Industrial Ethernet Switch Command Line Manual

Contents

CHAPTER 1 MANAGEMENT 5
1.1. MANAGEMENT METHOD 5
1.1.1. Out of Band Management 5
1.1.2. In-band Management 8
1.2. MANAGEMENT INTERFACE 11
1.2.1. CLI Interface 11
1.2.2. WEB Interface 16
CHAPTER 2 BASIC CONFIGURATION 16
2.1. BASIC CONFIGURATION COMMAND 16
2.1.1. config 16
2.1.2. add user 16
2.1.3. exit 17
2.1.4. help 17
2.1.5. hostname 17
2.1.6. Reload cold 18
2.1.7. reload default 18
2.1.8. copy 18
2.2. MAINTENANCE AND COMMISSIONING COMMANDS 19
2.2.1. ping 19
2.2.2. show 19
2.3. TELNET 20
2.3.1. Telnet Introduction 20
2.3.2. Telnet Task sequence 21
2.4. CONFIGURE THE IP ADDRESS OF THE SWITCH 21
2.4.1. Configure the IP address task sequence of the switch 22
2.4.2. Configuring the IP Address of the Switch 22
2.5. SNMP CONFIGURATION 23
2.5.1. SNMP Introduction 23
2.5.2. MIB Introduction 24
2.5.3. RMON Introduction 25
2.5.4. SNMP configuration 26
2.5.5. SNMP Typical configuration example 29
2.6. ALARM 30
2.6.1. Introduction 30
2.6.2. Alarm task sequence 30
2.7. LOG MANAGEMENT 31
2.7.1. Introduction 31
2.7.2. Log management task sequence 31
CHAPTER 3 PORT CONFIGURATION 32
3.1. PORT INTRODUCTION 32
3.2. PORT CONFIGURATION 32
3.2.1. Ethernet port configuration 32

3.2.2. Mirror configuration 35
3.3. PORT TROUBLESHOOTING HELP 37
3.3.1. Monitoring and debugging commands 37
3.3.2. Port troubleshooting help 38
CHAPTER 4 MAC ADDRESS TABLE CONFIGURATION 39
4.1. MAC ADDRESS TABLE INTRODUCTION 39
4.1.1. MAC address table to obtain 39
4.1.2. Forward or filter 40
4.2. MAC ADDRESS TABLE CONFIGURATION 41
4.2.1. mac address-table aging-time 41
4.2.2. mac address-table 41
4.3. MAC ADDRESS LEARNING CONFIGURATION 42
4.3.1. mac address-table learning 42
4.3.2. mac address-table learning vlan 42
4.4. TROUBLESHOOTING HELP 43
4.4.1. Monitoring and debugging commands 43
4.4.2. Troubleshooting help 43
CHAPTER 5 VLAN CONFIGURATION 45
5.1. VLAN INTRODUCTION 45
5.2. VLAN CONFIGURATION 46
5.2.1. VLAN configuration task sequence 46
5.2.2. VLAN configuration command 47
5.2.3. VLAN typical application 50
5.3. VLAN TROUBLESHOOTING HELP 51
5.3.1. Monitoring and debugging information 51
CHAPTER 6 IGMP SNOOPING CONFIGURATION 53
6.1. IGMP SNOOPING INTRODUCTION 53
6.2. IGMP SNOOPING CONFIGURATION 53
6.2.1. IGMP Snooping Configuration tasks 53
6.2.2. IGMP Snooping configuration command 54
6.3. IGMP SNOOPING EXAMPLE 54
6.4. IGMP SNOOPING TROUBLESHOOTING HELP 56
6.4.1. Monitoring and debugging commands 56
CHAPTER 7 ACL CONFIGURATION 57
7.1. ACL OVERVIEW 57
7.1.1. Access-list 57
7.1.2. Access-list Action 57
7.2. ACL CONFIGURATION 57
7.2.1. ACL Configuring task sequences 57
7.2.2. ACL Setting Demand 60
CHAPTER 8 QOS CONFIGURATION 65
8.1. QOS OVERVIEW 65
8.1.1. QoS term 65
8.2. QOS CONFIGURATION 66

8.2.1. QoS Configure the task sequence 66
8.2.2. QoS Configuration command 68
8.3. QoS EXAMPLE 72
CHAPTER 9 RSTP CONFIGURATION 74
9.1. INTRODUCTION 74
9.2. BASIC CONCEPT 74
9.3. BPDU CONFIGURATION MESSAGE 74
9.4. IMPLEMENTATION PROCESS 75
9.5. RSTP CONFIGURATION 76
9.5.1. RSTP configuration task 76
9.6. CONFIGURATION EXAMPLE 79
CHAPTER 10 HSTW-RING CONFIGURATION 81
10.1. INTRODUCTION 81
10.2. CONCEPT 81
10.3. IMPLEMENTATION 81
10.4. HSTW-RING CONFIGURATION 83
10.4.1. HSTW-Ring configuration task 83
10.4.2. Precautions 84
Chapter 11 ERPS（ Ethernet Ring Protection Switching） 85
11.1. ERPS FUNCTION CONFIGURATION 85
11.2. ERPS CONFIGURATION COMMAND 87
Chapter 12 L3 Routing Protocol 859
12.1. L3 FORWARDING 859
12.2. LAYER3 INTERFACE INTRODUCTION 879
12.3. ROUTING PROTOCOL 90
12.4 RIP INTRODUCTION 98
12.5 OSPF INTRODUCTION 110
12.6 INTRODUCTION OF VRRP 117

Chapter 1 Management

1.1. Management method

After the user purchases the switch, the switch needs to be configured to manage the network. To provide users with two management methods: out of band management and in-band management.

1.1.1. Out of Band Management

Out-of-band management is managed through the console port.

The procedure for managing the console port is as follows

1.1.1.1. Building Environment

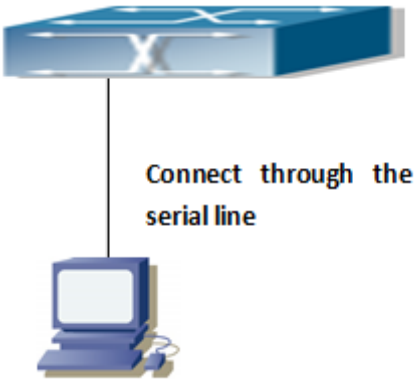


Figure 1-1 out of band management configuration environment

As shown in Figure 1-1, connect the PC's serial port (RS-232 interface) and the switch through serial cable. The following is a description of the device used in the connection:

Name	Specification
PC	There are intact keyboard and RS-232 serial port, and install the terminal emulation program
Serial line	One end connected with the PC's RS-232 serial port; the other end is connected with the console port of the switch.
Ethernet Switch	There is a good console port.

1.1.1.2. Enter HyperTerminal

Open the Windows system comes with HyperTerminal. The following is an example of opening Windows XP with HyperTerminal.

1. Click on the HyperTerminal:

Figure 1- 2 Open the HyperTerminal 1

2. Enter the name of the HyperTerminal at "Name", such as Define it as "Switch":

Figure 1-1 Open the HyperTerminal 2

3. In the "connect using", select the PC using the RS-232 serial port, such as the connection is the COM 4, then select the COM 4, click “ OK” .

Figure 1-2 Open the HyperTerminal 3

4. The COM4 attribute, the baud rate selects "115200", the data bit selects "8", the parity selects "no", the stop bit selects "1", the flow control selects "no", click “OK”.

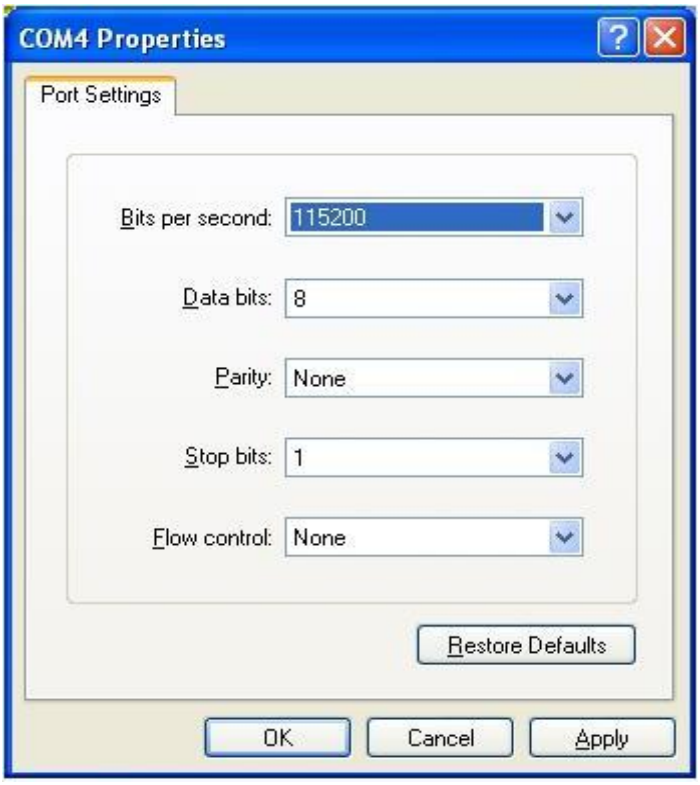


Figure 1-3 Open the HyperTerminal 4

5. Appears super terminal configuration interface, enter the default user name: admin, password:123

Figure 1-4 Open the HyperTerminal 5

1.1.2. In-band Management

In-band management (In-band management), that is, through the Telnet program to log on to the switch, or SSH configuration management of the switch. The switch provides in-band management that allows some devices connected to the switch to have the capability to manage the switch. When the switch configuration changes, resulting in in-band management failure, you can use out-of-band management of the switch configuration management

1.1.2.1. Manage the switch through Telnet

To manage the switch through Telnet:

1. Configuration IP address;

2. The IP address of the host as the Telnet client is the same as the IP address of the VLAN interface of the switch.

3. If it does not meet 2), the Telnet client can reach the IP address of the switch through a router or other device.

The switch can be configured with multiple IP addresses.

The following are the steps for the Telnet client Telnet to the VLAN1 interface of the switch:

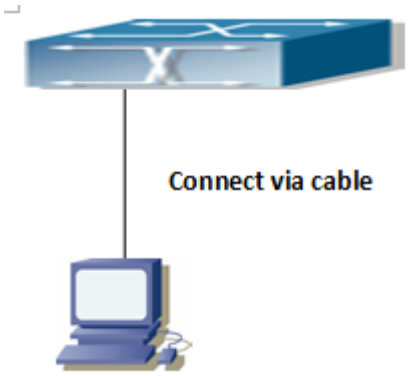


Figure 1-7 Manage the switch through Telnet

First: Configure the IP address.

First configure the IP address of the host to be in the same network segment as the VLAN 1 interface IP address of the switch. If the IP address of VLAN1 interface on the switch is 192.168.1.5, you can set the IP address of the host to 192.168.1.100. On the host, execute the "ping 192.168.1.5" command to show whether the ping succeeds; if the ping fails, check the cause.

The following describes the IP address configuration commands of the VLAN 1 interface on the switch. Before configuring in-band management, you must configure the IP address of the switch through outbound management or console port. The configuration commands are as follows:

configure terminal
(config)# interface vlan 1
(config-if-vlan)# ip address 192.168.1.5 255.255.255.0
(config-if-vlan)# exit
(config)# exit
copy running-config startup-config
Building configuration...
% Saving 2239 bytes to flash:startup-config

Second: Run the Telnet client program.

Run the Telnet client program that comes with Windows and specify the destination address for Telnet.

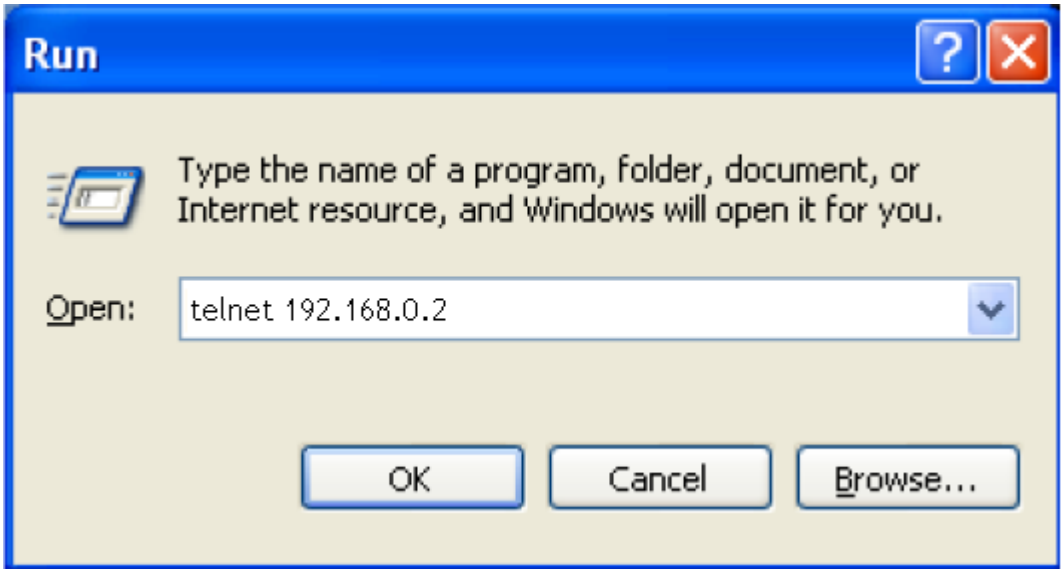


Figure 1- 8 running Windows comes with the telnet client program

Third: Log on the switch.

