Dahua Gigabit Industrial Managed Switch Command Line

Reference Manual

Version 1.0.0

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Legal Statement

Copyright

Any or full contents of the user's manual cannot be copied, transmitted, distributed or stored, partially or wholly, by any means, without the prior written notice of ZHEJIANG DAHUA VISION TECHNOLOGY CO.,LTD. (hereinafter "Dahua").

Dahua or the third party may reserve the right of the product described in this user's manual. Without the prior written approval of the corresponding party, any person cannot copy, distribute, amend, abstract, reverse compile, disassemble, decode, reverse engineering, rent, transfer or sub-license the software.

Trademark

, , and are the trademarks or registered trademarks of the Dahua in various jurisdictions.

HDMI logo, HDMI and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC. This product has been authorized by HDMI Licensing LLC to use HDMI technology.

VGA is the trademark of IBM.

Windows logo and Windows are trademarks or registered trademarks of Microsoft.

Other trademarks and company names mentioned are the properties of their respective owners

About this Document

This document is for reference only. Please refer to the actual product for more details.

This document serves as a reference for multiple types of products, whose specific operations won't be enumerated. Please operate according to actual products.

The user shall undertake any losses resulting from violation of guidance in the document.

In case that PDF document cannot be opened, please upgrade the reading tool to the latest version or use other mainstream reading tools.

This company reserves rights to revise any information in the document anytime; and the revised contents will be added to the new version without prior announcement. Some functions of the products may be slightly different before and after revision.

The document may include technically inaccurate contents, inconsistencies with product functions and operations, or misprint. Final explanations of the company shall prevail.

Preface

Overview

The manual is to introduce the command line of each feature for the gigabit industrial managed switch in details, which includes the function, parameter, command mode and example etc. of each command.

Applicable Models

Name	Model
8 RJ45 Ports 2 Fiber Ports Gigabit Industrial Managed PoE Switch	DH-PFS4210-8GT-DP
6 RJ 45 Ports 4 Fiber Ports Industrial Managed PoE Switch	DH-PFS4410-6GT-DP

Applicable Readers

Network Engineer

Command Line Format

The following symbols may appear in the manual, please refer to the following table for more details.

Symbol	Note
< >	Command line parameter (it has to be replaced by the actual value in the command) adopts <> to represent.
[ ]	"[ ]" means optional during command config.
{x | y |…}	It means selecting one from two or several options.
<x | y | …>	It means selecting one or none from two or several options.
{x | y |…}*	It means selecting 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	Note
	The icon and related description mean layer two and three Ethernet switch and the devices which operate layer-two protocol.

Port SN Example

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

Table of Contents

1 Log in Device

1.1 Device Login Mode Introduction

The device supports two login modes which are CLI (Command Line Interface) and WEB.

- It can directly input command line to configure and manage device after logging in the device via CLI. The login mode can be different according to the login port and login interface under CLI mode, which consists of Console port, Telnet and SSH. It can only log in via Console port if it is the first time to log in the device via CLI. It can log in the device via Telnet or SSH only when logging in the device via Console port and make corresponding config.
- Users can visually manage and maintain network device by using WEB interface after logging in device via WEB.

1.2 Login System Introduction

It can log in device via Console port when the users need to configure the device which is powered on for the first time.

Console port is a type of communication serial port, which is provided by the main control panel of the device. One main control panel provides one Console port. The users' terminal serial port can be directly connected to the device Console port, which can realize local config for the device.

1.3 First Login via Console Port

The most basic way to log in device is to log in locally via Console port, which is basis of logging in device via other modes.

Please operate according to the following steps when logging in the device via Console port.

Step 1

Power off the PC. Please do not plug the serial port line into or out of PC when it is powered on, because PC serial port fails to support hot plug.

Step 2

Please use the default config port cable to connect PC and device. Please first insert the DB-9 plug of config port cable into the 9-pin serial port of the PC, and then insert the RJ-45 plug into the device Console, which is shown in Figure 1-1.

Note

- Please confirm the symbol on the port during connection in case that it plugs into other ports.
- Please first plug out RJ-45 when removing config port cable, and then plug out DB-9.
- It needs a USB to serial port cable if there is no serial port interface on the laptop, please prepare by yourself.

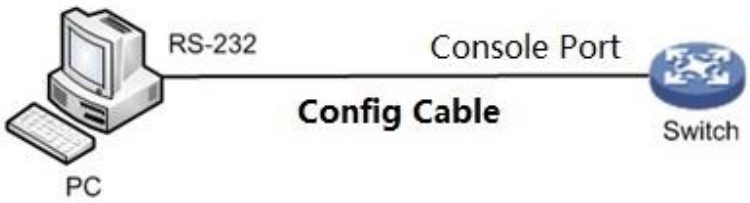


Figure 1-1

Step 3

Power on the PC.

Step 4

Operate terminal simulated program on the PC, select the serial port which is to connect to device and set terminal communication parameters. The parameter value has to be in accordance with that of the device, the default is shown as follows:

Baud rate: 115200

Data bit: 8

Stop bit: 1

Parity: None

Flow control: None

Note

If the PC uses Windows Server 2003 operating system, then please add super terminal program in the Windows module and then log in and manage the device according to the description in the text; if the PC uses Windows Server 2008, Windows Vista, Windows 7 or other operating system, please prepare third-party terminal control software, please refer to the use guidance or online help of software for the application method. Here it is to use SecureCRT as an example to make introduction.

Step 5

Power on the device, it will display self-inspection info on the terminal, it will prompt the users to press Enter after self-inspection is over, and then it will display username and password input prompt.

Step 6

Input username, it is admin by default, press Enter button.

Step 7

Input password, it is admin by default, press Enter button.

Step 8

It will display prompt symbol of command line (SWITCH#) after clicking Enter button, which is shown as follows.

```
+M25PXX : Init device with JEDEC ID 0xC22018.
Luton10 board detected (VSC7428 Rev. D).

RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_31-4752 - built 17:29:35, Jul 29 2017

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
```

```
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x88000000 [0x80028f20-0x87fdfffc available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 3.000 seconds - enter ^C to abort
RedBoot> diag -p
RedBoot> fis load -x linux
MD5 signature validated
Stage1: 0x80100000, length 4641272 bytes
Initrd: 0x80600000, length 188416 bytes
Kernel command line: init=/usr/bin/stage2-loader loglevel=4
RedBoot> exec
Now booting linux kernel:
Base address 0x80080000 Entry 0x80100000
Cmdline : init=/usr/bin/stage2-loader loglevel=4
Active fis: linux
[    0.374113] vcfw_uio vcfw_uio: UIO driver loading
[    0.378957] vcfw_uio vcfw_uio: Invalid memory resource
[    0.384141] iounmap: bad address   (null)
00:00:00 Stage 1 booted
00:00:00 Using device: /dev/mtd7
00:00:01 Mounted /dev/mtd7
00:00:01 Loading stage2 from NAND file 'n6G5Xw'
00:00:05 Overall: 4195 ms, ubifs = 748 ms, rootfs 3422 ms of which xz = 0 ms
of which untar = 0 ms
Starting application...wuxuwuxu
Using existing mount point for /switch/
system time:2017-10-14 17:59:53
W  icfg  18:00:22  71/icfg_commit_tftp_load_and_trigger#2695:  Warning:  TFTP
get bringup-config: Operation timed out.



Press ENTER to get started

Username: admin
Password:
SWITCH#
```

Step 9

Enter command, configure device or check device operation status, please enter ? anytime if you need help.

1.4 Log in Device via Telnet (Optional)

The Telnet server function of device is disabled by default. Therefore, it needs to log in the device via Console first before logging in device via Telnet, enable Telnet server function and then make corresponding config over authentication method, user role and public attribute, which is to guarantee that it can log in the device normally via Telnet.

Enable Telnet Server Function

aaa authentication login telnet local, enable Telnet function.

no aaa authentication login telnet, disable Telnet function.

Add New Telnet User

You can use default username (admin) and password (admin) to log in device, also you can add a new Telnet user to log in the device. The operation of adding new Telnet user is shown as follows:

//Add a new user which is called telnet, the password is admin123456.

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

Result Display

The device will display the following login interface when the user is to log in device via Telnet again after config is completed.

```
Username:
```

Input username and password to log in the device.

1.5 Log in Device via SSH (Optional)

SSH is able to utilize encryption and powerful authentication function to provide safety guarantee and protect the device from being attacked by IP address fraud and cleartext password interception etc. The SSH Server function of device is disabled by default, therefore it needs to log in the device via Console port when logging in device by SSH. It is to enable device SSH server function and make corresponding config over authentication mode and other attributes, which is to make sure that it can log in device normally via SSH.

Enable SSH Server Function

IP SSH, enable SSH function.

No IP SSH, disable SSH function, at this moment it fails to use SSH mode to manage switch.

Please refer to “8.1.2 IP SSH” for more details.

Add New SSH User

You can use default username (admin) and password (admin) to log in device, also you can add a new SSH user to log in device.

The operation of adding new SSH user is shown as follows:

//Add a new user which is called ssh, the password is admin123456.

```
Username SSH privilege 15 password unencrypted admin123456
```

Result Display

It is to input username and password to log in when the user is to log in device via SSH after config is completed.

```
SWITCH#
```

1.6 Log in Device via WEB (Optional)

It can log in the device via WEB, after it is successfully logged in, please refer to the corresponding WEB operation manual or user manual for more details. The operation steps of logging in device via WEB are shown as follows:

Step 1

Open browser, input device IP address in the address bar, the device IP is 192.168.1.110 by default, press **Enter** button.

The system will display the login interface, which is shown in Figure 1-2.

Figure 1-2

Step 2

Input username and password. The username and password are admin and admin by default.

Step 3

Click “Login”.

