   Do not contain the account name or the account name in reverse order;
    *   Do not use continuous characters, such as 123, abc, etc.;
    *   Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

    *   According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
    *   We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

    We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

    We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

    The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

    The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

    We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.