To log in to the Telnet configuration interface, you need to enter the correct login name and password, otherwise the switch will deny access to the Telnet user. This is to protect the switch from unauthorized operation by unauthorized users. If the switch does not have an authorized Telnet user, no user can access the CLI configuration interface of the switch. So the Telnet configuration interface, enter the correct login name and password, the default user: admin, password: 123; Telnet users can successfully enter the CLI configuration interface to the switch. After Telnet is logged in, the commands used to log in through the console port are exactly the same.

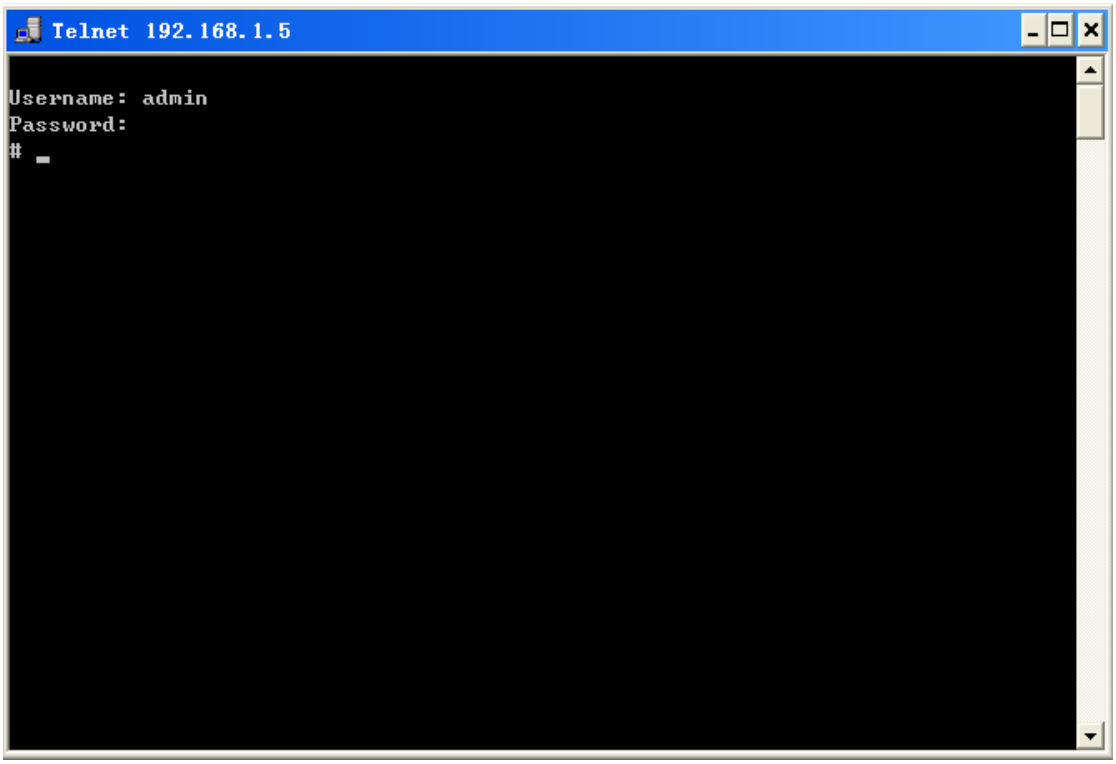


Figure 1-5 Telnet Configuration Interface

1.1.2.2. Manage the Switch Through SSH

The conditions under which the switch can be managed by SSH:

1. Configuration IP address;

2. The IP address of the host as the client is the same as the IP address of the VLAN interface of the switch.

3. If it does not meet 2), the client can reach the IP address of the switch through a router or other device.

The host must be able to ping the IP address of the switch so that the SSH client is running to manage the switch device. For details, how to manage the switch through SSH. Refer to the SSH Configuration section.

1.2. Management Interface

TR-IES 3500 Series Switch provide users with two management interface: CLI (Command Line Interfac) command line interface, web management interface. We will make a detailed introduction to the CLI interface,

1.2.1. CLI Interface

Users are familiar with the CLI interface, we mentioned in front of the band management,

Telnet login to the switch through the CLI interface configuration management of the switch.

1.2.1.1. Configuration Mode Introduction

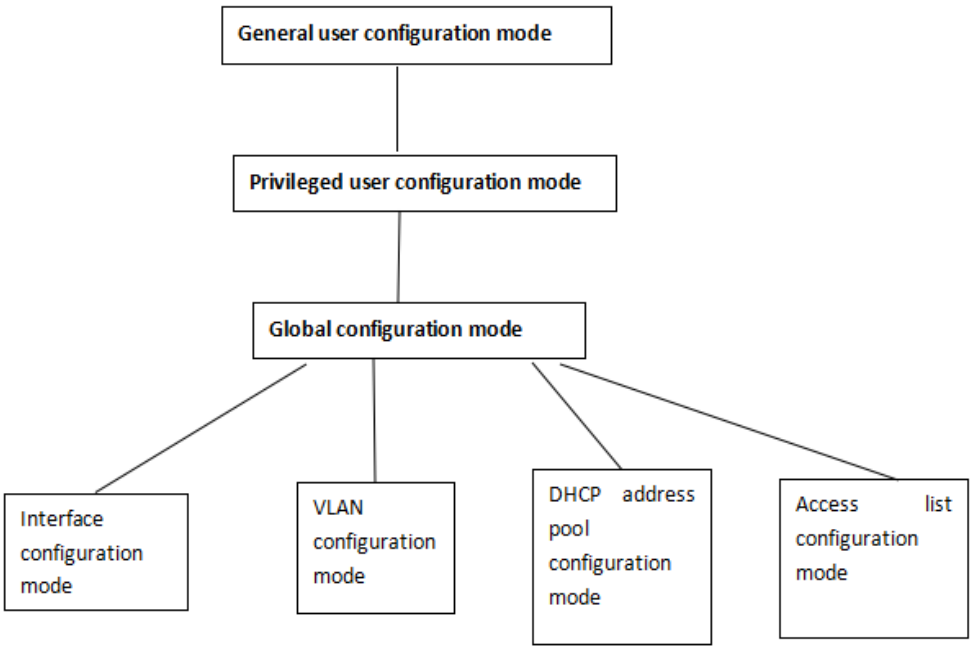


Figure 1-6 CLI Configuration Mode

1.2.1.1.1. Privileged user configuration mode

User enter the corresponding privileged user password to enter the privileged user configuration mode **" #"**. When the user exits from the global configuration mode by **exit**, you can also return to the privileged user configuration mode. In addition to provide "Ctrl + z" shortcut keys, so that the switch in any configuration mode (except for the general user configuration mode), can be returned to the privileged user configuration mode.

In the privileged user configuration mode, the user can query the switch configuration information, the connection of each port, send and receive data statistics. And enter the privileged user configuration mode, you can enter the global mode to modify the configuration of the switch.....

Global configuration mode

After entering the privileged user configuration mode, simply use the command **config termial** to enter the global configuration mode "**(Config)** #". You can use the command exit to return to the global configuration mode when the user is configured in other configuration modes, such as interface configuration mode and VLAN configuration mode.

In the global configuration mode, you can configure the switch globally, such as MAC

address table, port mirroring, VLAN creation, and IGMP Snooping, GVMP, and STP. Users in the global mode can also enter the port through the command to configure the port.

1.2.1.1.2. Interface configuration mode

In the global configuration mode, you can use the command **interface** to enter the corresponding interface configuration mode. There are two types of ports: 1.VLAN interface; 2. Ethernet port; so there are two interface configuration mode.

Type of Interface	Way of entry	Prompt	Executable operations
VLAN interface	In the global configuration mode, enter the command: **interface vlan <*Vlan-id*>**。	**(config-if-vlan) #**	Configure the IP of the switch
Ehthernet interface	In the global configuration mode, enter the command: **Interface GigabitEthernet <*port_type_list*>** **interface FastEthernet <*port_type_list*>** **interface 2.5GigabitEthernet <*port_type_list*>**	**(config-if)#**	Configure the duplex mode, rate, and so on of the Ethernet interface provided by the switch.

1.2.1.1.3. VLAN Configuration Mode

In the global configuration mode, you can use the command **vlan** <**vlan-id**> to enter the corresponding VLAN configuration mode. In VLAN configuration mode, you can configure a member port that belongs to this VLAN. Execute the **exit** command to return from the VLAN configuration mode to the global configuration mode.

1.2.1.1.4. DHCP Address Pool Configuration Mode

In the global configuration mode, use the **ip dhcp pool** <**name**> command to enter the DHCP address pool configuration mode "**(Config-<*name*>-dhcp)#**". You can configure the attributes of the DHCP address pool in the DHCP address pool configuration mode. Execute the "exit" command to return to the global configuration mode from the DHCP address pool configuration mode.

1.2.1.2. Configuration grammar

Provides users with a variety of configuration commands, although these configuration commands in different forms, but they follow the configuration command syntax. The following is the general command format provided by the switch:

cmdtxt <*variable*> { enum1 | … | enumN } [option]

Grammar description: Boldface **cmdtxt** Indicates a command keyword; **<*variable*>**Indicates that the parameter is a variable; **{enum1 | … | enumN }** Expressed in the parameter set **enum1~enumN.** You must select a parameter; in **[option],** "**[ ]**"Indicates that the parameter is optional. In a variety of orders will appear"< >", "**{ }**", "**[ ]**"Symbols are used in combination, such as: **[<*variable*>]**, **{enum1 <*variable*>| enum2}**, **[option1 [option2]]** etc.

Here are a few examples of configuration command syntax analysis:

- show version, There is no parameter, only the keyword has no parameters of the command, you can directly enter the command;
- vlan <vlan-id>, After entering the keyword, you also need to enter the corresponding parameter value;

1.2.1.3. Support shortcuts

In order to facilitate the user's configuration, in particular, provides a number of shortcut keys, such as above, under, left, right key and delete key BackSpace and so on. If the HyperTerminal does not support the cursor keys up and down, you can use ctrl + p and ctrl + n to replace.

Button	Function	
BackSpace	Delete the previous character of the cursor position, move the cursor forward	
"↑"	Displays the previous input command. You can display up to ten commands that have been entered recently	
"↓"	The next input command is displayed. When you use the cursor keys to go back to previously entered commands, you can also use the lower cursor keys to return to the next command relative to the previous command	
"←"	The cursor moves one position to the left	Use the left and right keys to make changes to the commands that have been entered
"→"	The cursor moves one position to the right	
Ctr+p	Relative to the cursor on the " ↑ " role	
Ctr+b	Relative to the cursor key "←" role	
Ctr+f	Relative to the cursor key "→" role	

Ctr+z	From other configuration modes (except for general user configuration mode) to the privileged user mode
Tab button	When the input string can be a conflict without a command or keyword, you can use the Tab key to add it as a complete command or keyword

1.2.1.4. Help function

The TR-IES 3500 Series switches provide users with a way to get help information, that is to use "?"" Command.

Help	Use methods and functions
Help	In any command mode, enter the "help" command to get a brief description of the help system.
“? ”	1. In any command mode, enter "?" To get all the commands in the command mode and their brief description; 2. After the keyword of the command, enter the space-separated "?", If the location is a parameter, the output of the parameter type, range, etc. description; if the location is a keyword, the list of keywords and its Simple description; if the output "<cr>", this command has been entered complete, where you can enter a carriage return. 3. After the string is followed by "?", All the commands beginning with the string are listed.

1.2.1.5. Support does not match exactly

CLI supports not exactly match the search commands and keywords, and when you enter a conflicting command or keyword, the CLI is parsed correctly.

Example：

1. For the privileged user configuration command "show interface 2.5GigabitEthernet 1/1 description", h in 2 1/1 d".

2. For the privileged user configuration command "show running-config", if only "sh r" is entered, the system will report "% Ambiguous word detected at '^' marker.”" Because the shell can not distinguish "show r" from "show rom" or "show running -config "command, so you must enter" sh ru ", Shell will be the correct analysis.

1.2.2. WEB Interface

The switch provides HTTP or HTTPS web management, the default is HTTP. Through the web browser, the user can configure the switch and detect the behavior of the switch.

You can through the following operations, to achieve through the web browser to manage the switch:

1. Configure a valid IP address and address mask for the switch.

2. Configure the management user, user password.

3. Through the Web browser on the switch connection, enter the user name, password, then you can through the Web on the switch

To manage.

1.2.2.1. WEB Home

When you enter the user name, password, verification code, after verification, you can see the following web management home page. Click the main menu link to browse other management links and display the configuration and statistics.

Chapter 2 **Basic Configuration**

2.1. Basic configuration command

The basic configuration of the switch includes commands such as entering and exiting the privileged user mode, entering and exiting the interface configuration mode, setting and displaying the clock of the switch, displaying the system version information of the switch, and so on.

2.1.1. config

Conmmand：config [terminal]

Function： From the privileged user configuration mode to the global configuration mode.

Parameter：[terminal] Indicates that the terminal is configured.

Command mode： Privileged user configuration mode

Example：

#con t

2.1.2. add user

Command：

1、username <username> privilege <priv> password none

2、username <username> privilege <priv> password unencrypted <password>

Function: Add or modify the user and password of the privileged user configuration mode. There is no password in command 1, and password is not encrypted in command 2

Command mode: global configuration mode

Default: The system defaults to admin and the password is empty.

Usage Guide: Configure a privileged user password to prevent unauthorized intrusion by nonprivileged users. It is recommended that the network administrator modify the privileged user password when configuring the switch for the first time. Also, when the administrator needs to leave the terminal for a long time, it is best to execute the exit command to exit the privileged user configuration mode.

Example: Set the password for the privileged user admin to admin.

(config)# username admin privilege 15 password unencrypted admin

2.1.3. exit

Command：exit

Function： From the current mode, enter the previous mode, such as in the global configuration mode using this command to return to the privileged user configuration mode, in the privileged user configuration mode using this command to return to the general user configuration mode.