2 Get Familiar with Command Line

2.1 Command Line Interface Introduction

CLI is a type of text command interactive interface between user and device. Users input text command and submit device corresponding command via clicking enter button, then it is to configure and manage device and confirm config result via checking output info.
The device supports several modes to enter the interface of command line interface, for example, it is to enter command line interface after logging in device via Console port/Telnet/SSH. The interface of CLI is shown as follows:

```
+M25PXX : Init device with JEDEC ID 0xC22018.
Luton10 board detected (VSC7428 Rev. D).

RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_31-4752 - built 17:29:35, Jul 29 2017

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x88000000 [0x80028f20-0x87fdfffc available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 3.000 seconds - enter ^C to abort
RedBoot> diag -p
RedBoot> fis load -x linux
MD5 signature validated
Stage1: 0x80100000, length 4641272 bytes
Initrd: 0x80600000, length 188416 bytes
Kernel command line: init=/usr/bin/stage2-loader loglevel=4
RedBoot> exec
Now booting linux kernel:
Base address 0x80080000 Entry 0x80100000
Cmdline : init=/usr/bin/stage2-loader loglevel=4
Active fis: linux
[    0.374113] vcfw_uio vcfw_uio: UIO driver loading
```

```
[    0.378957] vcfw_uio vcfw_uio: Invalid memory resource
[    0.384141] iounmap: bad address   (null)
00:00:00 Stage 1 booted
00:00:00 Using device: /dev/mtd7
00:00:01 Mounted /dev/mtd7
00:00:01 Loading stage2 from NAND file 'n6G5Xw'
00:00:05 Overall: 4195 ms, ubifs = 748 ms, rootfs 3422 ms of which xz = 0 ms of which untar = 0 ms
Starting application...wuxuwuxu
Using existing mount point for /switch/
system time:2017-10-14 17:59:53
W icfg 18:00:22 71/icfg_commit_tftp_load_and_trigger#2695: Warning: TFTP get bringup-config: Operation timed out.



Press ENTER to get started

Username: admin
Password:
SWITCH#
```

2.2 Command Mode

2.2.1 Command Mode Introduction

The device provides various functions; different functions are corresponding to different config and query commands. The device divides these commands into different organizations according to functions in order to make it convenient for users to use these commands. The function classification is corresponding to command mode. First it needs to enter the mode of the command when it has to configure some command of some function. Each mode is equipped with unique and clear prompt symbol. For example, the prompt symbol SWITCH (config) # means that the current command mode is global mode, you can configure port/VLAN (Virtual Local Area Network) in this mode and other attributes.

Command mode adopts layered structure, which is shown in Figure 2-1.

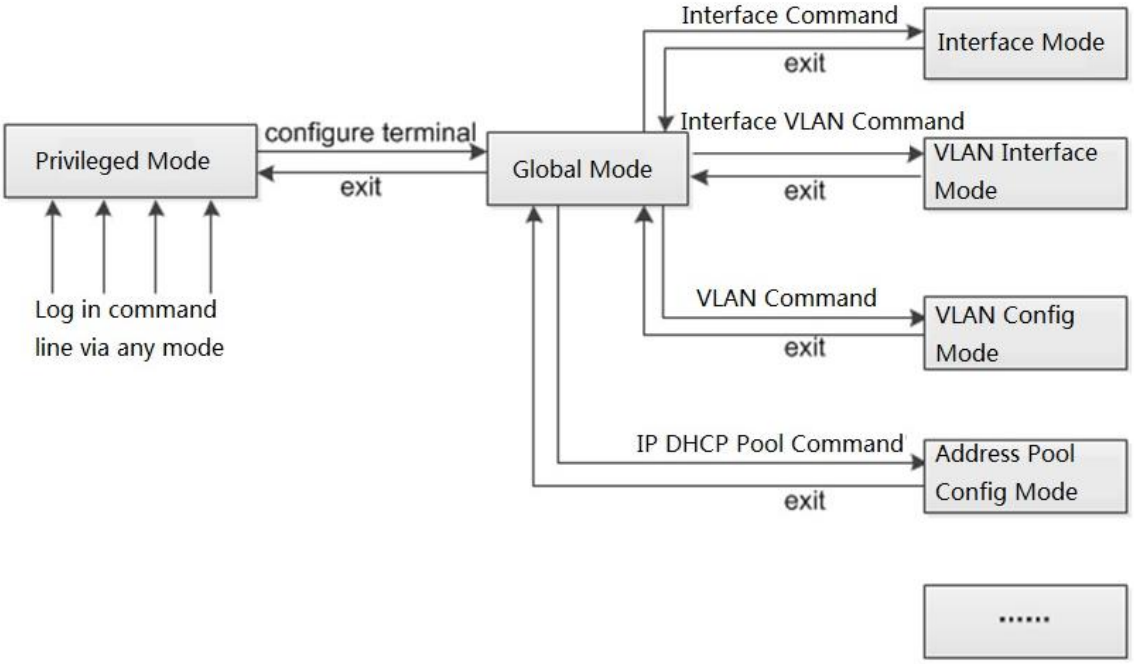


Figure 2-1

- It will enter privileged mode directly after users log in device. At this moment the prompt symbol which is displayed on the screen is device name #. The operations which can be implemented under privileged mode main includes check, debug, file management, set system time, reboot device, FTP and Telnet etc.
- It can enter global mode from privileged mode, at this moment the prompt symbol which displayed on the screen is device name *(config)* #. It can configure device operating parameter and some functions in the privileged mode, such as configure DST, welcome info and shortcut key etc.
- Input specific command in the privileged mode and it can enter corresponding function mode and complete config of corresponding functions, such as enter interface mode to configure interface parameters, enter VLAN interface mode, add interface for VLAN and so on.

Please input <?> after the prompt symbol of the command if you want to know which commands are supported in some certain command mode.

Note

"Device Name" means the name of the device.

2.2.2 Enter Global Mode

It is to enter global mode, please refer to Table 2-1 for more details.

Operation	Command	Note
Enter global mode	configure terminal	The command is implemented in privileged mode

Table 2-1

2.2.3 Return to the Previous Mode

The function config is completed in the current mode, use the command to exit current mode and return to the previous mode, and please refer to Table 2-2 for more details.

Operation	Command	Note
Return to previous mode from the current mode	exit	The command can be implemented in any mode.

Table 2-2

2.3 Use Command Line Online Help

It can input <?> in any location of the command line to acquire detailed online help when entering command line. The following are the common online help application scenes which are for reference.

1. In any mode, input <?> to acquire all the usable commands and simple description of the mode. Example:

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

2. Input the key words of a command, and it is connected with <?> and it is divided by blank. If <?> location is key word, then it will list all the key words and their simple description. Example:

```
SWITCH(config)# ip ?
   arp              Address Resolution Protocol
   dhcp             Dynamic Host Configuration Protocol
   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
```

3. Input incomplete key word of the command and it is connected with <?>, it will display all the command key words which start with the character string. Example:

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

2.4 NO Form of Command

The NO form of the command is generally used to restore default, forbid some function or delete some setting. Most of config commands are equipped with corresponding NO forms. For example, logging on command is used to enable log server mode, no logging on command is used to forbid logging server mode.

2.5 Command Line Input

2.5.1 Edit Command Line

The system supports single button when editing command line, please refer to Table 2-3 for more details.

Button	Function
Common Button	If the edition buffer area is not full, then it can insert to the current cursor location and move the cursor rightward (the command line will be cached in the edition buffer area temporarily before issuing the command line, the size of buffer area is 511 characters; the follow-up characters are invalid if the edition buffer area is full)
<Backspace>	Delete the previous character of the cursor location, 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> button	The system will automatically complement key words after inputting incomplete key word and press <Tab> button. ● The system will use this complete key word to replace the original input and display with line feed if the matched key word is unique. ● It has to press <Tab> button for several times if the matched key word is not unique, the system will display circularly the entire key words which start with input character string. ● The system will not make any modifications if there is not matched key words, it will display original input with line feed again.

Table 2-3

Press <Enter> button to implement the command after users input command line via keyboard. The total length of the input command line cannot exceed 512 characters, including spacing, key word and special symbol etc.

2.5.2 Fast Input Command Line

The device supports incomplete key word input. It means that in current mode, it does not have to input complete key word when there are enough input characters to match unique key word. The function provides a type of rapid input mode, which is helpful to enhance operation efficiency. For example, in global mode, the commands which start with c have configure terminal and clear etc.

It can directly input con ter if it needs to input configure terminal (it cannot input c only, because the matched key word is not unique when it only inputs c).

It can press <Tab> button and the system will automatically complements all the characters of key word, which is to make sure if the input key word is selected by the system.

2.6 Common Input Error Prompt Info

Please press <Enter> button to implement the command after inputting all the command lines. First it will check the grammar of command line when the device is implementing the command. It will implement correctly if it passes grammar check; otherwise, it will output wrong info. Please refer to Table 2-4 for more details.

English Wrong Info	Error Reason
% Incomplete command.	The input command line is incomplete
% Ambiguous word detected at '^' marker.	The input command line is wrong.

Table 2-4

2.7 Use History Command

The commands which are successfully implemented on the device by users will be stored into the history command buffering zone which is only for users. Please refer to Table 2-5 for more details.

History Command Buffer Zone	Whether it can check or not	Whether it can call or not	If history command will be stored continuously after logging out
Exclusive history command buffer zone, each user is corresponding to an exclusive history command buffer zone	It can check via show history	Use up cursor button ↑ and press enter, it can call previous history command. Use down cursor button ↓ and press enter, it can call the next history command.	Not stored

Table 2-5

It has to conform to the following principles when the device is to store history command:

- The format of history command stored by device is the same as that of the command input by users. The format of stored history command is not incomplete if the users use incomplete format of the command; the stored history command is also alias format if users use the alias format of command key word.
- The device history command can be stored only once if users implement the same command continuously for several times.

Attention

It can use cursor to visit history command in the super terminal of Windows 200X and Windows XP and Telnet, but the cursor of ↑ and ↓ are invalid for the super terminal of Windows 9X, this is because the super terminal of Windows 9X has made different explanations for these two buttons.

2.8 Check Display Info Conveniently

Split Screen Display

The system will display info via split screen when there is too much display info covering more than one screen, and it will pause automatically between screens, which is convenient to check display info.

At this moment the users can use button to select the operation of next step, which is shown in

Button	Function
Space	Continue to display the info of next screen.
Enter	Continue to display the info of next line.
<Ctrl+C>	Stop displaying, return to the edition status of command line.
<PageUp>	Display info of previous page
<PageDown>	Display info of next page

Table 2-6

3 System Status Command

3.1 Mode Instruction

Command Description

The chapter is to describe how to enter or exit various mode statuses, including privileged mode, global mode, and interface mode etc.

The system default username and password are admin and admin respectively.

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 Info

3.2.1 Function Introduction

In this module, it can check device name, software and hardware version, MAC address, compilation time, system operation time, system current time and so on.

3.2.2 Show Version

Command Description

Show version, check version info including device name, software and hardware version, MAC address, compilation time, system operation time and so on.

Parameter

None

Command Mode

Privileged mode

Example

// Check version info

```
Username: admin
Password: admin（The password is in the hidden status）
SWITCH # show version
```

3.2.3 Show Clock

Command Description

Show clock, it can check the current system time.

Parameter

None

Command Mode

Privileged Mode

Example

// Check current system time

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

3.3 System Log

3.3.1 Function Introduction

In this module you can check some system log info during the process of device operation, which is convenient for maintenance personnel to make analysis.

3.3.2 Show Logging

Command Description

Show logging <log_id>, check the log info of exact serial number.

Show logging [informational] [notice] [warning] [error], check current log info of the switch.

Parameter

Parameter	Note
log_id	Check log info of exact serial number, value range is 1～4294967295
informational	Check log info of informational.
notice	Check log info of notice.
warning	Check log info of warning
error	Check log info of error

Table 3-1

Command Mode

Privileged Mode

Example

// Check current log info 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

Parameter	Note
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

Table 3-2

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.

Parameter	Note
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
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

Table 3-3

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

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

Table 3-4

Command Mode

Privileged mode

Example

//It is to 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
```

//It is to display the data packet statistics except those have key word 4

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

//It is to 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

parameter	Note
static	Check the config which is manually added by users.
loop-protect	Check config module of loop protection
dhcp	Check the config with DHCP (Dynamic Host Configuration Protocol) module
ptp	Check PTP (Picture Transfer Protocol) module config
upnp	Check general and agreement module config.
arp-inspection	Check ARP (Address Resolution Protocol) detection module config
ipmc	Check IPMC module config
ip-source-guard	Check source address protection module config
conflicts	Check conflict rule caused by hardware restriction

Table 3-5

Command Mode

Privileged Mode

Example

//Check ACL rule info

```
SWITCH# show access-list ace-status
```

3.7 LACP Status

3.7.1 Function Introduction

In this function module, you can check the LACP (Link Aggregation Control Protocol) port config, LACP neighbor info, LACP statistics and LACP system priority etc.

3.7.2 Show LACP

Command Description

Show lacp {internal | statistics | system-id | neighbor}, check LACP system status.

Parameter

Parameter	Note
internal	Check LACP port config
statistics	Check LACP statistics
system-id	Check LACP system priority
neighbor	Check LACP neighbor info

Table 3-6

Command Mode

Privileged Mode

Example

//Check LACP neighbor info

```
SWITCH # show lacp neighbor
```

//Check LACP port config

```
SWITCH# show lacp internal
```

3.8 STP Status

3.8.1 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 config and STP summary info etc.

3.8.2 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

Parameter	Note
<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 config

Table 3-7

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
```

3.9 LLDP Neighbor

3.9.1 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.

3.9.2 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

Parameter	Parameter sub item	Note
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.

Table 3-8

Command Mode

Privileged Mode

Example

//Check LLDP neighbor info

```
SWITCH #show lldp neighbors
```

3.10 Layer Two Forwarding Table

3.10.1 Function Introduction

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

3.10.2 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

Parameter	Note
<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.

Table 3-9

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 Config

IP config commands:

Show ip interface brief

IPaddress

4.1.1 Function Introduction

IP config 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 config, 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 ip interface brief
```

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

Parameter	Note
address	IP address of VLAN port
netmask	Subnet mask
dhcp	Acquire IP info automatically

Table 4-1

Command Mode

VLAN port mode

Example

//Modify switch management IP

```
SWITCH (config)# interface vlan 1
```

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

//Save config after IP is modified.

```
SWITCH# copy running-config startup-config
```

4.2 Log Config

Log config 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

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

Table 4-2

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

Parameter	Note
information	Prompt
notice	Notice
warning	Warning
error	Error

Table 4-3

Command Mode

Global Mode

Example

//It is to configure and upload log level to log server

```
SWITCH (config) # logging level error
```

4.3 User Config

User config 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 config.

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

Parameter	Note
input_username	Username
password	User password, include the following: Encrypted, the password is encrypted Unencrypted, the password is not encrypted. **Note** 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).

Table 4-4

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 config info of the switch.

Parameter

None

Command Mode

Privileged Mode

Example

//Check config info of all current users

```
SWITCH # show users
```

4.4 NTP Config

User config 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

Parameter	Note
index_var	Value range 1~5
ipv4_var	IPv4 address
ipv6_var	IPv6 address
name_var	Domain name

Table 4-5

Command Mode

Global Mode

Example

//It is to set IP address of NTP server.

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

5 Port Config Command

5.1 Port Config

Port config 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.

No duplex, it is restored to default value.

The duplex mode of port is auto by default.

Attention

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

Parameter

Parameter	Note
auto	Auto negotiation
full	Full duplex
half	Half duplex

Table 5-1

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 full
```

//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 full
```

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

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

Table 5-2

Command Mode

Port Mode

Example

//It is to 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 Description

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

Parameter	Note
session_number	Range 1～5
port_type	Mirror destination interface
di_list	Port number

Command Mode

Overall 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

Parameter	Note
session_number	Range 1～5
port_type	Mirror Source Port
si_list	Port Number

Parameter	Note
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

Overall Mode

Example

//it is to 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
```

//It is 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

parameter	Note
rate_limiter_list	Rate limit ID group, range 1～16
pps_rate	Rate value：<0-3276700>
kpbs100_rate	Rate value：<0-10000>

Command Mode

Overall mode

Example

//It is to configure the limit value of ID 4 which is 100000 pps.

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

6 Advanced Config Command

6.1 Link Aggregation

Static aggregation config command:

aggregation mode

aggregation group

Dynamic aggregation config command:

lacp

lacp key

lacp port-priority

lacp role

lacp timeout

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 config, these configurations mainly includes STP, QoS, VLAN port attribute, MAC address learning, ERPS config, loop Protect config, mirror, 801.1x, IP filter, Mac filter and port segregation etc.

LACP is a type of protocol which realizes link dynamic aggregation. LACP protocol interacts info with opposite terminal via LACPDU.

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 config of aggregation load balancing algorithm.

Parameter

Parameter	Note
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

Parameter	Note
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

Overall Mode

Example

//Based on smac dmac load balancing mode

```
SWITCH(config)# aggregation mode smac dmac
```

6.1.3 Aggregation Group

Command Description

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

No aggregation group, delete static convergence config 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
```

//Delete aggregation group

```
SWITCH(config-if)# no aggregation group
```

6.1.4 LACP

Command Description

Lacp, it is to configure port dynamic aggregation enable.

No lacp, disable port dynamic aggregation.

Parameter

None

Command Mode

Port Mode

Example

//1-4 port added to dynamic aggregation group.

```
SWITCH(config)# interface GigabitEthernet 1/1-4
SWITCH(config-if)# lacp
```

//Disable port dynamic aggregation

```
SWITCH(config-if)# no lacp
```

6.1.5 LACP Key

Command Description

lacp key { <v_1_to_65535> | auto }, it is the management key value of dynamic aggregation port, and it is the sign that the port can be added to an aggregation group. LACP protocol can generate an operation key according to port config (rate, duplex, basic config, management key), as for dynamic aggregation group, the same group members must have the same operation key to converge successfully.

The management key of dynamic convergence port can be automatically negotiated by default.

Parameter

Parameter	Note
v_1_to_65535	Manual designated range 1～65535
auto	Key value auto negotiation

Command Mode

Port Mode

Example

//Config key value is 100

```
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)# lacp key 100
```

6.1.6 LACP Port-Priority

Command Description

In the dynamic aggregation group, the port may be in two statuses: select and standby. Both can receive and transmit LACP protocol, but standby port cannot transmit user packet.

The max number of port in the aggregation group is limited, therefore the home terminal system and opposite terminal system will make negotiation if the current number of member port exceeds the max port number limit. It can decide the port status according to the size of port ID at one end of the device ID.

lacp port-priority <v_1_to_65535>, it is to configure LACP port priority.

LACP port priority is 32768 by default.

Parameter

v_1_to_65535, priority range 1～65535, the smaller the value is, the higher the priority becomes.

Command Mode

Port Mode

Example

//Configure LACP port priority

```
SWITCH (config)# interface GigabitEthernet 1/1
SWITCH (config-if)# lacp port-priority 100
```

6.1.7 LACP Role

Command Description

lacp role { active | passive }, it is to configure dynamic aggregation port role.

Dynamic aggregation port role is active mode by default.

Parameter

Parameter	Note
active	It means port role is active mode. In active mode, the port will actively send LACPDU packet to the opposite terminal and make LACP protocol calculation.
passive	It means port role is passive mode. In passive mode, the port will not actively send LACPDU packet, the port will enter protocol calculation status after receiving LACP packet sent by opposite terminal.

Command Mode

Port Mode

Example

//Set port 1 role as active mode

```
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)#lacp role active
```

//Set port 1 role as passive mode

```
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH(config-if)#lacp role passive
```

6.1.8 LACP Timeout

Command Description

lacp timeout { fast | slow }, it is to configure dynamic aggregation timeout option.

Dynamic aggregation timeout is fast timeout by default.

Parameter

Parameter	Note
fast	Fast timeout, which means it sends one LACP packet per second.

Parameter	Note
slow	Slow timeout, which means it sends one LACP packet every 30 seconds.

Command Mode

Port Mode

Example

//It is to configure dynamic aggregation fast timeout

```
SWITCH(config)# interface GigabitEthernet 1/5
SWITCH(config-if)# lacp timeout fast
```

//It is to configure dynamic aggregation slow timeout