Command mode： Various configuration modes

Example：

(config)#exit

#

2.1.4. help

Command：help

Function: Outputs a brief description of the command interpreter help system.

Command mode: Various configuration modes

Usage Guide: The switch provides online help anytime, anywhere. The help command displays information about the entire help system, including full help and some help, where users can type ? anytime, anywhere. Get online help.

For example:

2.1.5. hostname

Command：hostname <*hostname*>

Function: Sets the prompt for the switch's command line interface.

Parameters: <hostname> is a string of prompts, up to 30 characters long.

Command mode: global configuration mode

Default: The system default is "".

Usage Guide: This command allows the user to set the prompt for the switch command line

according to the actual situation.

Example: Set the prompt to Test.

(Config)#hostname Test

Test(Config)#

2.1.6. Reload cold

Command：reload cold

Function: Reboot the switch.

Command mode: Privileged user configuration mode

Usage Guide: The user can use this command to restart the switch without shutting down the power supply.

2.1.7. reload default

Command：1、reload default

2、reload defaults keep-ip

Function: Restore the factory settings of the switch.

Command mode: privileged user configuration mode, command 1 device restore factory configuration, including device management IP, command 2 device restore factory settings, but device management IP does not change

Usage Guide: Restore the factory settings of the switch, that is, the user to do all the configuration of the switch are gone, the user restart the switch, the prompt appears the same as the switch for the first time.

For example:

reload defaults keep-ip

% Reloading defaults, attempting to keep VLAN 1 IP address. Please stand by.

After this command is executed, the device restores the factory settings, but VLAN 1 IP remains the original IP.

2.1.8. copy

Command：copy running-config startup-config

Function: Save the current runtime configuration parameters to Flash Memory.

Command mode: Privileged user configuration mode

Usage Guide: When you complete a set of configurations and have reached the intended function, you should save the current configuration to Flash so that the system can automatically revert to the previously saved configuration when you shut down or power off.

For example:

 # copy running-config startup-config

Building configuration...

% Saving 1522 bytes to flash:startup-config

2.2. Maintenance and commissioning commands

When the user configures the switch, it is necessary to check whether the configuration is correct and whether the switch is working properly. If the network fails, the user needs to diagnose the fault. This provides ping, telnet, show ect debugging commands, To help users view the system configuration, running status, find the cause of the malfunction.

2.2.1. ping

Command：ping ip { <v_ip_addr> | <v_ip_name> } [repeat <count>] [size <size>] [interval <seconds>]

Function: The switch sends an ICMP request packet to the remote device to check whether the switch is reachable with the remote device.

Parameters: <ip-addr> is the IP address of the destination host to ping, dotted in decimal format.

Default: 5 ICMP request packets; packet size is 56 bytes ;.

Command mode: Privileged user configuration mode

Usage Guide: When the user enters the ping command, you can detect the connection status of the switch to the target host based on the result.

For example:

#ping ip 192.168.0.200 repeat 6 size 64 interval 2

Ping destination **IP:192,168.0.2 , Repeat 6 times, the size of 64 bytes, the interval is 2s**

2.2.2. show

The show command is used to display the system information, port information, protocol operation, and so on. This section describes the show command for the display system information of the switch. Other show commands are described in the relevant sections.

-

2.2.2.1. show running-config

Command：show running-config

Function: Displays the switch parameter configuration that takes effect in the current running state.

Default: The configuration parameters that are in effect are not displayed if they are the same as the default operating parameters.

Command mode: Privileged user configuration mode

Usage Guide: When the user completes a set of configurations and needs to verify that the

configuration is correct, you can run the show running-config command to view the currently valid parameters

.For example:

#show running-config

2.2.2.2. show users

Command：show users

Function: Displays information about the current user with the switch.

Usage Guide: This command is used to view the information of the user who is currently logged in to the system.

For example:

#show user

2.2.2.3. show version

Command：show version

Function: Displays the switch version information.

Command mode: Privileged user configuration mode

Usage Guide: Use this command to view the version information of the switch, including the hardware version and software version information.

2.3. Telnet

2.3.1. Telnet Introduction

Telnet remote login is a simple remote terminal protocol. The user can register with Telnet (ie, log on) to another remote host (using an IP address or host name) at their location. Telnet can pass the user's keystrokes to the remote host, but also can return the remote host's output through the TCP connection to the user screen. This service is transparent because the user feels that the keyboard and the monitor are directly connected to the remote host.

Telnet uses the client-server mode, the local system is the Telnet client, and the remote host is the Telnet server. Either as a Telnet server or as a Telnet client.

When the switch serves as a Telnet server, the user can log in to the switch through the Telnet client software that comes with Windows or other operating system, as described in the Inline Management section earlier. When the switch serves as a Telnet server, you can establish a TCP connection with up to five Telnet clients at the same time.

When used as a Telnet client, you can use the telnet command to log in to other remote hosts in the privileged user configuration mode of the switch. When the switch as a Telnet client can only establish a TCP connection with a remote host, if you want to establish a connection with

another remote host, you must first disconnect the TCP connection from the previous remote host.

2.3.2. Telnet Task sequence

1. Configure Telnet Server
2. Telnet to the remote host

1. Configure Telnet server

Command	Explanation
Global configuration mode	
aaa authentication login telnet local **no aaa authentication login telnet**	Open the Telnet server function of the switch; the no operation of this command is to disable the Telnet server function.
username <username> privilege <priv> password unencrypted <password> **no username <username>**	Configure Telnet to log in to the user name and password of the switch; delete the authorized Telnet user.
access management **access management <access_id> <access_vid> <start_addr> [to <end_addr>] { [web] [snmp] [telnet] | all }**	Configure the secure IP address that allows Telnet to log in to the switch.
no access management **no access management <access_id_list>**	The no operation of this command is to delete the authorized Telnet security address.

2.4. Configure the IP address of the switch

All Ethernet interfaces on the switch default to Layer 2 (DataLink Layer) ports for Layer 2 forwarding. The IP address is also the IP address of the switch. VLAN-related configuration commands can be configured in VLAN interface mode. Provide users with three ways to configure IP addresses:

- manual configuration
- DHCP way

Manually configure the IP address, that is, the user assigns an IP address to the switch.

DHCP is the DHCP client as the DHCP client, and sends the request packet to the DHCP server. The DHCP server sends the address to the switch after receiving the request. In addition, it

also has the function of DHCP server, which can dynamically allocate network parameters such as IP address, gateway address and DNS server address for the DHCP client. The configuration of the specific DHCP server is described in the following sections.

2.4.1. Configure the IP address task sequence of the switch

1. Manual configuration
2. DHCP

1. Manual configuration

Command	Explanation
ip address <*ip_address*> <*mask*> **no ip address**	Configure the IP address of the VLAN interface of the switch. The no operation of this command is to remove the IP address of the VLAN interface of the switch.

2. DHCP

Command	Explanation
ip address dhcp fallback <fallback_address> <fallback_netmask>timeout<fallback_timeout> **no ip address dhcp**	Enable the DHCP client to obtain the IP address and gateway address through DHCP negotiation. When the IP timeout is dynamically acquired, the device IP can become a pre-preset IP. The no operation of this command is to disable the DHCP client function.

2.4.2. Configuring the IP Address of the Switch

2.4.2.1. ip address

Command：ip address <*ip-address*> <*mask*>

no ip address

Function: Set the IP address and mask of the specified VLAN interface of the switch. The no operation of this command is to delete the IP address.

Parameters: <ip-address> is the IP address, dotted in decimal format; <mask> is the subnet mask, dotted in decimal format;

Default: The switch has a default IP address at the factory.

Command mode: VLAN interface configuration mode

Usage Guide: To configure an IP address for a switch, you must first create a VLAN interface.

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

(Config)#interface vlan 1
(Config-If-Vlan1)#ip address 10.1.128.1 255.255.255.0
(Config-If-Vlan1)#exit
(Config)#

2.4.2.2. ip address dhcp

Command：ip address dhcp fallback <fallback_address> <fallback_netmask> timeout <fallback_timeout>

no ip address dhcp

Function: Enable the DHCP client to obtain the IP address and gateway address through DHCP negotiation. When the switch obtains IP timeout through dhco, the IP of the switch can automatically jump to the default IP. The no operation of this command is disabled. DHCP client function, and release the address and gateway address obtained by DHCP.

By default, the DHCP client function is disabled by default.

Command mode: VLAN interface configuration mode

Example: Obtain an IP address through DHCP.

(Config)#interface vlan 1
(config-if-vlan)#ip address dhcp fallback 192.168.0.4 255.255.255.0 timeout 30
(Config-If-Vlan1)#exit
(Config)#

Related command：ip address、ip bootp-client enable

2.5. SNMP configuration

2.5.1. SNMP Introduction

SNMP(Simple Network Management Protocol) is a framework that uses the TCP / IP protocol suite to manage devices in the network. Administrators use the SNMP function to query device information, modify device parameter values, monitor device status, and discover network faults.

SNMP protocol uses management station / proxy mode, so SNMP network elements are divided into NMS and Agent two parts.

- NMS(Network Management Station) is a workstation that runs a network management software client program that supports the SNMP protocol and plays a central role in SNMP network management.
- Agent is a process that resides on a managed network device and is responsible for receiving and processing requests from NMS. When an alarm occurs, Agent also actively informs the NMS.

NMS is the manager of the SNMP network. The agent is the manager of the SNMP network. NMS and Agent through the SNMP protocol to interactively manage information. SNMP provides five basic operations:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

NMS through the Get-Request, Get-Next-Request and Set-Request message to the Agent issued a query and configuration management variable request, Agent received the request, with the Get-Response message to respond to the request. When an alarm occurs, the Agent initiates a trap message to the NMS to notify the NMS that an abnormal event has occurred.

This series of devices SNMP Agent supports SNMP v2 version, SNMP v2 compatible SNMP v1 version.

SNMP v1 uses community name authentication, and community name acts like a password to restrict SNMP NMS access to the SNMP agent. If the community name of the SNMP packet is not acknowledged by the device, the packet will be discarded.

SNMP v2 also uses community name authentication. It is compatible with SNMP v1 while also expanding the SNMP v1 function.

SNMP v3 provides a user-based security model (USM, User-Based Security Model) authentication mechanism. The user can configure the authentication and encryption functions. The authentication is used to verify the legitimacy of the sender of the packet and avoid the access of the illegal user. The encryption encrypts the transmission packets between the NMS and the agent so as to avoid eavesdropping. It provides higher security for communication between SNMP NMS and SNMP agents through a combination of authentication and encryption.

NMS and Agent SNMP version matching is a prerequisite for successful visits between them. Agent can configure multiple versions at the same time, with different versions of NMS communication.

2.5.2. MIB Introduction

Any managed resource is represented as an object, called a managed object. The MIB (Management Information Base) is a collection of managed objects that defines the hierarchical relationships between the managed objects and a series of attributes of the object, such as the name of the object, access rights, and data type. Each Agent has its own MIB library, NMS according to the authority of the object can be read / write MIB. The relationship between NMS, Agent, and MIB is shown in the following figure: OID is a set of

integers separated by a period that names the node and can indicate the location of the node in the MIB tree structure, as shown in the following figure:

Figure 2-1 Relation chart of NMS、Agent and MIB

MIB defines a tree structure, the tree node that is managed objects, each node contains a A unique OID (Object Identifier), OID indicates that the node is in the MIB tree node Position in the structure. As shown below:

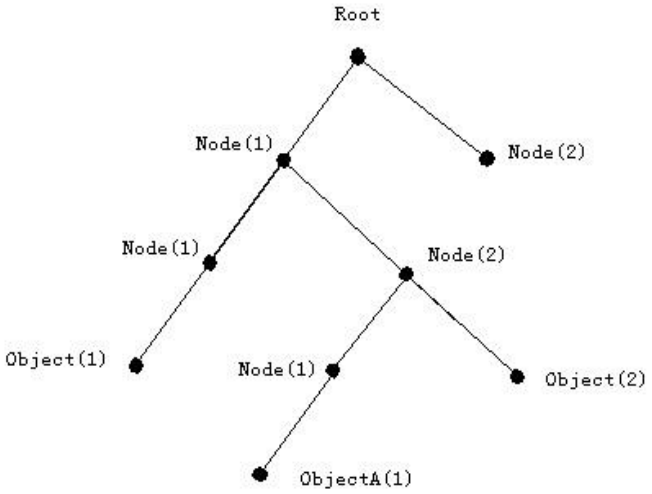


Figure 2-2 MIB tree structure

In this figure, the OID of object A is 1.2.1.1, and the NMS can access the object without ambiguity through this unique OID to obtain the standard variable contained in the object. The MIB defines a set of standard variables for the monitored network device according to this structure.

Can be used as SNMP agent, support SNMPv1 / v2c / v3, support basic MIB-II, RMON public MIB, also supports BRIDGE MIB and other related public MIB.

2.5.3. RMON Introduction

RMON is the most important extension to the basic SNMP system. RMON is a set of MIB definitions that define standard network monitoring functions and interfaces that enable communication between SNMP-based management terminals and remote

monitors. RMON provides an effective and efficient way to monitor subnet-wide behavior. RMON MIB is divided into 10 groups, switches support one of the most commonly used 1,2,3,9 group, namely:

Statistics: The basic usage and error statistics of each subnet that the maintenance agent monitors.

History: A periodic statistical sample of the information available from the statistical group.

Alarm group: Allows the management console personnel to set the sampling interval and alarm threshold for any count or integer recorded by the RMON agent.

Event: A table of all events generated by the RMON agent.

Where the alert group relies on the implementation of the event group. The statistics group and the history group are some of the subnet statistics that show now or before. Alert groups and event groups provide a way to monitor any integer data changes on the network and provide some warning actions (send traps or record logs) when the data is abnormal.

2.5.4. SNMP configuration

2.5.4.1. SNMP Configuration the task sequence

1. Turn on or off the SNMP proxy server function
2. Turn on or off the SNMP V1 version, V2C version, V3 version, all versions
3. Configure the SNMP community string
4. Configure TRAP
5. Add or remove SNMP V3 users, user groups, access tables, views

1. Turn on or off the SNMP proxy server function

Command	Explanation
snmp-server **no snmp-server**	Open the switch as an SNMP proxy server function; the no operation of this command is to turn off the SNMP proxy server function.

2. Open or close SNMP V1 version, V2C version, V3 version, all versions

Command	Explanation
snmp-server version {v1|v2c|v3} **no snmp-server version**	Open the switch SNMP V1, V2C, V3 version; the command no operation to turn off all SNMP version.

3. Configure the SNMP community string

Command	Explanation
snmp-server community v2c <comm> [ro | rw] **no snmp-server community *v2c***	Set the community string of snmp v2c; this command does not delete the configured community string.
snmp-server community v3 <v3_comm> [<ipv4_addr> <ipv4_netmask>]	Set the community string for snmp v3 and the allowed IP address

4. TRAP Configuration

Command	Explanation
snmp-server trap **no snmp-server trap**	Enable the device to send trap messages. The no operation of this command prevents the sending of Trap messages.
host <ipv4_ucast> <udp_port> traps version { v1 [<v1_comm>] | v2 [<v2_comm>] | v3 [probe | engineID <word10_to_64>] [<securtyname>] } **traps [authentication snmp-auth-fail] [system [coldstart] [warmstart]] [switch [stp] [rmon]]**	Add the IP address of the network management station that receives SNMP Trap messages, UDP port; Trap version, user name; Configure the contents of the trap

5. Add or remove SNMP V3 users, user groups, access tables, contexts, views

Command	Explanation
snmp-server user <username> engine-id <engineID> [{ md5 <md5_passwd> | sha <sha_passwd> } [priv { des | aes } <pripasswd>]] **snmp-server view <view_name> <oid_subtree> { include | exclude }**	Add or remove SNMP V3 users, ID, encryption, password, security level Add view

2.5.4.2. SNMP configuration command

2.5.4.2.1. snmp-server community

Command：snmp-server community v2c <comm> [ro | rw]

no snmp-server community v2c

Function: Set the community string of the switch snmp v2c. The operation of this command is to delete the configured community string.

Command mode: global configuration mode

Parameters: <comm> for the set of community strings; ro | rw for the specified access to the MIB library, ro read-only way or rw read and write mode.

For example:

Add community of read and write permissions. private

(Config)#snmp-server community v2c private rw

Add a community string with read-only permission public

(Config)#snmp-server community v2c public ro

2.5.4.2.2. snmp-server enable

Command：snmp-server

no snmp-server

Function: Turns on the switch as the SNMP proxy server function. The no operation of this command is to disable the SNMP proxy server function.

Command mode: global configuration mode

Default: The system automatically shuts down the SNMP proxy server function.

Usage Guide: To configure the management through the NMS, you must first use this command to enable the SNMP agent server function of the switch.

Example: Open the SNMP agent server function of the switch.

(Config)#snmp-server

2.5.4.2.3. snmp-server trap enable

Command：snmp-server trap

no snmp-server trap

Function: This command allows the device to send trap messages. The no operation of this command prevents the sending of Trap messages.

Command mode: global configuration mode

Default: The system prevents the sending of Trap messages by default.

Usage Guide: When a device sends a Trap message, the device sends a Trap message to the management station that receives the Trap message if the port of the device is Down / Up or the system has a Down / Up function.

For example:

Allows to send trap messages.

(Config)#snmp-server trap

Do not send trap messages.

(Config)#no snmp-server trap

2.5.4.2.4. snmp-server host

Command：host <ipv4_ucast> <udp_port> traps version { v1 [<v1_comm>] | v2 [<v2_comm>] | v3 [probe | engineID <word10_to_64>] [<securtyname>] }

Function: Set the IP address of the network management station that receives SNMP traps. Trap version number and parameters

Command mode: snmp host mode

Usage Guide: None

For example:

Set an IP address to accept Trap.

(config)# snmp-server host 123

(config-snmps-host)# host 192.168.0.200 162 traps

2.5.5. SNMP Typical configuration example

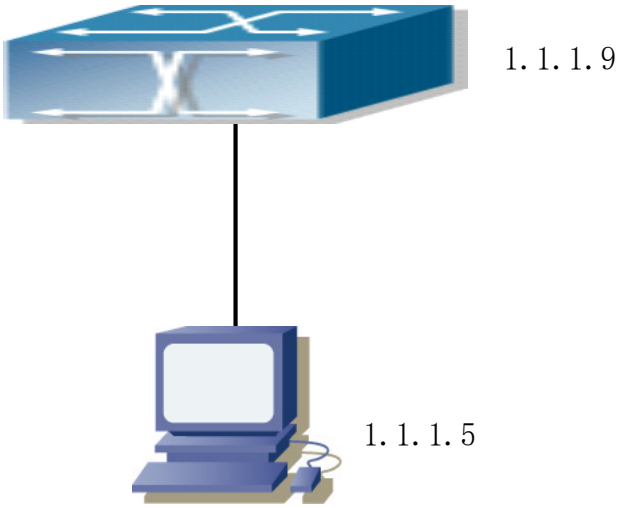


Figure 2-2 SNMP Configuration example

The IP address of the management station (NMS) is 1.1.1.5; the IP address of the switch is 1.1.1.9.

Case 1: The network management software of the management station uses the SNMP protocol to obtain data from the switch.

The configuration of the switch is as follows:

(Config)#snmp-server

(Config)#snmp-server version v2c

(Config)#snmp-server community v2c private rw
(config)# snmp-server community v2c public ro
In this way, the management station can use private as a community string to read and write access to the switch, you can also use public as a community string to read-only access to the switch.

Case 2: The management station is receiving Trap messages from the switch.
The configuration of the switch is as follows:
(Config)#snmp-server trap
(config)# snmp-server host 123
(config-snmps-host)# host 1.1.1.5 162 traps
(config-snmps-host)# version v2

2.6. Alarm

2.6.1. Introduction

This series of devices supports the following two types of alarms:

- Power alarm: dual power supply module equipment in the case of power supply alarm is enabled, the power module power failure or abnormal alarm.
- Port Alert: Includes port down alarm and port traffic aliasing
  - Port alarm: When enabled, the port will cause an alarm when it is down.

When the alarm is enabled, the alarm mode is logged, the front panel alarm indicator flashes, the alarm terminal is triggered, and the SNMP trap message is sent.

2.6.2. Alarm task sequence

1. Configuration alarm
2. View alarm

1. Configuration alarm

Command	Explanation
Global configuration mode	
power alarm | no power alarm	Port configuration mode
Port configuration mode	
alarm | no alarm	Set or cancel port down alarm

2. View alarm

Command	Explanation
Privilege mode	
show alarm	Check the port alarm status.
show alarm power	Check the power alarm status

2.7. Log management

2.7.1. Introduction

The log function of the switch mainly records the status of the switch system, fault, debugging, abnormal and other information. Through the configuration can be real-time upload log information to support the Syslog protocol server.

Log information is divided into four levels by importance, from high to low as follows: Error、Warning、Notice、Information

2.7.2. Log management task sequence

1. Configure log management
2. View the log management

1. Configure log management

Command	Explanation
Global configuration mode	
logging on | no logging on	Turns on or off to save the log to the log server.
logging host { <ipv4_addr> | <domain_name> } | no logging host	Set the log server IP address / off.
logging level { informational | notice | warning | error }	Set the upload log information level
Privilege configuration mode	
clear logging [informational] [notice] [warning] [error] [switch <switch_list>]	Clear the corresponding or all levels of log messages

2. View the log management

Command	Explanation
Privilege mode	
show logging [informational] [notice] [warning] [error] [switch <switch_list>]	Displays the corresponding level or all log information.

Chapter 3 Port Configuration

3.1. Port Introduction

The port number of each port is marked on the panel of the switch. In order to distinguish the port on the panel, the port number (software port number) provided by the switch operating system is Fastethernet 1 / X, GigabitEthernet1 / X.

If you want to configure some ports, you can use the command interface to enter the corresponding Ethernet interface configuration mode.

3.2. Port Configuration

3.2.1. Ethernet port configuration

3.2.1.1. Ethernet port configuration task sequence

1. Enter the Ethernet interface configuration mode
2. Configure the attributes of the Ethernet port
   1) Turn the port on or off
   2) Configure the port connection type
   3) Configure port rate duplex
   4) Configure bandwidth control
   5) Configure flow control

1. Enter the Ethernet interface configuration mode

Command	Explanation
Configuration mode	
interface GigabitEthernet <***port_type_list***> **interface FasteEhernet** <***port_type_list***>	Enter the Ethernet interface configuration mode

2. Configure the attributes of the Ethernet port

Command	Explanation
Interface configuration mode	
shutdown **no shutdown**	Close or open the specified port.

speed {1000 | 100 | 10 | auto }	Sets the rate of the specified port.
duplex { half | full | auto }	Sets the duplex mode for the specified port.
flowcontrol on **flowcontrol off**	Turns on or off traffic control for the specified port.

3.2.1.2. Introduction to Ethernet port configuration commands

3.2.1.2.1. flow control

Command：flow control

no flow control

Function: Enable the flow control function of the specified port. The no operation of this command is to disable the flow control function of the port.

Command mode: Interface configuration mode

By default, the flow control function of a port is disabled by default.

Usage Guide: When the traffic of the port is enabled, when the traffic received by the port is larger than the size that the port cache can hold, the port will notify the device that sends traffic to it by slowing down the sending speed to prevent packet loss. The switch's port supports 802.3X traffic control based on back pressure; the port operates in half-duplex mode and supports back pressure flow control. When the backpressure control reaches a critical head clogging (HOL), the switch will automatically perform header blocking control (discarding some packets in the COS queue that may have header blocking) to avoid a significant drop in network performance.

Note: Unless the user needs a slow, low performance, but the packet loss of smaller networks, or do not recommend users to open the port flow control function. When opening the port's flow control function, make sure that both ends are the same in duplex and duplex mode.

Example: Turn on the flow control function of port 1/2.

(config)# interface GigabitEthernet 1/2

(config-if)# flowcontrol on interface ethernet

Command：interface interface GigabitEthernet <*port_type_list*>

Function: Enter from the global configuration mode to the Ethernet interface configuration mode.

Parameters: <interface-list> is the port number, and the format and range of the port number are described in the chapter description of the port.

Command mode: global configuration mode

Usage Guide: Use the command exit to return to the global configuration from the Ethernet interface configuration mode.

Example: Enter Ethernet port 1/2

(config)# interface GigabitEthernet 1/2

(Config-if)#

3.2.1.2.2. shutdown

Command：shutdown

no shutdown

Function: Turn off the specified Ethernet port. The no operation of this command is to open the port.

Command mode: Interface configuration mode

By default, the Ethernet port is enabled by default.

Usage Guide: When the Ethernet port is shut down, the Ethernet port will not send the data frame, and the port status is down when the user enters the show interface command.

Example: Open port 1/2.

(Config)#interface GigabitEthernet 1/2

(Config-if)#no shutdown

3.2.1.2.3. speed

Command：speed {auto| 10|100| 1000}

Function: Sets the rate of the specified port.

Parameters: auto for the automatic negotiation rate; 10 for the mandatory 10Mbit / s; 100 for the mandatory 100Mbit / s; 1000 for the mandatory 1000Mbit / s.

Command mode: Interface configuration mode

By default, the port defaults to auto-negotiation rate.

Usage Guide: According to the IEEE 802.3 protocol, port rate and duplex automatic negotiation are uniform. When the port rate is set to auto-negotiation, the duplex mode of the port is automatically set to auto-negotiation. When the port's rate mode changes from auto-negotiation to mandatory, the duplex mode of the port becomes mandatory. Full-duplex mode The It is strongly recommended that the user set the rate and duplex mode of each port to auto-negotiation so that the connection problem caused by the protocol can be avoided as much as possible. If the user needs to set the port to forced rate / duplex, make sure that both the rate / duplex settings are consistent and both are forced rate / duplex.

For example: 1/2 port for the electrical port, forced 100Mbit / s.

(Config)#interface GigabitEthernet 1/2

(Config-if)#speed 100

3.2.1.2.4. duplex

Command：duplex {auto| full|half}

Function: Set the duplex mode of the specified port.

Parameters: auto for auto-negotiation; full for forced full duplex; half for forced half-duplex.

Command mode: Interface configuration mode

Default: Default auto-negotiation

3.2.2. Mirror configuration

3.2.2.1. Port mirroring introduction

Mirror function refers to the switch to a port or VLAN to receive or send the same data frame to another port; which is copied port / VLAN called the mirror source port / VALN, copy the port is called the mirror destination port. A protocol analyzer (such as Sniffer) or RMON monitor is usually connected at the destination port of the mirror to monitor and manage the network and to diagnose network failures. Mirroring is divided into remote mirroring and local mirroring. This section focuses on native mirroring.

3.2.2.2. Local Mirroring

Local mirroring refers to the source port / VLAN

1. Specify the mirror source port
2. Specify the destination port for mirroring

1. Specify the mirror source port

Command	Explanation
Global configuration mode	
monitor session <*1*> source interface <*interface-list*> {rx| tx| both} **no monitor session <*1*> source interface <*interface-list*> {rx| tx| both}**	Specify the mirror source port. The no operation of this command is to remove the mirroring source port.