```
SWITCH(config)# interface GigabitEthernet 1/5
SWITCH(config-if)# lacp timeout slow
```

6.1.9 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.

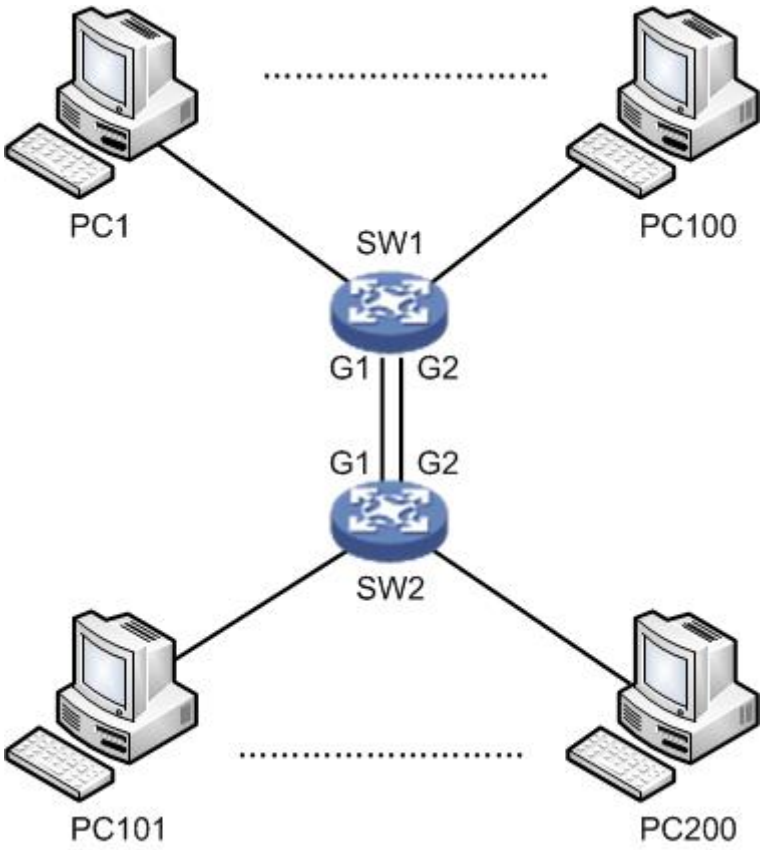


Figure 6-1

Config Example

SW1/SW2 config 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 config command:

vlan

name

switchport mode

switchport access vlan

switchport forbidden vlan

switchport hybrid acceptable-frame-type

switchport hybrid egress-tag

switchport hybrid native

switchport trunk allowed

show vlan

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:

1. 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.
2. 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.
3. 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 config, it uses 1～4094.

Command Mode

Overall 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 config 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.

Parameters

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

//It is to configure switch port 2, 3, 4 mode as access

```
SWITCH(config)# interface GigabitEthernet 1/2-4
SWITCH(config-if)#switchport mode access
```

//It is to 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
```

//5-8 port 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

Parameter	Note
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.

Parameters

Parameters	Note
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 config.

Data egress port attribute is untag port VLAN by default.

Parameters

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

Command Mode

Port mode

Example

//It is to configure data egress port 5 tag attribute

```
SWITCH (config)# interface Gigabit Ethernet 1/5
SWITCH (config-if)# switch port hybrid egress-tag all
```

//It is to restore data egress port tag attribute as default config

```
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.

Parameters

Pvid, VLAN number, value range 1～4094

Command Mode

Port mode

Example

//It is to 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.

Parameters

vlan_list, VLAN number, value range is 1～4094

Command Mode

Port mode

Example

//It is to 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 config via VLAN ID or VLAN name, and check VLAN total config info.

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 config of each port.

Parameters

Parameter	Note
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

Privilege mode

Example

//Check config info of vlan 2

```
SWITCH# show vlan id 2
```

//Check VLAN total config info

```
SWITCH# show vlan brief
```

//Check VLAN config 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.

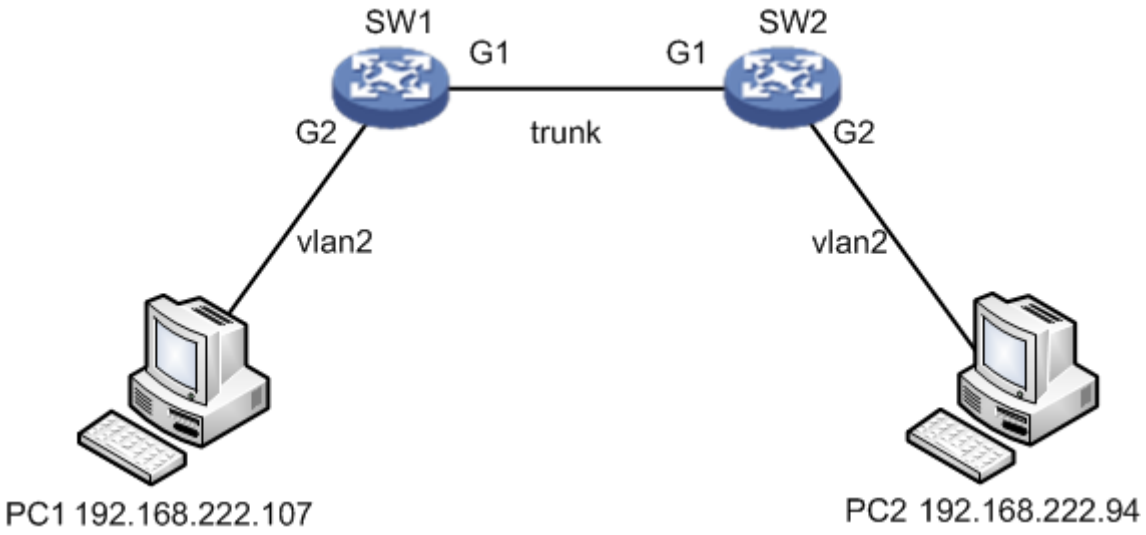


Figure 6-2

Config Example

//Configure SW1 port 1 and port 2 mod

```
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.

```
C:\Users\Administrator>ping 192.168.222.94

正在 Ping 192.168.222.94 具有 32 字节的数据:
来自 192.168.222.94 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.222.94 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.222.94 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.222.94 的回复: 字节=32 时间<1ms TTL=64
```

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.

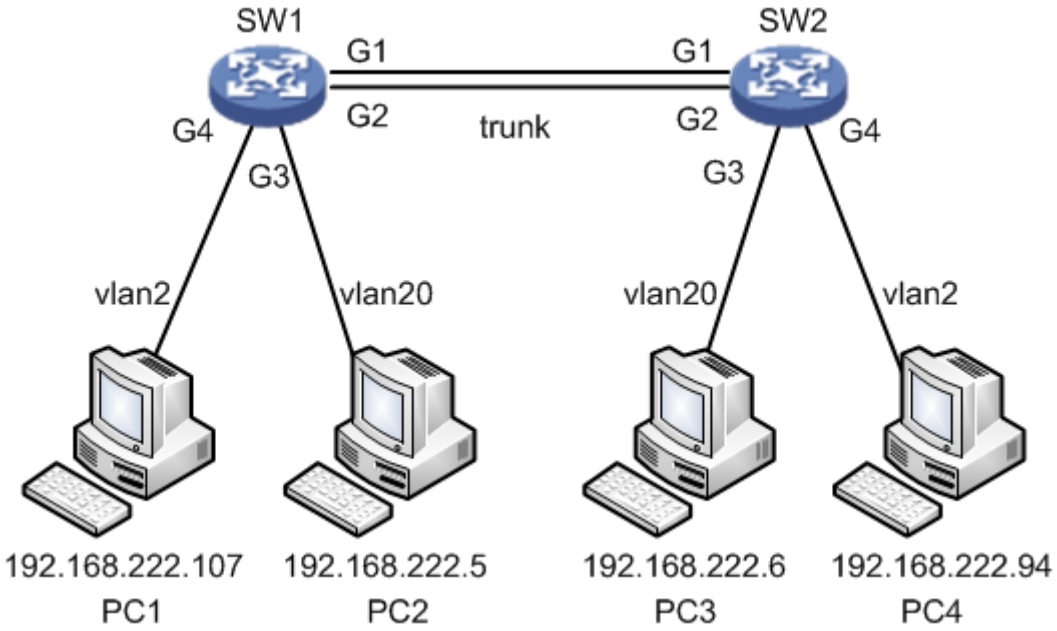


Figure 6-3

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

//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 Config

VCL config 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.

Note

- 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.

Parameters

Parameters	Note
mac_addr	48 bit MAC address, format is ××：××：××：××：××：××
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