2. Specify the destination port for mirroring

Command	Explanation
Global configuration mode	
monitor session <*1*> destination interface <*interface-number*> **no monitor session <*1*> destination interface <*interface-number*>**	Specify the mirroring destination port. The no operation of this command is to remove the mirroring destination port.

3.2.2.3. Port mirroring configuration

3.2.2.3.1. monitor session source interface

Command：monitor session <*session*> source interface <*interface-list*> {rx| tx| both}

no monitor session <*session*> source interface <*interface-list*> {rx| tx| both}

Function: Specifies the mirroring source port. The no operation of this command is to remove the mirroring source port.

Parameters: <session> is the mirror session value, currently only supports 1 ~ 7; <interface-list> is the mirror source port list, support "-" ";" and other special characters; **rx** for the mirror source port to receive traffic; **Tx** is the traffic that mirrors the source port; **both** for mirroring source port incoming and outgoing traffic.

Command mode: global configuration mode

Usage Guide: This command sets the source port of the mirror. There is no restriction on the port of the mirror source. It can be a port or multiple ports. It can not only emit the source port and send the bidirectional traffic, but also the source port Send traffic and receive traffic. If you do not specify the [rx | tx | both] keyword, the default is both. When mirroring multiple ports, the direction of multiple source ports can be inconsistent, but to be configured several times.

Example: Set the source port for 1 / 1-4 outgoing traffic and 3/5 receive traffic.

(Config)#monitor session 1 source interface ethernet 1/1-4 tx

(Config)#monitor session 1 source interface ethernet 3/5 rx

3.2.2.3.2. monitor session destination interface

Command：monitor session <*session*> destination interface <*interface-number*>

no monitor session <*session*> destination interface <*interface-number*>

Function: Specifies the destination port for mirroring. The no operation of this command is to remove the mirroring destination port.

Parameters: <session> is the mirroring session value. Currently, only 1 to 7 are supported. <Interface-number> is the destination port for mirroring.

Command mode: global configuration mode

Usage Guide: Supports 7 mirrored destination ports. Note that the mirroring destination port can not be a member of the port aggregation group and the port throughput is preferably greater than or equal to the sum of the throughput of all source ports it mirrors.

Example: Set the destination port to 4/7.

(Config)#monitor session 1 destination interface ethernet 4/7

3.2.2.4. Port mirroring troubleshooting help

3.2.2.4.1. show monitor

Command: show monitor

Function: Displays the information of the mirror source and destination port.

Command mode: Privileged user configuration mode

Usage Guide: This command displays the currently set source port and destination port.

For example:

#show monitor session all

3.2.2.4.2. Port mirroring troubleshooting help

When configuring port mirroring problems, check for the following reasons:

- ☞ · Mirror destination port is a member of a port aggregation group; if yes, modify the port aggregation group;
- ☞ · The destination port of the mirroring port is less than the sum of the mirroring source port throughput. The destination port can not completely copy the source port traffic; reduce the number of source ports or copy the unidirectional traffic, or select the port with the higher throughput as the destination port.

3.3. Port troubleshooting help

3.3.1. Monitoring and debugging commands

3.3.1.1. clear statistics GigabitEthernet

Command：clear statistics GigabitEthernet <port_type_list>

Function: Clear the statistics of the Ethernet port.

Parameters: <port_type_list> is the Ethernet port number.

Command mode: global configuration mode

By default, the statistics of Ethernet ports are not deleted by default.

Example: Clear the statistics of Ethernet port 1/1.

clear statistics GigabitEthernet 1/1

3.3.1.2. show interface GigabitEthernet

Command: show interface GigabitEthernet **<port_type_list>**statistics

Function: Displays information about the specified switch port.

Parameters: <port_type_list> is the port number, and the format and range of the port number are described in the chapter description of the port.

Command mode: global configuration mode

Usage Guide: This command displays the port rate of the port, duplex mode, flow control switch, broadcast storm suppression, and statistics on sending and receiving packets.

Example: Displays information about ports 1 / 1-8.

show interface GigabitEthernet 1/1-8 statistics

3.3.2. Port troubleshooting help

The usual situation that users encounter when configuring a port is as follows:

- ☞ When the two optical interfaces are connected to each other, if the one end is set to auto-negotiation and the other end sets the forced rate / duplex, the optical interface will not be linked up. This is determined by the IEEE 802.3 protocol.
- ☞ Some settings that are not recommended by the user. Please try to avoid the following settings:
  - Open a port flow control, and set the port multicast suppression
  - Set a port broadcast, multicast or unknown address unicast suppression, and set the port bandwidth limit.

In the case of the above settings, the port traffic may be lower than expected.

Chapter 4 MAC Address Table Configuration

4.1. MAC Address Table Introduction

The MAC address table is a table that identifies the mapping relationship between the destination MAC address and the switch port. The MAC address is divided into static MAC address and dynamic MAC address. The static MAC address is configured by the user and has the highest priority (can not be covered by the dynamic MAC address). The dynamic MAC address is learned by the switch during the forwarding of the data frame and takes effect within a limited time. When the switch receives the data frame to be forwarded, it first learns the source MAC address of the data frame and establishes the mapping relationship with the receiving port. Then, the MAC address table is checked according to the target MAC address. If the entry is hit, the switch will frame the data frame from the corresponding port Forward; otherwise, the switch broadcasts the data frame within its own broadcast domain. If the dynamic MAC address is not learned from the forwarding data frame for a long time, the switch deletes it from the MAC address table.

The operation of the MAC address table can be divided into two steps:

1. 1. Access to the MAC address;
2. According to the MAC address table forwarding or filtering.

4.1.1. MAC address table to obtain

MAC address table can be divided into static configuration and dynamic learning. Static configuration that is created by the user MAC address and port mapping; dynamic learning that is dynamically discovered by the MAC MAC address and port mapping, and regularly update the MAC address table. Below we will focus on MAC address table dynamic learning process.

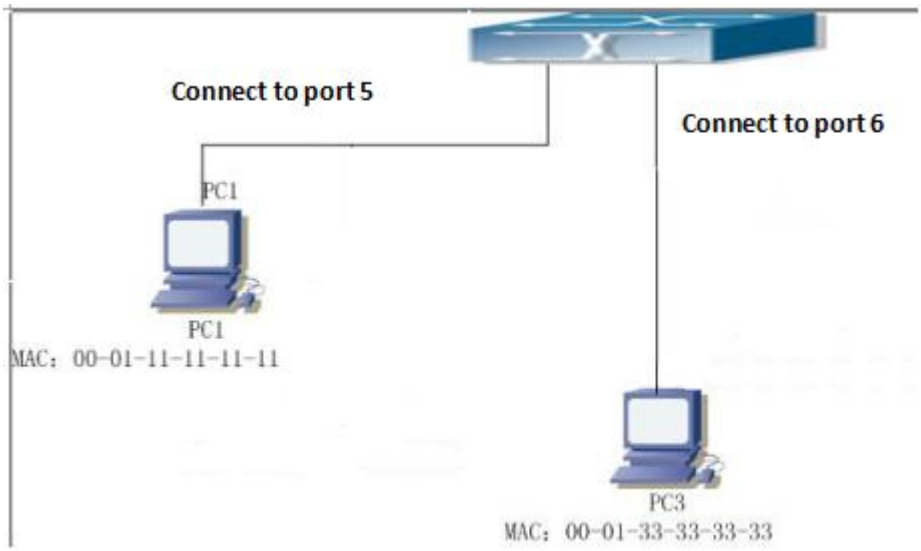


Figure 4-1 MAC address table dynamic learning

The topological environment of the above figure is: 2 hosts connected to the switch. Host 1 is connected to port 1/5 of the switch. Host 3 is connected to port 1/6 of the switch.
In the initial state, there is no learned address mapping entry in the MAC address table. Taking the mutual communication between host 1 and host 3 as an example, the MAC address table learning process is as follows:

1. When the host 1 transmits information to the host 3, the switch receives the source MAC address 00-01-11-11-11-11 of the message at the port 1/5. The MAC address table of the switch increases the MAC address 00-01-11-11-11-11 and port 1/5 mapping entries;
2. At the same time, the switch will check the target MAC address 00-01-33-33-33-33 of the information. At this time, only the MAC address 00-01-11-11-11-11 and port 1/5 mapping Table entries, there is no port mapping corresponding to 00-01-33-33-33-33, so the switch can only broadcast the information to each port of the switch (assuming all ports of the switch belong to the default VLAN);
3. Host 3 located at port 1/6 will respond to host 1. At that time, the 1/6 port of the switch receives the information from the host 3, and the MAC address table 00-01-33-33-33-33 and the port 1/6 mapping table are added to the MAC address table of the switch.
4. The contents of the current MAC address table are MAC address 00-01-11-11-11-11 Dynamic corresponds to port 1/5, MAC address 00-01-33-33-33-33 Dynamic corresponds to port 1/6 The after a period of communication between host 1 and host 3, the switch never receives the information sent from host 1 and host 3, and after 300 seconds the MAC address table of the switch will delete the above saved MAC address mapping entry. Where 300 seconds is the aging time of the switch's default MAC address, and the switch provides modification of the aging time.

4.1.2. Forward or filter

The switch will make a decision to forward or filter the received data frame according to the MAC address table. The above figure shows, for example, that the MAC address table of the current switch dynamically learns the MAC addresses of Host 1 and Host 3. The MAC address table of the switch is:

MAC Address	Port no.	method of obtaining
00-01-11-11-11-11	1/5	Dynamic
00-01-33-33-33-33	1/6	Dynamic

1. According to the MAC address table forwarding situation

If the host 1 sends a message to the host 3, the switch sends the data received from port 1/5 from port 1/6 according to the MAC address table.
In addition, the switch can forward three types of frames:

- ✧ Broadcast frame;
- ✧ Multicast frame;
- ✧ Unicast frame.

The following briefly describes the switch on the three types of frame processing

1. Broadcast frame: The switch can block the collision domain, but can not block the broadcast domain. In the case where no VLAN is set, all the devices connected to the switch are in the same broadcast domain. When the switch receives the broadcast frame, it will The broadcast

frame is forwarded to all ports. When the switch sets the VLAN, the MAC address table will also adjust accordingly, will increase the VLAN information, then the switch receives the broadcast frame, the broadcast frame will not be forwarded to all ports within the switch, and changed to only To all ports belonging to the same VLAN.

2. Multicast frame: When the switch does not set the function of IGMP snooping, the switch performs the same process as the multicast. When the switch sets up IGMP snooping, the switch forwards the multicast only to the port that belongs to the multicast group. frame.
3. 3Unicast frame: When the VLAN MAC address of the unicast frame received by the switch is present in the MAC table, the switch will forward the unicast frame directly to the corresponding port when the VLAN is not set. When receiving the single When the destination MAC address of the broadcast frame does not exist in the MAC address table, the switch broadcasts the unicast frame. When the switch sets the VLAN, the switch will only forward the unicast frame in the same VLAN. When the destination MAC address of the unicast frame is in the MAC address table but does not belong to the same VLAN, the switch can only transmit the unicast frame Broadcast in the VLAN to which it belongs.

4.2. MAC Address table configuration

4.2.1. mac address-table aging-time

Command：mac address-table aging-time <0_10_to_1000000>

no mac address-table aging-time

Function: Set the aging time of the address mapping entries dynamically learned in the MAC address table. The no operation of this command is to restore the default aging time of the system for 300 seconds.

Parameters: <age> is the aging time, in seconds, in the range of 10 to 1000000; 0 is not aging.

Command mode: global configuration mode

Default: The system defaults to 300 seconds.

Usage Guide: Aging time set too small, the switch will increase a lot of unnecessary broadcast and affect performance; aging time set too large, and will make some of the long list of long-term exist in the MAC address table. So the user should be based on the actual situation to set the aging time. When the aging time is set to 0 seconds, the switch dynamically learns that the address will not age with time. The dynamically learned address will be kept in the MAC address table.

Example: Set the MAC address table to dynamically learn the aging time of the MAC address to 400 seconds.

(Config)#mac address-table aging-time 400

4.2.2. mac address-table

Command: mac address-table static <mac_addr> vlan <vlan_id> [interface <port_type> [<port_type_list>]]

no mac address-table static <mac_addr> vlan <vlan_id> [interface <port_type>

[<port_type_list>]]

Function: Add a static address entry. The no operation of this command is to delete a static address entry.

Parameter: **static** static address; <mac_addr> MAC address; vlan <vlan_id> VLAN ID interface <port_type> The port to which the mac address is bound.

Command mode: global configuration mode

Default: No static mac address

Usage Guide: In some special purpose or the switch can not dynamically learn the MAC address, the user can use this command to MAC address and port and VLAN manually establish a mapping relationship.

The no mac-address-table command is used to delete all dynamic, static, and filtering MAC address entries that exist in the MAC address table of the switch. Except for the default mapping entries.

Example: Port 1/2 belongs to VLAN 1 and establish address mapping with MAC address bc-9c-c5-00-00-01.

(config)# $e static bc-9c-c5-00-00-01 vlan 1 interface GigabitEthernet 1/2

4.3. MAC Address learning configuration

4.3.1. mac address-table learning

Command: mac address-table learning [secure]

no mac address-table learning [secure]

Function: MAC address learning mode configuration; the no operation of this command is to cancel MAC address learning.

Parameters: [secure] safe mode

Command mode: Interface configuration mode

Usage Guide: Configure the port mac address learning mode configuration, need to enter the interface mode.

Example: Turn off port 1/3 mac learning ability.

(config)# interface GigabitEthernet 1/3

(config-if)# no mac address-table learning

4.3.2. mac address-table learning vlan

Command: mac address-table learning vlan <vlan_list>

no mac address-table learning vlan <vlan_list>

Function: Set vlan MAC address learning ability.

Parameters: vlan <vlan_list> VLAN ID.

Command mode: global configuration mode

Default: The system can enable VLAN MAC address learning by default.

Example: Disable the MAC address learning capability of VLAN 2.

#(Config)#no mac address-table learning vlan 2

4.4. Troubleshooting help

4.4.1. Monitoring and debugging commands

4.4.1.1. show mac-address-table

Command:show mac address-table [conf | static | aging-time | { { learning | count } [interface <port_type> [<port_type_list>] | vlan <vlan_id_2>] }]

Function: Displays the contents of the current MAC address table of the switch.

Parameter: **conf** user configuration's static table. **static** all static table, **Aging-time** address aging time, **Learning** mac address learning mode. **count** address amount. **Interface<port_type>** corresponds to the port MAC address entry. **<Vlan-id>** corresponds to the address entry of the VLAN.

Command mode: Privileged user configuration mode

By default:

Usage Guide: This command can be used to display various MAC address entries.

Example: Display the MAC address entries of VLAN 1.

#show mac address-table vlan 1

4.4.2. Troubleshooting help

When you enter **show mac address-table** command, you find that the port does not learn the MAC of the device to which the port is connected. possible reason:

- The Ethernet cable used to connect is damaged and the Ethernet cable is replaced.
- The switch starts SpanningTree and the port is discarding; or the port is connected to the device. Spanning Tree is still in the calculation. If the Spanning Tree is calculated, the port can learn the MAC address.
- If above is not the problem, please see if port is damaged, or find technical support to solve.

Chapter 5 VLAN Configuration

5.1. VLAN Introduction

VLAN(Virtual Local Area Network) This technology can be based on the function, application or management needs of the LAN internal equipment is logically divided into a network segment, thus forming a virtual workgroup, and do not need to consider the actual physical location of the device. IEEE promulgated the IEEE802.1Q protocol to specify the implementation of standardized VLAN program, the switch's VLAN function that is in accordance with the 802.1Q standard implementation.

VLAN technology is characterized by the need to dynamically according to the needs of a large local area network is divided into many different broadcast domain:

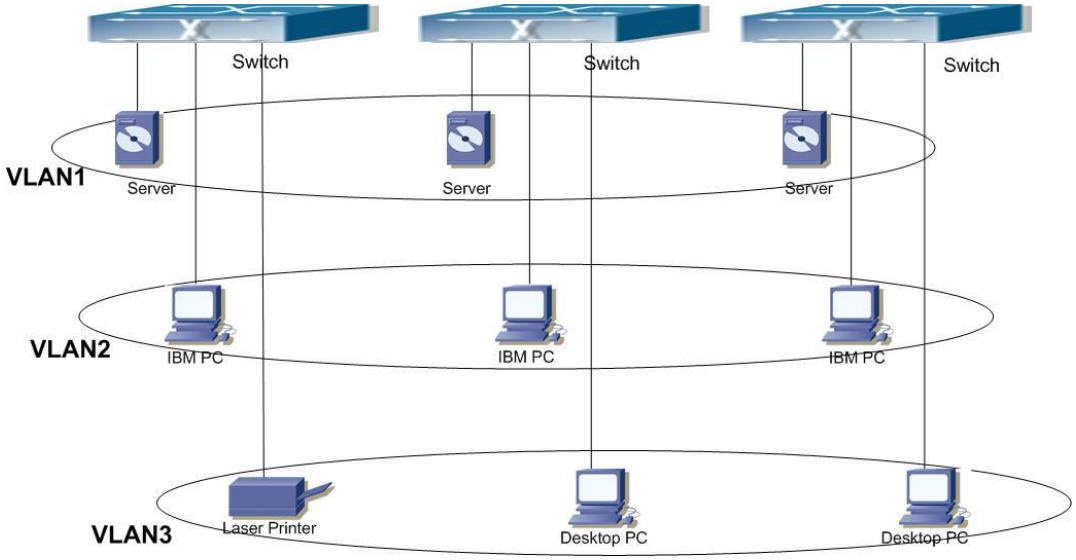


Figure 5-1 Logical definition of the VLAN network

Each broadcast domain is a VLAN, VLAN and physical LAN have the same attributes, the only difference is that the VLAN is logical rather than physical division, so VLAN division does not have to be based on the actual physical location, and each VLAN internal Broadcast, multicast, and unicast traffic are isolated from other VLANs.

VLAN-based features, VLAN technology to bring us the following convenience:

-
- Improve network performance
- Save network resources
- Simplify network management
- Reduce network costs
- Improve network security

In the switch, the 802.1Q VLAN is defined. In this chapter, the usage and configuration of VLANs in the switch are described in detail.

5.2. VLAN Configuration

5.2.1. VLAN configuration task sequence

1. Create or delete a VLAN
2. Specify or delete the VLAN name
3. Assign the switch port to the VLAN
4. Set the switch port type
5. Set the trunk port
6. Set the Access port
7. Turn on or off the port's portal entry rules

1. Create or delete VLAN

Command	Explanation
Global configuration mode	
vlan <vlan-id> **no vlan <vlan-id>**	Create/delete VLAN or enter VLAN mode

2. Specify or delete a VLAN name

Command	Explanation
VLAN configuration mode	
name <vlan-name> **no name**	Set / delete the VLAN name.

3. Set the switch port type

Command	Explanation
Interface configuration mode	
switchport mode { access | trunk | hybrid }	Set the current port mode.

4. Set Trunk port

Command	Explanation
Interface configuration mode	
switchport trunk allowed vlan { all | none | [add | remove | except] <vlan_list> } **no switchport trunk allowed vlan**	Set / delete the VLANs allowed by the trunk port.
switchport trunk native vlan <*vlan-id*> **no switchport trunk native vlan**	Set / delete the PVID of the trunk port.

5. Set Access port

Command	Explanation
Interface configuration mode	
switchport access vlan <*vlan-id*> **no switchport access vlan**	Add / exits the current port to the specified VLAN.

5.2.2. VLAN configuration command

5.2.2.1. vlan

Command: vlan <*vlan-id*>

no vlan <*vlan-id*>

Function: Create a VLAN and enter VLAN configuration mode. In VLAN mode, you can configure the VLAN name and assign the switch port to the VLAN. The no operation of this command is to delete the specified VLAN.

Parameters: <vlan-id> VID of the VLAN to be created / deleted, in the range of 1 to 4094.

Command mode: global configuration mode

By default, the switch has VLAN1 only by default.

Usage Guide: VLAN 1 is the default VLAN of the switch. You can not configure or delete VLAN1. The total number of VLANs allowed to be configured is 4094. Another reminder is that you can not use this command to delete the dynamic VLAN learned through GVRP.

Example: Create VLAN 100 and enter VLAN 100 configuration mode.

(config)# vlan 100

(config-vlan)#

5.2.2.2. name

Command: name <*vlan-name*>

no name

Function: Specify the name for the VLAN. The name of the VLAN is a descriptive string for the

VLAN. The no operation of this command is to delete the name of the VLAN.

Parameters: <vlan-name> is the specified vlan name string.

Command mode: VLAN configuration mode

Default: VLAN default name is vlanXXX, where XXX is VID.

Usage Guide: The switch provides the function of specifying the name for different VLANs, which helps the user to remember the VLAN and facilitate the management.

Example: Specify the name named test for VLAN 100.

(config-vlan)# name test

5.2.2.3. switchport access vlan

Command: switchport access vlan <*vlan-id*>

no switchport access vlan

Function: Add the current access port to the specified VLAN. The operation of this command is to remove the current port from the VLAN.

Parameters: <vlan-id> is the vlan VID of the current port, in the range of 1 to 4094.

Command mode: Interface configuration mode

By default, all ports belong to VLAN1 by default.

Usage Guide: Only ports that belong to Access mode can join the specified VLAN, and the Access port can only be added to a VLAN at the same time.

Example: Set an access port to VLAN 100.

(Config) # interface GigabitEthernet 1/4

(config)# interface GigabitEthernet 1/4

(config-if)# switchport mode access

(config-if)# switchport access vlan 3

5.2.2.4. switchport mode

Command: switchport mode { access | trunk | hybrid }

Function: Set the port of the switch to access, trunk or hybrid mode.

parameter:

Command mode: Interface configuration mode

Default: the port defaults to Access mode.

Usage Guide: The port that operates under trunk mode is called a trunk port. Trunk ports can communicate with multiple VLANs through interconnection between trunk ports. You can implement the same VLAN interworking on different switches. A port is called an Access port, and an Access port can be assigned to a VLAN and can only be assigned to a VLAN. A hybrid port can allow multiple VLANs to pass through, and can receive and send packets of multiple VLANs. It can be used for connection between switches and can be used to connect to a user's computer.

Example: Set port 5 to trunk mode and port 8 to access mode.

(config)# interface GigabitEthernet 1/5

(config-if)# switchport mode trunk

(config-if)# exit

(config)# interface GigabitEthernet 1/8

(config-if)# switchport mode access

5.2.2.5. switchport trunk allowed vlan

Command: switchport trunk allowed vlan { all | none | [add | remove | except] <vlan_list> }

no switchport trunk allowed vlan

Function: Set or modify the trunk port to allow VLANs. The no operation of this command is to restore the default.

Parameter: **all** Allowed through all vlan; **none** Not allowed through all vlan; **add** add passable vlan; **remove**, Remove the original passable vlan; **except,** Remove the <vlan-list> vlan, the other are allowed to pass.

Command mode: Interface configuration mode

By default, the trunk port is allowed to pass through all VLANs by default.

Usage Guide: You can use this command to set which VLAN traffic through the trunk port, and the VLAN traffic that is not included is disabled.

Example: Set the traffic of the trunk port to pass through VLAN 1, 3, 5-20.

(config)# interface GigabitEthernet 1/5

(config-if)# switchport mode trunk

(config-if)# switchport trunk allowed vlan 1,3,5-20

5.2.2.6. switchport trunk native vlan

Command: switchport trunk native vlan <*vlan-id*>

no switchport trunk native vlan

Function: Set the PVID of the trunk port. The no operation of this command is to restore the default value.

Parameters: <vlan-id> is the PVID of the trunk port.

Command mode: Interface configuration mode

Default: the default PVID of the trunk port is 1.

Usage Guide: Define the concept of PVID in 802.1Q. The role of the PVID of the trunk port is that when an untagged frame enters the trunk port, the port will tag the untagged frame with the native PVID set with this command.

Example: Set the native vlan of a trunk port to 100.

(config)# interface GigabitEthernet 1/5

(config-if)# switchport mode trunk

(config-if)# switchport trunk native vlan 100

5.2.3. VLAN typical application

Application

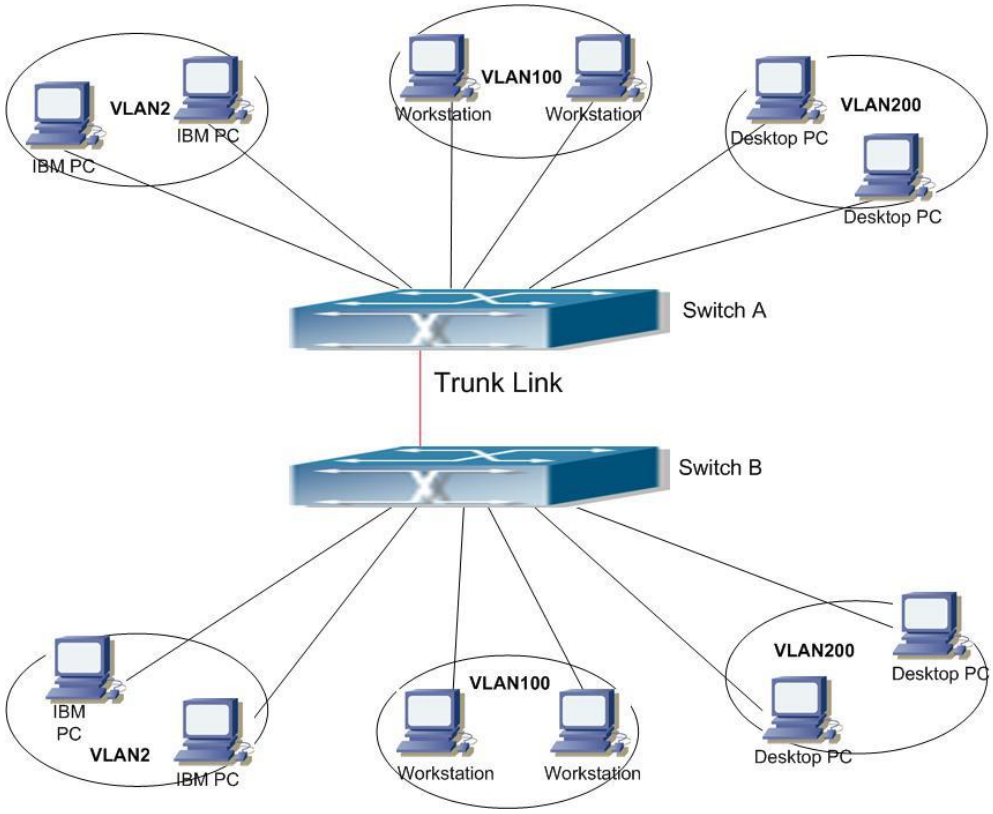


Figure 5-2 VLAN typical application topology

Due to the need of LAN security and application, the existing LAN is divided into three VLANs: VLAN2, VLAN100 and VLAN200, and the three VLANs are required to span two areas A and B, and two switches are placed separately. So VLAN traffic as long as you can transfer between the switch, you can meet the requirements of cross-regional.