Parameters

Parameter	Note
ipv4	IP address and subnet mask
vid	VLAN number

Command Mode

Port mode

Example

//Config 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 id 1 192.168.4.0/255.255.255.0 vlan 2
```

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.

Parameters

Parameter	Note
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.

Parameters

Parameter	Note
etype	Value range 0x600～0xFFFF
oui	Value range 0x000000～0XFFFFFF
pid	Value range 0x0～0xFFFF

Parameter	Note
dsap	Value range 0x00～0xFF
ssap	Value range 0x00～0xFF
grp_id	Protocol group name

Command Mode

Overall 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 Config Example

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 config 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.

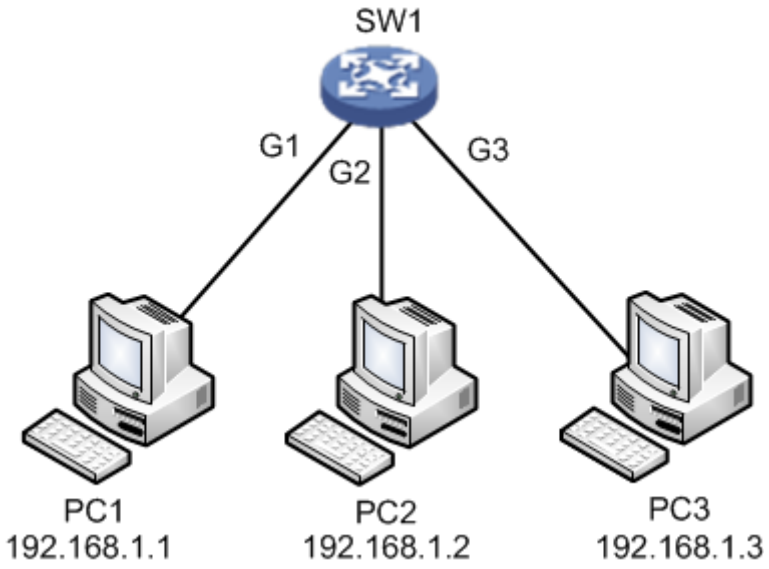


Figure 6-4

Config 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.

2. VLAN partition based on subnet mask

Networking Requirements

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.

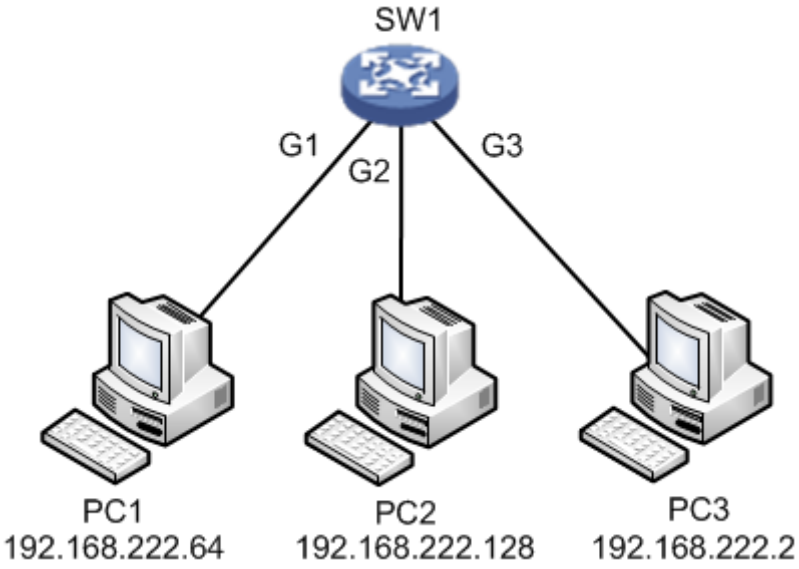


Figure 6-5

Config 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.

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 transmit in vlan 2 via VLAN config based on protocol, and it fails to transmit in other VLAN.

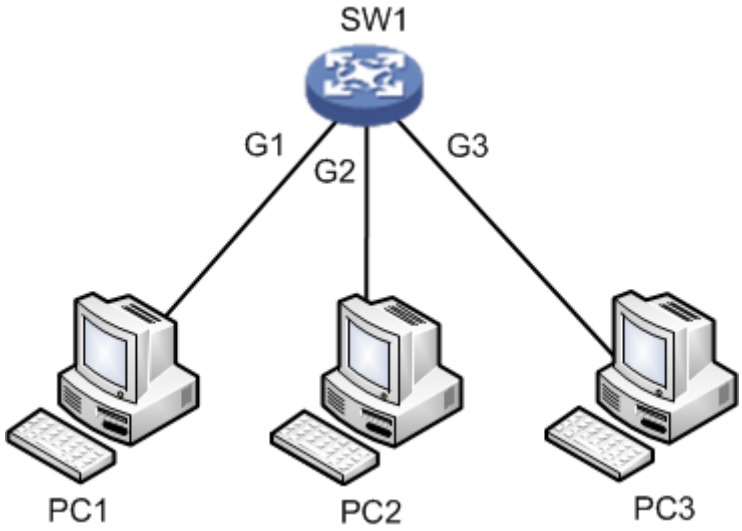


Figure 6-6

Config 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 config 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 config 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 config 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.

1. Trusted ports normally transmit the received DHCP packets.
2. 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 config mode.

No ip dhcp snooping, disable DHCP snooping config mode.

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

Parameters

None

Command Mode

Overall mode

Example

//Enable DHCP snooping config mode

```
SWITCH(config)# ip dhcp snooping
```

//Disable DHCP snooping config 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.

Parameters

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.

Parameters

None

Command Mode

Overall mode

Example

//Check DHCP dynamic snooping information table

```
SWITCH (config) # 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.

Parameters

Parameter	Note
port_type	Port type
in_port_list	Port No.

Command Mode

Privilege 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 Example

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.

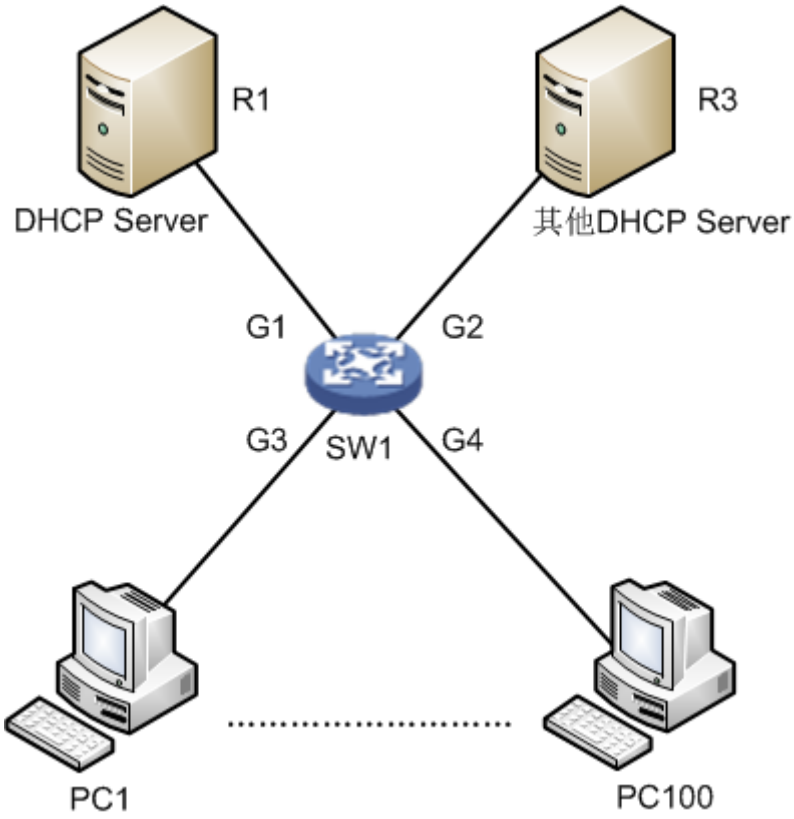


Figure 6-7

Config 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 config 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 config of DHCP Server can be divided into three parts: mode config, IP exclusion, address pool config.

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.

Parameters

None

Command Mode

Overall mode/VLAN port mode.

Example

//Overall enables DHCP Server. 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.

Parameters

Pool_name, it is the address pool name.

Command Mode

Overall mode

Example

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

```
SWITCH (config) # ip dhcp pool vlan2_test1
```

//It is to 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.

Parameters

Parameter	Note
ip	IP address
subnet_mask	Subnet mask

Command Mode

Address pool config mode.

Example

//It is to 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.

Parameters

Parameter	Note
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

Overall mode

Example

//It is to 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.

Parameters

Parameter	Note
day	Day
hour	Hour
min	Minute
infinite	Infinite

Command Mode

Address pool config mode

Example

//It is to configure the lease of address pool as infinite.

```
SWITCH(config)#ip dhcp pool 1
SWITCH(config-dhcp-pool)# lease infinite
```

//It is to 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.

Parameters

IP, DNS server address.

Command Mode

Address pool config mode.

Example

//It is to 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.

Parameters

IP, gateway IP address

Command Mode

Address pool config mode

Example

//It is to 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 config.

Show ip dhcp server, check server config.

Parameters

pool_name, address pool name.

Command Mode

Privilege mode

Example

//Check address pool config

```
SWITCH# show ip dhcp pool
```

//Check server config

```
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.

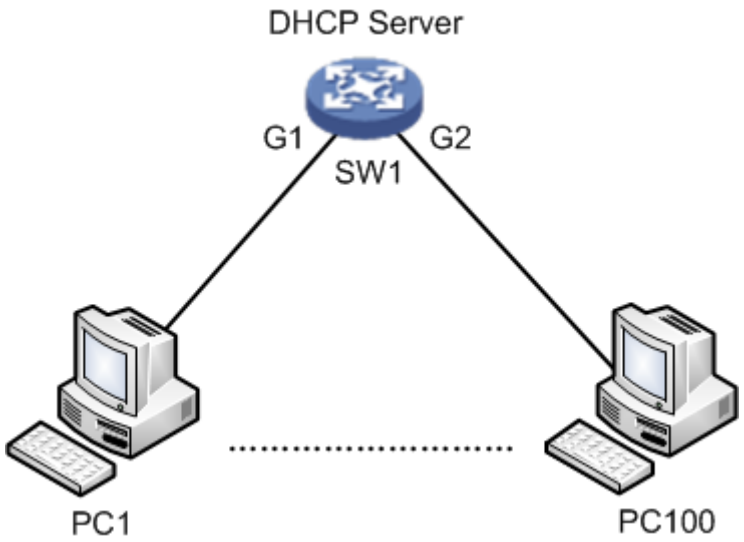


Figure 6-8

Config 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 client can acquire correct IP info from DHCP Server (SW1).

Note

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 IGMP Snooping

IGMP Snooping config commands:

ip igmp snooping

ip igmp snooping vlan

ip igmp unknow-flooding

ip igmp-snooping immediate-leave

show ip igmp snooping

6.6.1 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.

6.6.2 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

Overall mode, VLAN port mode or port mode.

Example

//Enable IGMP Snooping function

SWITCH (config) # ip igmp snooping

6.6.3 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.

Parameters

v_vlan_list, VLAN number

Command Mode

Overall mode

Example

//Enable IGMP Snooping function of vlan 1

```
SWITCH (config)# ip igmp snooping vlan 1
```

6.6.4 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.

Parameters

None

Command Mode

Overall mode

Example

//It is to enable unknown multicast flooding

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

6.6.5 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.

Parameters

None

Command Mode

Port mode

Example

//It is to enable the function of immediate leave for port 1.

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

6.6.6 Show ip igmp snooping

Command Description

show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail], check IGMP config.

show ip igmp snooping mrouter [detail], check the multicast router port status of IGMP.

Parameters

Parameter	Note
v_vlan_list	VLAN number
port_type	Port type
v_port_type_list	Port number

Command Mode

Privilege mode

Example

//Check IGMP config

```
SWITCH #show ip igmp snooping
```

6.6.7 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.

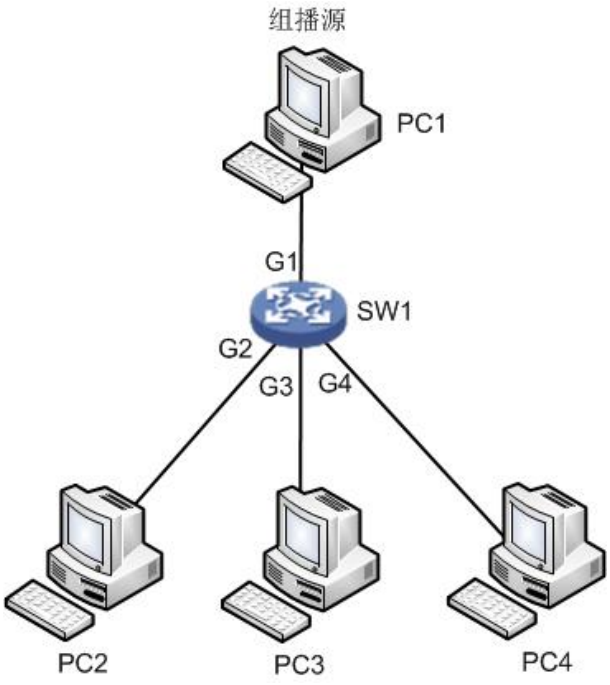


Figure 6-9

Config Example

// Enable IGMP Snooping in vlan 1