Configuration item	Configuration instructions
VLAN2	1 to 2 ports of switches of A , B points
VLAN100	3 to 4 ports of switches of A , B points
VLAN200	5 to 6 ports of switches of A , B points
Trunk port	7 port of switches of A , B points

Connect the Trunk ports of the two switches to the Trunk link to carry the vlan traffic across the switch. To connect the various network devices to the ports of the VLANs of the switch, they are assigned to the corresponding VLANs.

The configuration steps are as follows:

Switch A:

(config)# vlan 2

(config-vlan)# exit

(config)# vlan 100

(config-vlan)# exit

(config)# vlan 200

(config-vlan)# exit

(config)# interface GigabitEthernet 1/1-2

(config-if)# switchport mode access

(config-if)# switchport access vlan 2

(config-if)# exit

(config)# interface GigabitEthernet 1/3-4

(config-if)# switchport mode access

(config-if)# switchport access vlan 100

(config-if)# exit

(config)# interface GigabitEthernet 1/5-6

(config-if)# switchport mode access

(config-if)# switchport access vlan 200

(config-if)# exit

(config)# interface GigabitEthernet 1/7

(config-if)# switchport mode trunk

(config-if)# switchport trunk allowed vlan 1,2,100,200

(config-if)# exit

Switch B: The configuration is the same as A

5.3. VLAN Troubleshooting help

5.3.1. Monitoring and debugging information

5.3.1.1. show vlan

Command: show vlan [id <vlan_list> | name <name> | brief] [all]

Function: Displays detailed status information for all VLANs or specified VLANs.

Parameters: **id** View the vlan of the id; **name** View the vlan of the name; **brief** View the simple information; **all** View all vlan

Command mode: Privileged user configuration mode

Example: Displays the current VLAN status information. Displays the current VLAN statistics.

```
#    show vlan
VLAN    Name                                Interfaces
----    --------------------------------    ----------
1       default                             Gi 1/8-16 2.5G 1/1-2
2       VLAN0002                            Gi 1/1-2,7
100     VLAN0100                            Gi 1/3-4,7
200     VLAN0200                            Gi 1/5-7
```

Chapter 6 IGMP Snooping Configuration

6.1. IGMP Snooping introduction

IGMP(Internet Group Management Protocol) used to achieve IP multicast. IGMP is supported by multicast network devices (such as routers) for host qualification inquiries, but also want to join a multicast group host to notify the router to accept a multicast address of the packet, which are through the IGMP message Exchange to complete. The router first sends an IGMP Host Membership Query message using a group address that can be addressed to all hosts (ie 224.0.0.1). If a host wants to join a multicast group, it responds to an IGMP Host Membership Report message with the group address of the multicast group.

IGMP Snooping is IGMP Snooping. The switch restricts the flooding of multicast traffic through IGMP Snooping, and forwards the multicast traffic only to the port connected to the multicast device. The switch listens to the IGMP message between the multicast router and the host, maintains the multicast forwarding table according to the listening result, and the switch decides the forwarding of the multicast packet according to the multicast forwarding table.

This switch implements IGMP snooping and provides the function of sending Query to the switch so that the user can use the switch to implement IP multicast.

6.2. IGMP Snooping Configuration

6.2.1. IGMP Snooping Configuration tasks

1. Enable IGMP snooping
2. Configure IGMP snooping
3. Configure to send IGMP Query

1. Enable IGMP Snooping function

Command	Explanation
Global configuration mode	
ip igmp snooping **no ip igmp snooping**	Enable IGMP Snooping function

2. Set IGMP Snooping

Command	Explanation
Global configuration mode	
ip igmp snooping vlan <***vlan-id***> **no ip igmp snooping vlan** <***vlan-id***>	Enable specify VLAN's IGMP Snooping function

6.2.2. IGMP Snooping configuration command

6.2.2.1. ip igmp snooping

Command: ip igmp snooping

no ip igmp snooping

Function: Enable IGMP snooping on the switch. The no operation of this command is to disable IGMP Snooping.

Command mode: global configuration mode

Default: IGMP snooping is disabled by default on the switch.

Usage Guide: Enable IGMP Snooping on the switch so that the switch can monitor the multicast traffic of the network and decide which ports can receive multicast traffic.

Example: Enable IGMP snooping in global mode.

(Config)#ip igmp snooping

6.2.2.2. ip igmp snooping vlan

Command: ip igmp snooping vlan <*vlan-id*>

no ip igmp snooping vlan <*vlan-id*>

Function: Enable IGMP snooping on the specified VLAN. The no operation of this command is to disable IGMP Snooping for the specified VLAN.

Parameters: <vlan-id> is the VLAN ID.

Command mode: global configuration mode

Default: IGMP Snooping is disabled by default.

Usage Guide: You must enable IGMP snooping on the switch to enable IGMP Snooping for the specified VLAN. This command is mutually exclusive with the command **ip igmp snooping vlan <vlan-id> query**, that is, in the same VLAN can only do **snooping** or **query** in a function.

Example: Enable IGMP snooping in VLAN 100 in global configuration mode.

(Config)#ip igmp snooping vlan 100

6.3. IGMP Snooping example

Example 1： IGMP Snooping function

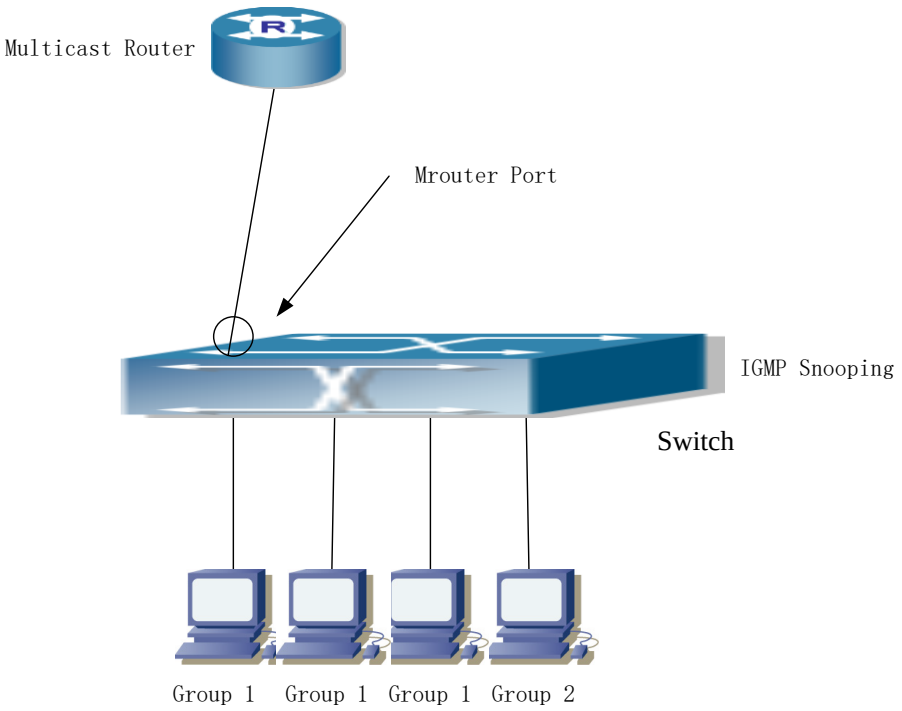


Figure 6-1 Enable IGMP Snooping function

As shown in the figure, the vlan 100 on the Switch contains ports 1, 2, 6, 10, and 12. Four hosts are connected to ports 2, 6, 10, and 12 respectively, and the multicast router is connected to port 1. Suppose we need to do igmp snooping on vlan 100. By default, the global igmp snooping function and the igmp snooping function on each VLAN are not enabled. Therefore, you need to open the global igmp snooping function, while the vlan 100 open igmp snooping.

Configuration steps as follow:

#config

(config)#ip igmp snooping

(config)#ip igmp snooping vlan 100

Multicast configuration:

Assuming that the multicast server provides two programs, the group addresses Group1 and Group2 are used, and the multicast application software is running on the four hosts. The three hosts on the ports 2, 2,6, and 10 play the program 1 on the port 12 The host broadcasts the program 2.

IGMP snooping listener results:

Vlan 100 The multicast table created by igmp snooping shows: Ports 1, 2, 6, 10 In group Group1,

port 1, 12 is in group Group2.

Four hosts can normally receive their own programs of interest, ports 2,6,10 will not receive the flow of program 2, port 12 will not receive the flow of program 1.

6.4. IGMP Snooping troubleshooting help

6.4.1. Monitoring and debugging commands

6.4.1.1. show ip igmp snooping

Command: show ip igmp snooping [v lan <*vlan-id*>]

Parameters: <vlan-id> specifies the vlan number of the IGMP snooping information to be displayed.

Command mode: Privileged user configuration mode

Usage Guide: If you do not specify a VLAN ID, this command displays IGMP Snooping information for all VLANs. If the VLAN ID is specified, the IGMP snooping details of the VLAN are displayed.

For example:

1. Display the IGMP snooping information of the switch

#show ip igmp snooping

2. Display the IGMP snooping details of VLAN1.

#show ip igmp snooping vlan 1

Chapter 7 ACL Configuration

7.1. ACL Overview

ACL (Access Control Lists)is a packet filtering mechanism implemented by switch. By allowing or rejecting specific packets to access the network, the switch can control network access and effectively guarantee the safe operation of the network. The user can create a set of rules based on specific message (rule), each rule is described by the data package, some information of action: allow or reject (permit) through (deny). Users can apply these rules to a specific switch port so that a particular direction of data flow on a particular port must enter and exit the switch in accordance with the specified ACL rules.

7.1.1. Access-list

Access-list is an ordered set of statements, each of it corresponds to a specific rule (rule). Each rule includes filtering information and actions that should be taken to match the rule. The information contained in Rule can include a valid combination of conditions such as Action, dmac-type, evc-policer, frame-type, ingress, mirror, and so on.

7.1.2. Access-list Action

Access-list actions are divided into three types: allowing filtering through (permit) or rejection through (deny) or port selection (filter). Details are as follows:

- permit indicates permission to pass, under this command, effective port range for all ports.
- Deny indicates rejection, and under this command, the port is valid for all ports.
- Filter means port selection filtering, followed by port selection, rejection of selected ports, and instruction

7.2. ACL Configuration

7.2.1. ACL Configuring task sequences

1. Set access-list ace
2. Set access-list rate-limiter
3. Delect access-list statistics
4. Recover access-list rate-limiter
5. Delect access-list ace
6. Delect access-list rate-limiter
7. Check access-list interface ect
8. Check access-list ace status

1. Set access-list ace

Global configuration mode

Command:

access-list ace [update] <ace_id> [next { <ace_id_next> | last }] [ingress { switch <ingress_switch_id> | switchport { <ingress_switch_port_id> | <ingress_switch_port_list> } | 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 }] [dmac { <etype_dmac> | any }] | arp [sip { <arp_sip> | any }] [dip { <arp_dip> | any }] [smac { <arp_smac> | any }] [arp-opcode { arp | rarp | other | any }] [arp-flag [arp-request { <arp_flag_request> | any }] [arp-smac { <arp_flag_smac> | any }] [arp-tmac { <arp_flag_tmac> | any }] [arp-len { <arp_flag_len> | any }] [arp-ip { <arp_flag_ip> | any }] [arp-ether { <arp_flag_ether> | any }]] | ipv4 [sip { <sipv4> | any }] [dip { <dipv4> | any }] [ip-protocol { <ipv4_protocol> | any }] [ip-flag [ip-ttl { <ip_flag_ttl> | any }] [ip-options { <ip_flag_options> | any }] [ip-fragment { <ip_flag_fragment> | any }]] | ipv4-icmp [sip { <sipv4_icmp> | any }] [dip { <dipv4_icmp> | any }] [icmp-type { <icmpv4_type> | any }] [icmp-code { <icmpv4_code> | any }] [ip-flag [ip-ttl { <ip_flag_icmp_ttl> | any }] [ip-options { <ip_flag_icmp_options> | any }] [ip-fragment { <ip_flag_icmp_fragment> | any }]] | ipv4-udp [sip { <sipv4_udp> | any }] [dip { <dipv4_udp> | any }] [sport { <sportv4_udp_start> [to <sportv4_udp_end>] | any }] [dport { <dportv4_udp_start> [to <dportv4_udp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_udp_ttl> | any }] [ip-options { <ip_flag_udp_options> | any }] [ip-fragment { <ip_flag_udp_fragment> | any }]] | ipv4-tcp [sip { <sipv4_tcp> | any }] [dip { <dipv4_tcp> | any }] [sport { <sportv4_tcp_start> [to <sportv4_tcp_end>] | any }] [dport { <dportv4_tcp_start> [to <dportv4_tcp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_tcp_ttl> | any }] [ip-options { <ip_flag_tcp_options> | any }] [ip-fragment { <ip_flag_tcp_fragment> | any }]] [tcp-flag [tcp-fin { <tcpv4_flag_fin> | any }] [tcp-syn { <tcpv4_flag_syn> | any }] [tcp-rst { <tcpv4_flag_rst> | any }] [tcp-psh { <tcpv4_flag_psh> | any }] [tcp-ack { <tcpv4_flag_ack> | any }] [tcp-urg { <tcpv4_flag_urg> | any }]] | ipv6 [next-header { <next_header> | any }] [sip { <sipv6> [sip-bitmask <sipv6_bitmask>] | any }] [hop-limit { <hop_limit> | any }] | ipv6-icmp [sip { <sipv6_icmp> [sip-bitmask <sipv6_bitmask_icmp>] | any }] [icmp-type { <icmpv6_type> | any }] [icmp-code { <icmpv6_code> | any }] [hop-limit { <hop_limit_icmp> | any }] | ipv6-udp [sip { <sipv6_udp> [sip-bitmask <sipv6_bitmask_udp>] | any }] [sport { <sportv6_udp_start> [to <sportv6_udp_end>] | any }] [dport { <dportv6_udp_start> [to <dportv6_udp_end>] | any }] [hop-limit { <hop_limit_udp> | any }] | ipv6-tcp [sip { <sipv6_tcp> [sip-bitmask <sipv6_bitmask_tcp>] | any }] [sport { <sportv6_tcp_start> [to <sportv6_tcp_end>] | any }] [dport { <dportv6_tcp_start> [to <dportv6_tcp_end>] | any }] [hop-limit { <hop_limit_tcp> | any }] [tcp-flag [tcp-fin { <tcpv6_flag_fin> | any }] [tcp-syn { <tcpv6_flag_syn> | any }] [tcp-rst { <tcpv6_flag_rst> | any }] [tcp-psh { <tcpv6_flag_psh> | any }] [tcp-ack { <tcpv6_flag_ack> | any }] [tcp-urg { <tcpv6_flag_urg> | any }]] }] [action { permit | deny | filter { switchport <filter_switch_port_list> | interface (<port_type> [<fliter_port_list>]) } }] [rate-limiter { <rate_limiter_id> | disable }] [evc-policer { <evc_policer_id> | disable }] [mirror [disable]] [logging [disable]] [shutdown [disable]] [lookup-second [disable]] [redirect { switchport { <redirect_switch_port_id> | <redirect_switch_port_list> } | interface