```
SWITCH# conf terminal
SWITCH(config)# ip igmp snooping
SWITCH(config)# no ip igmp unknown-flooding
SWITCH(config)#ip igmp snooping vlan 1
```

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.

6.7 MVR Config

MVR (Multicast VLAN Registration) config commands are:

mvr

mvr vlan

mvr name/vlan type

mvr immediate-leave

show mvr

6.7.1 Function Description

MVR is created when it is to solve the problem that receivers are placed in different VLAN and IGMP Snooping fails to do it in the IGMP Snooping protocol. MVR solved the problem of flooding when receivers are located in different VLAN, it uses a dedicated and manually-configured VLAN, which is multicast VLAN, it transmits multicast stream in layer two network and it can be used together with IGMP.

MVR is just like IGMP Snooping, it allows layer two switch to snoop IGMP control protocol, these two protocols operate independently and both can be configured on the switch. If both two features are enabled, MVR will only snoop the group john and report info which is statically configured to MVR function, while the other group info is still managed by IGMP Snooping. There are two types of MVR port when configuring MVR function.

- Source port, it is the port through which multicast stream passes in the multicast VLAN.
- Reception port, it is the port which connects snooping multicast host to switch. It can be placed in any VLAN or no VLAN except multicast VLAN, no VLAN generally refers to VLAN1, which is the flow without any mark. It means that the switch which enables MVR function is to implement the VLAN label replacement, it is to replace the VLAN label of multicast reception port as source port VLAN label. Multicast VLAN means the VLAN which needs to be manually configured in the exact network and it is specifically used by MVR. As for all source ports, it needs to be clearly configured, it is often used to transmit multicast stream in the network and meanwhile it is to avoid multicast stream repetition in different VLAN. MVR VID has to be in accordance with VLAN PVID of the multicast source.

6.7.2 MVR

Command Description

Mvr, globally enable MVR mode.

No mvr, globally disable MVR mode.

MVR mode is in the status of disabled by default.

Parameters

None

Command Mode

Overall Mode

Example

//Globally enable MVR mode

SWITCH(config)# mvr

//Globally disable MV

SWITCH(config)# no mvr

6.7.3 MVR VLAN

Command Description

mvr vlan <v_vlan_list> [name <mvr_name>], configure MVR VLAN port.

no mvr vlan <v_vlan_list> [name <mvr_name>], delete MVR VLAN port config.

Parameters

Parameter	Note
v_vlan_list	VLAN number
mvr_name	MVR multicast VLAN name

Command Mode

Overall mode

Example

//Establish mvr vlan100 and its name is 123

SWITCH(config)# mvr vlan 100 name 123

6.7.4 MVR Name/VLAN Type

Command Description

mvr name <mvr_name> type { source | receiver }

mvr vlan <v_vlan_list> type { source | receiver }

It is to configure current MVR group port as receiver port or source port.

Parameters

Parameter	Note
mvr_name	MVR group name
v_vlan_list	VLAN number

Command Mode

Port mode

Example

//Configure port 8 as the multicast source port of mvr 123

```
SWITCH(config)#interface GigabitEthernet 1/8
SWITCH(config-if)# mvr name 123 type source
```

//Configure port 8 as multicast source port of mvr vlan100

```
SWITCH(config)#interface GigabitEthernet 1/8
SWITCH(config-if)# mvr vlan 100 type source
```

6.7.5 MVR Immediate-leave

Command Description

MVR immediate-leave, it is to enable port MVR immediate leave function.

No mvr immediate-leave, it is to disable port mvr immediate leave function.

Port MVR immediate leave function is in the status of disabled by default.

Parameters

None

Command Mode

Port mode

Example

//It is to enable port 8 MVR immediate leave function.

```
SWITCH(config)#interface GigabitEthernet 1/8
SWITCH(config-if)# mvr immediate-leave
```

//It is to disable port 8 MVR immediate leave function.

```
SWITCH(config-if)# no mvr immediate-leave
```

6.7.6 Show MVR

Command Description

Show MVR, check MVR config.

Parameters

None

Command Mode

Privilege mode

Example

//Check MVR config

```
SWITCH#show mvr
```

6.7.7 MVR Config Example

Networking Requirement

As it is shown in Figure 6-10, port 1, 2 and 8 are access ports respectively, port 1 sets PVID as 10, port 2 sets PVID as 11, and port 8 sets PVID as 100.

Enable MVR, set MVR VID as 100, MVR name is 123, the others are default.

Set port 1 and port 2 type as receiver, port 8 type as source. Enable immediate leave.

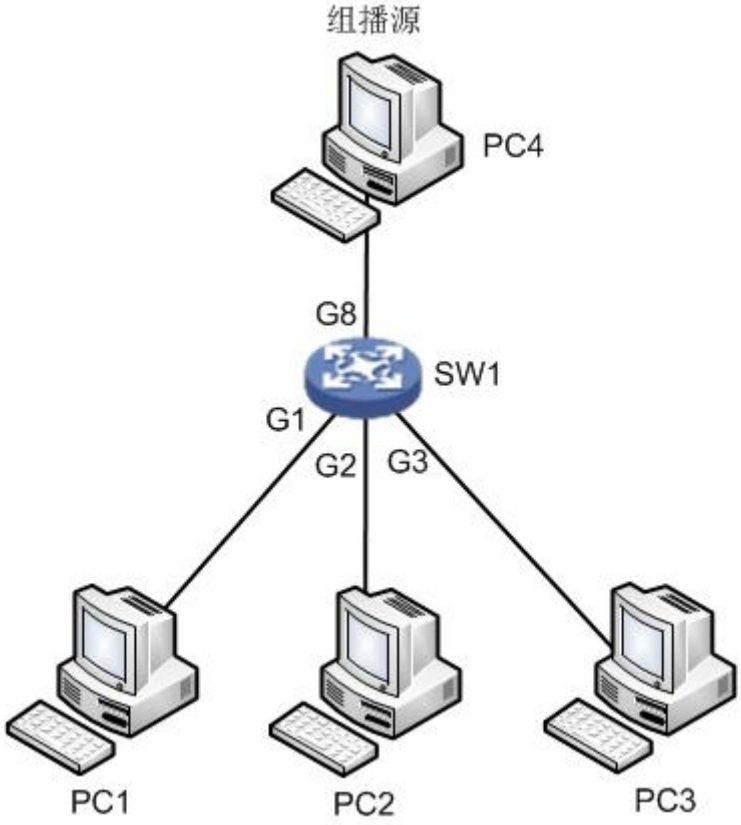


Figure 6-10

Config Example

//Mark vlan 100 as VLAN for multicast source and it is named after it.

```
SWITCH(config)# mvr
SWITCH(config)#mvr vlan 100 name 123
```

//Configure G1 as access port, pvid 10

```
SWITCH(config)#interface GigabitEthernet 1/1
SWITCH(config)#switchport mode access
SWITCH(config)#switchport access vlan 10
```

```
//Add G1 as receiver port, and enable immediate leave .
SWITCH(config-if)#mvr immediate-leave
SWITCH(config-if)#mvr name 123 type receiver
//Configure G2 as access port, pvid 11
SWITCH(config-if)#exit
SWITCH(config)#interface GigabitEthernet 1/2
SWITCH(config)#switchport mode access
SWITCH(config)#switchport access vlan 11
//Add G2 as receiver port, and enable immediate leave.
SWITCH(config-if)#mvr immediate-leave
SWITCH(config-if)#mvr name 123 type receiver
//Configure G8 as access port, pvid 100
SWITCH(config-if)#exit
SWITCH(config)#interface GigabitEthernet 1/8
SWITCH(config)#switchport mode access
SWITCH(config)#switchport access vlan 100
//Add G8 as multicast source port
SWITCH(config-if)#mvr name 123 type source
```

Result Verification

After multicast source starts to play video, you can see that PC1 and PC2 can receive multicast stream, PC3 cannot multicast stream.

6.8 PoE

PoE (Power over Ethernet) config commands are:

poe management mode

poe supply

poe system-power-reserve

poe mode

show poe interface

6.8.1 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.

6.8.2 PoE Management Mode

Command Description

PoE management mode {class-consumption | lldp-consumption}, it is to configure the distribution mode of remaining power.

The distribution mode of remaining mode is class-consumption by default.

Parameters

Parameter	Note
class-consumption	It is to distribute remaining power according to PD level.
lldp-consumption	It is to distribute remaining power according to LLDP.

Command Mode

Overall mode

Example

//It is to configure the distribution of remaining power according to PD level.

```
SWITCH (config) # PoE management mode class-consumption
```

6.8.3 PoE Supply

Command Description

PoE supply <supply_power>, it is to configure port max external output power.

The port max external output power is 115W by default.

Parameters

Supply_power, max external output power, value range is 1~120, the unit is W.

Command Mode

Overall mode

Example

//It is to configure max external output power is 110W.

```
SWITCH (config) # PoE supply 110
```

6.8.4 PoE System-Power-Reserve

Command Description

PoE system-power-reserve < power_reserve>, it is to configure PoE reserved power.

PoE reserved power is 10W by default.

Parameters

Power_reserve, reserved power, value range is 1~120, the unit is W.

Command Mode

Overall mode

Example

//it is to configure reserved power as 15W.

```
SWITCH (config) # PoE system-power-reserve 15
```

6.8.5 PoE Mode

Command Description

PoE mode {standard | plus}, 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.

Parameters

Parameter	Note
standard	General PoE port, max power supports 40W.
plus	Hi-PoE port, max power supports 60W **Note** Only port 1 and port 2 support plus mode, other ports fail to support.

Command Mode

Port mode

Example

//It is to configure port 3 as general PoE port

```
SWITCH (config) #interface Gigabit Ethernet 1/3
SWITCH (config) # PoE mode standard
```

6.8.6 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.

Parameters

Parameters	Note
port_type	Port type
v_port_type_list	Port number

Command Mode

Privilege mode

Example

//It is to configure PoE info of all ports.

```
SWITCH# show poe
```

//It is to configure PoE info of port 1

```
SWITCH# show poe interface GigabitEthernet 1/1
```

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.

Parameters

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.

Parameters

Parameter	Note
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

Overall mode

Example

It is to 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.

Parameters

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

Overall 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.

Parameters

Parameter	Note
conf	Static MAC address added by users
static	Static MAC address table
aging-time	MAC address table aging time

Parameter	Note
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

Privilege mode

Example

//It is to 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.

Parameters

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.

Parameters

Parameter	Note
unicast	Unicast packet, value range 1～1024000
multicast	Multicast packet, value range 1～1024000
broadcast	Broadcast packet, value range 1～1024000

Command Mode

Overall mode

Example

//It is to 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.

Parameters

None

Command Mode

Overall mode

Example

//Enable IP source protection function

```
SWITCH (config)# ip verify source
```

//It is to 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.

Parameters

None

Command Mode

Overall mode

Example

//It is to 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.

Parameters

cnt_var, dynamic client amount, value range 0～2

Command Mode

Port mode

Example

//It is to restrict 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.

Parameters

parameter	Note
port_type	Port type
in_port_type_id	Port number
vlan_var	VLAN number
ipv4_var	IP address
mac_var	Subnet mask

Command Mode

Overall 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.

Parameters

None

Command Mode

Privilege mode

Example

//Check IP source protection config status

```
SWITCH# show IP verify source
```

7.5 ARP Detection Config

ARP detection config 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.

Parameters

None

Command Mode

Overall 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.

Parameters

None

Command Mode

Port mode

Example

//It is to enable the ARP detection function of port 8.

```
SWITCH (config)#interface Gigabit Ethernet 1/8
SWITCH (config-if)#ip arp inspection trust
```

//It is to 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.

Parameters

None

Command Mode

Port mode

Example

//It is to 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.

Parameters

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

Command Mode

Overall 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.

Parameters

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

Command Mode

Overall 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 config info of ARP detection.

Parameters

None

Command Mode

Privilege mode

Example

//Check config info of ARP detection.

```
SWITCH# show ip arp inspection
```

7.6 ACL Config

ACL config 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 config is related to port security (port ACL strategy config) 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

Parameter	Note
ace_id	ACE entry ID, allowed range is 1～256
next	Add new ACE entry in the current ACE entry
ingress interface	Ingress port

Parameter	Note
policy	Strategy config item
vid	VID filter domain config item
tag-priority	vlanTag priority config 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 config option
redirect	Port redirection config option
frame-type	Frame type

Command Mode

Overall mode

Example

//Configure ACL entry

```
SWITCH(config)# access-list ace 1 ingress interface GigabitEthernet 1/1 frame-type ipv4 action deny rate-limiter 1 redirect interface GigabitEthernet 1/2 logging
```

//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 config info of ACE

Parameters

None

Command Mode

Privilege mode

Example

//Check ACE config info

```
SWITCH# show access-list ace statistics
```

7.7 STP Config

STP config 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 config info 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.

Parameters

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.

Parameters

None

Command Mode

Overall 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.

Parameters

Parameter	Note
instance	Value range 0～7
prio	Network bridge priority

Command Mode

Overall 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.

Parameters

Fwdtime, value range is 4s~30s.

Command Mode

Overall 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.

Parameters

Hello time, value range is 1s~10s.

Command Mode

Overall 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.

Parameters

None

Command Mode

Port config

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.

Parameters

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.

Parameters

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.

Parameters

Parameter	Note
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.

Parameters

Parameter	Value
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.

Parameters

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.

Parameters

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 config.

Parameters

Parameters	Note
port_type	Port type
v_port_type_list	Port number
instance	Value range 0～7

Command Mode

Privilege mode

Example

//Check STP config status

```
SWITCH # show spanning-tree
```

7.7.15 STP Config 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 elected as root network bridge.

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

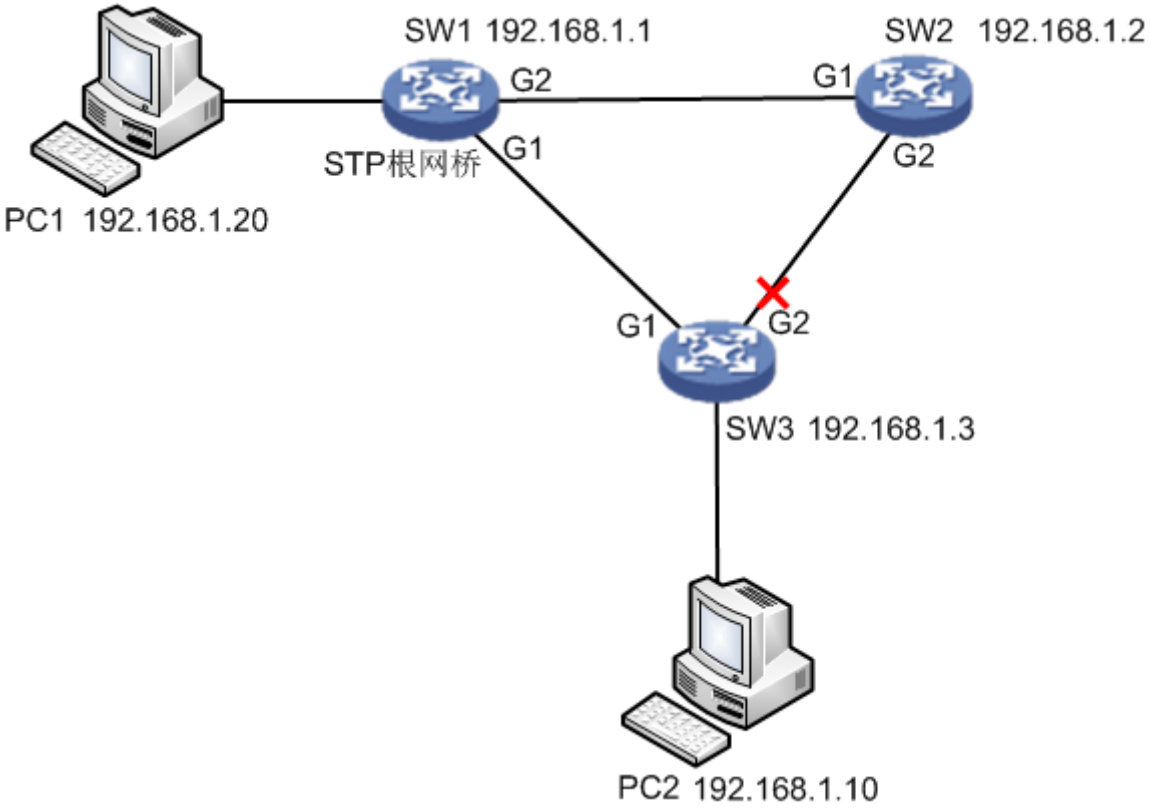


Figure 7-1

Config 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
```

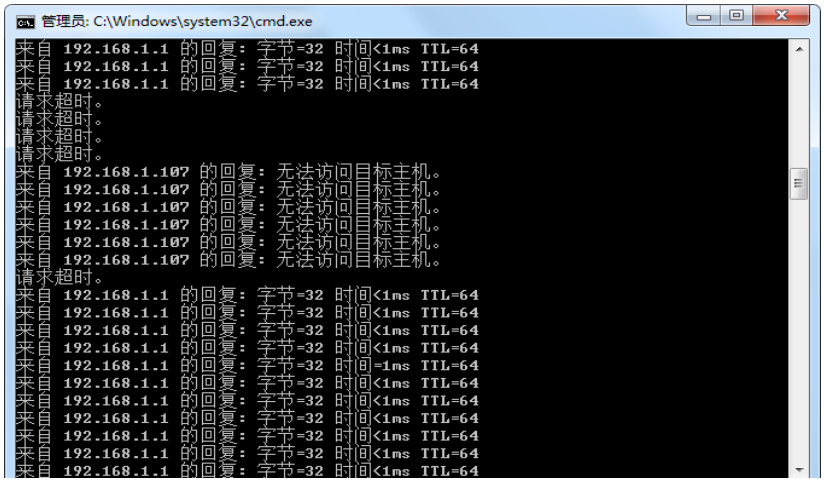
SW3：

```
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 config commands are:

loop-protect

loop-protect tx-mode

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 overall or port loop protection function.

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

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

Parameters

None

Command Mode

Overall mode/port mode

Example

//Enable overall 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.

Parameters

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.

Parameters

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

Command Mode

Overall mode

Example

//It is to 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.

Parameters

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

Command Mode

Overall mode

Example

//It is to 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.

Parameters

Parameter	Note
port_type	Port type
plist	Port number

Command Mode

Privilege mode

Example

//It is to 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 overall loop protection status.

Parameters

None

Command Mode

Privilege mode

Example

//Check overall 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.

The loop protection can realize fast switch when

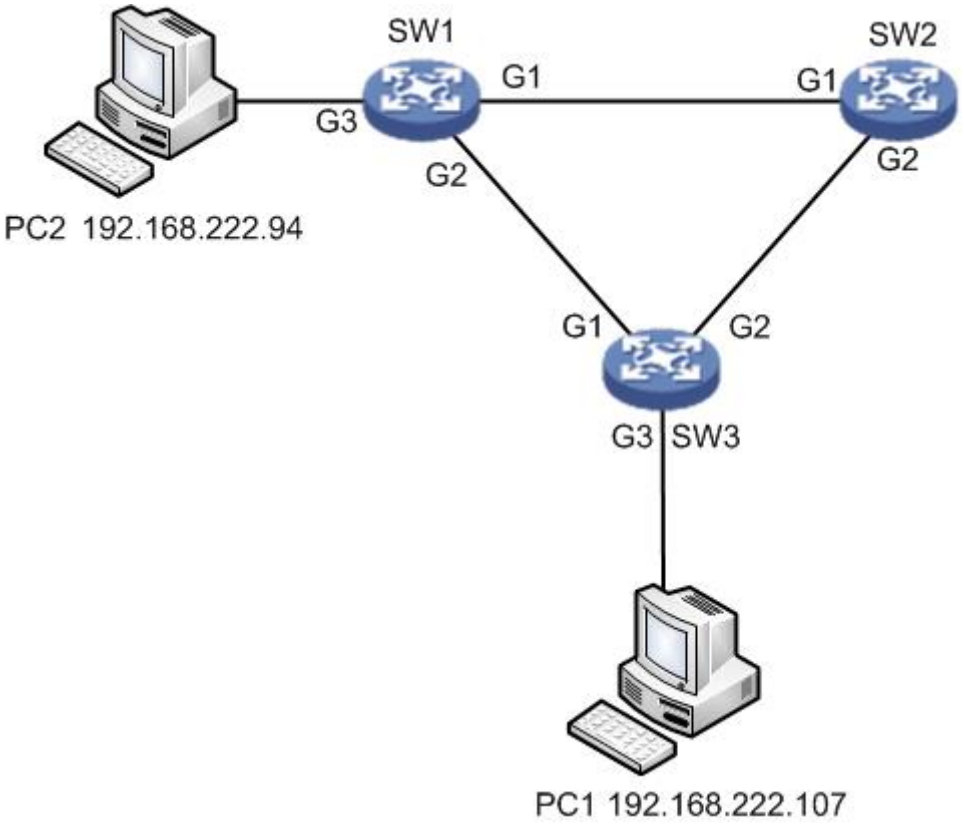


Figure 7-2

Config Example

SW1：

//Enable overall 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.

Note

- 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.

8 Network Management Command

8.1 SSH Config

SSH config 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.

Parameters

None

Command Mode

Overall mode

Example

//It is to enable SSH function

```
SWITCH (config)# ip ssh
```

8.2 HTTPS Config

HTTPS config 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.

Parameters

None

Command Mode

Overall mode

Example

//It is to 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

Overall mode

Example

//It is to 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.

Parameters

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

Command Mode

Overall mode

Example

//Generate secure certificate

```
SWITCH (config)# ip http secure-certificate generate
```

8.3 LLDP Config

LLDP config commands are:

lldp

lldp holdtime

lldp transmission-delay

lldp timer

lldp reinit

show lldp neighbors

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 lldp

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 disabled 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.

Parameters

Val, value range is 2S~10S.

Command Mode

Overall 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

Parameters

Val, the value range is 1s~8192s.

Command Mode

Overall 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.

Parameters

Val, value range is 5s~32768s.

Command Mode

Overall mode

Example

//It is to 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.

Parameters

Val, value range is 1s~10s.

Command Mode

Overall mode

Example

//It is to 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.

Parameters

None

Command Mode

Privilege mode

Example

//It is to display brief info of neighbor

```
SWITCH# show lldp neighbors
```

8.4 802.1x Config

802.1x config commands are:

dot1x system-auth-control

radius-server host

dot1x port-control

dot1x re-authentication

dot1x authentication timer re-authenticate

show dot1x statistics

Note

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.

Parameters

None

Command Mode

Overall 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.

Parameters

parameters	Note
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

//It is to 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.

Parameters

Parameter	Note
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.

Parameters

None

Command Mode

Overall 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.

Parameters

v_1_to_3600, value range is 1s～3600s

Command Mode

Overall 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.

Parameters

Parameter	Note
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

Privilege mode

Example

//Check all ports authentication statistics

```
SWITCH# show dot1x statistics all
```

8.4.8 802.1x Config Example

Networking Requirement

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

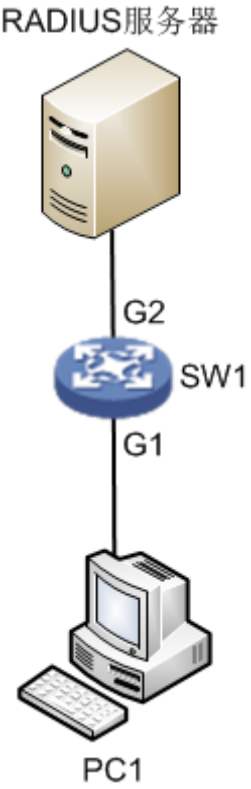


Figure 8-1

Config Example

//Enable overall 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

Note

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 Config

SNMP config 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 enabled by default.

Parameters

None

Command Mode

Overall 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.

Parameters

Parameter	Note
source_name	Function name, include following options: alarmTrapStatus authenticationFailure coldStart entConfigChange fallingAlarm ipTrapInterfacesLink linkDown linkUp lldpRemTablesChange newRoot psecTrap risingAlarm topologyChange warmStart

Command Mode

Overall mode

Example

//Add linkup event

```
SWITCH(config)# snmp-server trap linkup
```

8.5.4 SNMP-Server Community

Command Description

snmp-server community, configure authentication name and community

Parameters

Ro: Read only

Rw: read write

Default

Public

Command mode

Overall mode

Example

//Version is v2c, authentication name is 123, community is read only

```
SWITCH(config)# snmp-server community v2c 123 ro
```

8.5.5 SNMP-Server Host

Command Description

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

Parameters

conf_name, host name

Command Mode

Overall mode

Example

//Config host name is 1111

```
SWITCH(config)# snmp-server host 1111
```

8.5.6 Host

Command Description

Hostname <hostname>, configure host name.

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

Parameters

Parameter	Note
hostname	Host name
v_ipv4_ucast	Host address

Command Mode

Overall mode

Example

//Configure host name as 1111

```
SWITCH(config)#snmp-server host 1111
```

//Configure host address

```
SWITCH(config-snmps-host)# host 192.168.111.111
```

8.5.7 SNMP Config 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.

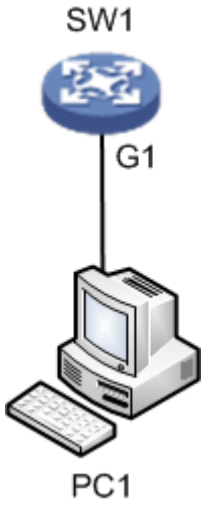


Figure 8-2

Config Example

SW1：

//Configure SNMP read write community

```
SWITCH(config)#snmp-server
SWITCH(config)#snmp-server community v2c 123 ro
SWITCH(config)#snmp-server community v2c 123 rw
```

//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
```

PC1:

Step 1

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

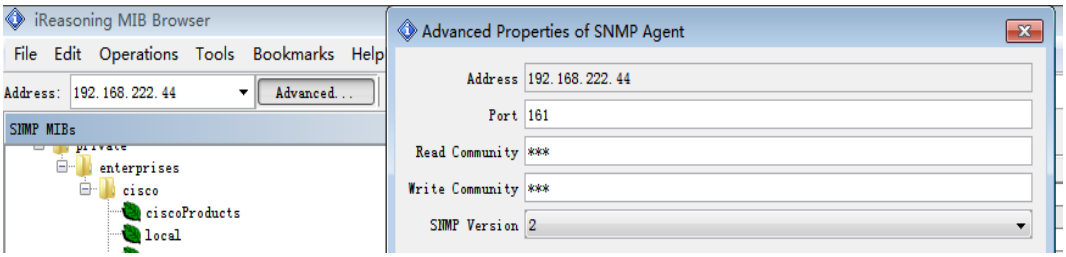


Figure 8-3

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.

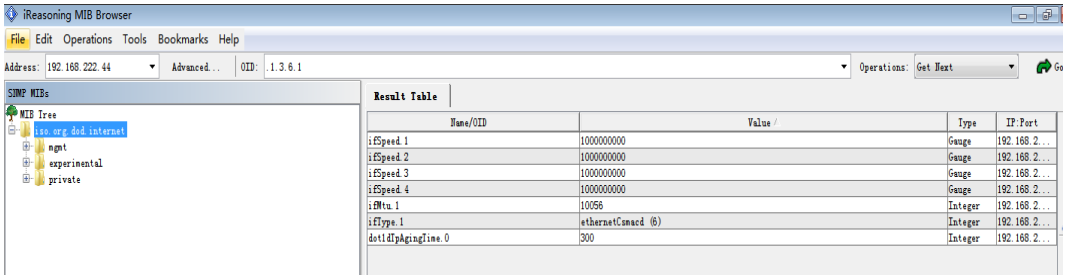


Figure 8-4

Step 3

Select “Tools>Trap Receive”, you can check uploaded Trap info, which is shown in Figure 8-5.

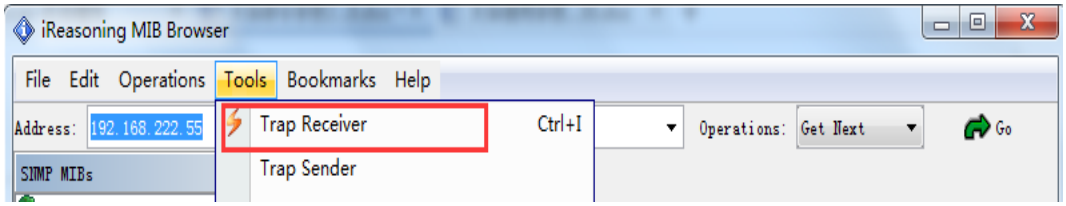


Figure 8-5

8.6 RMON Config

RMON CLI config 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.

Note

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.

Parameters

Parameters	Note
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

Overall 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.

Parameters

Parameter	Note
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> 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.

Parameters

Parameter	Note0
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
ifIndex	Corresponding port of bridging port
rising_threshold	Threshold upper limit

Parameter	Note0
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

Overall mode

Example

//It is to 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.

Parameters

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.

Parameters

None

Command Mode

Privilege mode

Example

//It restarts the device after saving config.

```
SWITCH# copy running-config startup-config
SWITCH# reload cold
```

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.

Parameters

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

Command Mode

Privilege mode

Example

//Restore factory default config, it will be valid after the device reboots.

```
SWITCH# reload defaults
```

9.3 Save Config

9.3.1 Function Introduction

The module can be used to save config.

9.3.2 Copy Running-Config Startup-config

Command Description

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

Parameters

None

Command Mode

Privilege mode

Example

//Save config

```
SWITCH#copy running-config startup-config
```

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.

Parameters

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

Command Mode

Privilege mode

Example

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

```
SWITCH# ping ip 192.168.255.3
```

Note

- This quick start guide is for reference only. Slight difference may be found in user interface.
- All the designs and software here are subject to change without prior written notice.
- If there is any uncertainty or controversy, please refer to the final explanation of us.
- Please visit our website or contact your local service engineer for more information.

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address：No.1199 Bin'an Road, Binjiang District, Hangzhou, PRC.
Postcode: 310053
Tel: +86-571-87688883
Fax: +86-571-87688815
Email:overseas@dahuatech.com
Website: www.dahuasecurity.com