{ <port_type> <redirect_port_id> | (<port_type> [<redirect_port_list>]) } | disable }]

Explanation:

Global configuration mode, configuration access-list ace

2. Set access-list rate-limiter

Demand	Explanation
Global configuration mode	
access-list rate-limiter [<rate_limiter_list>] { pps <pps_rate> | 10pps <pps10_rate> | 100pps <pps100_rate> | 25kbps <kpbs25_rate> | 100kbps <kpbs100_rate> }	Set access-list classification of speed limits.

3. Delect access-list statistics

Demand	Explanation
Privileged mode	
clear access-list ace statistics	Delect access-list statistics

4. Recover access-list rate-limiter

Demand	Explanation
Global configuration mode	
default access-list rate-limiter [<rate_limiter_list>]	Recoverter access-list rate-limiter。

5. Delect access-list ace

Demand	Explanation
Global configuration mode	
no access-list ace <ace_list>	Delect access-list ace

6. Delect access-list rate-limiter

Demand	Explanation
Global configuration mode	
no access-list rate-limiter [<rate_limiter_list>]	Delect access-list rate-limiter

7. Check access-list interface ect

Demand	Explanation
Privileged mode	
show access-list [interface [(<port_type> [<port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [<ace_list>]]	Check access-list interface ect confiration

8. Check access-list ace-status

Demand	Explanation
Privileged mode	
show access-list ace-status [static] [link-oam] [loop-protect] [dhcp] [ptp] [upnp] [arp-inspection] [evc] [mep] [ipmc] [ip-source-guard] [ip-mgmt] [tt-loop] [y1564] [ztp] [conflicts] [switch <switch_list>]	Check access-list ace status

7.2.2. ACL Setting Demand

7.2.2.1. access-list ace

Command: access-list ace [update] <ace_id> [next { <ace_id_next> | last }] [ingress { switch <ingress_switch_id> | switchport { <ingress_switch_port_id> | <ingress_switch_port_list> } | 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 }] [dmac { <etype_dmac> | any }] | arp [sip { <arp_sip> | any }] [dip { <arp_dip> | any }] [smac { <arp_smac> | any }] [arp-opcode { arp | rarp | other | any }] [arp-flag [arp-request { <arp_flag_request> | any }] [arp-smac { <arp_flag_smac> | any }] [arp-tmac { <arp_flag_tmac> | any }] [arp-len { <arp_flag_len> | any }] [arp-ip { <arp_flag_ip> | any }] [arp-ether { <arp_flag_ether> | any }]] | ipv4 [sip { <sipv4> | any }] [dip { <dipv4> | any }] [ip-protocol { <ipv4_protocol> | any }] [ip-flag [ip-ttl { <ip_flag_ttl> | any }] [ip-options { <ip_flag_options> | any }] [ip-fragment { <ip_flag_fragment> | any }]] | ipv4-icmp [sip { <sipv4_icmp> | any }] [dip { <dipv4_icmp> | any }] [icmp-type { <icmpv4_type> | any }] [icmp-code { <icmpv4_code> | any }] [ip-flag [ip-ttl { <ip_flag_icmp_ttl> | any }] [ip-options { <ip_flag_icmp_options> | any }] [ip-fragment { <ip_flag_icmp_fragment> | any }]] | ipv4-udp [sip { <sipv4_udp> | any }] [dip { <dipv4_udp> | any }] [sport

{ <sportv4_udp_start> [to <sportv4_udp_end>] | any }] [dport { <dportv4_udp_start> [to <dportv4_udp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_udp_ttl> | any }] [ip-options { <ip_flag_udp_options> | any }] [ip-fragment { <ip_flag_udp_fragment> | any }]] | ipv4-tcp [sip { <sipv4_tcp> | any }] [dip { <dipv4_tcp> | any }] [sport { <sportv4_tcp_start> [to <sportv4_tcp_end>] | any }] [dport { <dportv4_tcp_start> [to <dportv4_tcp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_tcp_ttl> | any }] [ip-options { <ip_flag_tcp_options> | any }] [ip-fragment { <ip_flag_tcp_fragment> | any }]] [tcp-flag [tcp-fin { <tcpv4_flag_fin> | any }] [tcp-syn { <tcpv4_flag_syn> | any }] [tcp-rst { <tcpv4_flag_rst> | any }] [tcp-psh { <tcpv4_flag_psh> | any }] [tcp-ack { <tcpv4_flag_ack> | any }] [tcp-urg { <tcpv4_flag_urg> | any }]] | ipv6 [next-header { <next_header> | any }] [sip { <sipv6> [sip-bitmask <sipv6_bitmask>] | any }] [hop-limit { <hop_limit> | any }] | ipv6-icmp [sip { <sipv6_icmp> [sip-bitmask <sipv6_bitmask_icmp>] | any }] [icmp-type { <icmpv6_type> | any }] [icmp-code { <icmpv6_code> | any }] [hop-limit { <hop_limit_icmp> | any }] | ipv6-udp [sip { <sipv6_udp> [sip-bitmask <sipv6_bitmask_udp>] | any }] [sport { <sportv6_udp_start> [to <sportv6_udp_end>] | any }] [dport { <dportv6_udp_start> [to <dportv6_udp_end>] | any }] [hop-limit { <hop_limit_udp> | any }] | ipv6-tcp [sip { <sipv6_tcp> [sip-bitmask <sipv6_bitmask_tcp>] | any }] [sport { <sportv6_tcp_start> [to <sportv6_tcp_end>] | any }] [dport { <dportv6_tcp_start> [to <dportv6_tcp_end>] | any }] [hop-limit { <hop_limit_tcp> | any }] [tcp-flag [tcp-fin { <tcpv6_flag_fin> | any }] [tcp-syn { <tcpv6_flag_syn> | any }] [tcp-rst { <tcpv6_flag_rst> | any }] [tcp-psh { <tcpv6_flag_psh> | any }] [tcp-ack { <tcpv6_flag_ack> | any }] [tcp-urg { <tcpv6_flag_urg> | any }]] }] [action { permit | deny | filter { switchport <filter_switch_port_list> | interface (<port_type> [<fliter_port_list>]) } }] [rate-limiter { <rate_limiter_id> | disable }] [evc-policer { <evc_policer_id> | disable }] [mirror [disable]] [logging [disable]] [shutdown [disable]] [lookup-second [disable]] [redirect { switchport { <redirect_switch_port_id> | <redirect_switch_port_list> } | interface { <port_type> <redirect_port_id> | (<port_type> [<redirect_port_list>]) } | disable }]

Functions: Use the access-list ace global configuration mode command to set up access-list ace. Any parameter that is not described will be set to the default value.

Parameters：

Policy ID：The allowed value is 0-255, the default value is 0; Action: configurable to allow forwarding or deny forwarding, and the default configuration is to allow forwarding. Rate Limiter ID: configurable value to be closed or configuration value 1-16, default configuration is closed. EVC Policer: set the EVC speed limiter to enable or close. The default value is off. Note: the ACL speed limiter and the EVC speed limiter do not work at the same time. EVC Policer ID: configurable values are closed or 1-256. The default value is off.

Demand Mode：Global configuration mode

Default：No access lists are configured.

Usering Guide：When a user first configures a specific ACE ID, creates the ACE of this number, and then adds the table entry in this ACE.

Example：Create a ACE ID 110 access control list, allowing the frame format of ipv4-icmp

message from 1/4 through ACE port; create ID 111 access control list, prohibit the format for the frame type ARP from the port by radio.

(config)# access-list ace 110 action permit frame-type ipv4-icmp ingress interface GigabitEthernet 1/4

(config)# access-list ace 111 dmac-type broadcast frame-type arp action deny

7.2.2.2. **access-list rate-limiter**

Command: access-list rate-limiter [<rate_limiter_list>] { pps <pps_rate> | 10pps <pps10_rate> | 100pps <pps100_rate> | 25kbps <kpbs25_rate> | 100kbps <kpbs100_rate> }

Function: set access-list speed limit's classification of grade

Parameters：Rate Limiter ID：Rate limitation ID setting.Rate：optional unit:pps and kbps。

Demand Mode：Global configuration mode

Default：Default 1pps。

Using Guide：Users can configure different values as needed.

Example：Set Rate Limiter ID as 1 level,rate limitation is 200kbps.

(config)# access-list rate-limiter 1 100kbps 2

7.2.2.3. Clear access-list

Command: clear access-list ace statistics

Functions：Delect access-list statistics。

Demand Mode：Privileged mode

Using Guide：In the configured access control settings, hit count statistics are allowed or prohibited messages, execute this command, reset the counter, and start counting again.

Example：Perform the cleanup access-list statistics command.

clear access-list ace statistics

7.2.2.4. **default access-list rate-limiter**

Command: default access-list rate-limiter [<rate_limiter_list>]

Functions：Recover access-list default rate limitation

Command Mode：Global configuration mode

Using Guide: This command restores the access-list default rate limit to 1PPS as the default value.

Example：Recover access-list rate-limiter ID1 rate limitation,recover default

(config)# default access-list rate-limiter 1

7.2.2.5. **no access-list ace**

Command: no access-list ace <ace_list>

Functions：Recover access-list default rate limitation

Command Mode： Global configuration mode

Using Guide： This command restores the access-list default rate limit to 1PPS as the default value.

Example： Recover access-list rate-limiter ID1 rate limitation,recover default

(config)# no access-list ace 10

7.2.2.6. no **access-list rate-limiter**

Command：no access-list rate-limiter [<rate_limiter_list>]

Functions： Delect access-list rate limitation

Command Mode： Global configuration mode

Using Guide： This command removes the access-list rate limit.

Example： Delect access-list rate-limiterID10 rate limitation.

(config)#no access-list rate-limiter 10

7.2.2.7. **show access-list**

Command：show access-list [interface [(<port_type> [<port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [<ace_list>]]

Functions：Check access-list interface ect

Parameters：<port_type> [<port_type_list>]Represents the type of port required to query and the number of ports.

Command Mode： Privileged mode

Using Guide： Under the show access-list command, you can query the interface or speed limit configuration as needed.

Example： Query port configuration for port 2; query rate configuration for speed limit level 2.

show access-list interface GigabitEthernet 1/2；

show access-list rate-limiter 2 。

7.2.2.8. **show access-list ace-status**

Command：show access-list ace-status [static] [link-oam] [loop-protect] [dhcp] [ptp] [upnp] [arp-inspection] [evc] [mep] [ipmc] [ip-source-guard] [ip-mgmt] [tt-loop] [y1564] [ztp] [conflicts] [switch <switch_list>]

Functions： Check access-list ace status

Parameters：

Static：The status displayed here is the parameter value.

Command Mode： Privileged mode

Example： Shows the configuration number of the switch access-list ace and the configuration detail results.

show access-list ace-status static

Chapter 8 **Qos Configuration**

8.1. QoS Overview

QoS (Quality, of, Service) is the ability of a network to provide better services to selected network communications using a wide variety of technologies. QoS is the quality of service, to provide a stable and predictable data transfer services, to meet the application requirements, QoS can not generate new bandwidth, but according to the needs of the application of network bandwidth management and network management to effectively set.

8.1.1. QoS term

CoS：Class of Service level,the classification information carried by the L2 802.1Q frame, occupies 3bits in the Tag field of the frame head, called the user priority, and the range is 0~7.

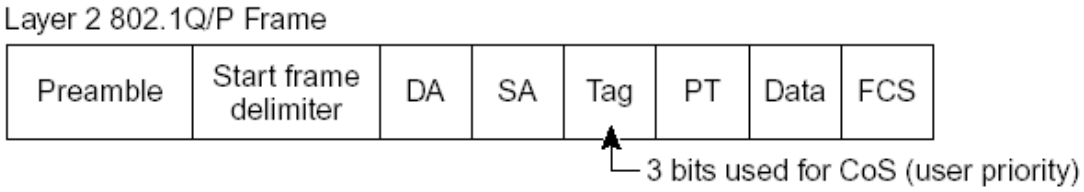


Diagram 10-1 CoS Priority

ToS：Type of Service，L3 IPv4 carries a byte field, the service type that marks the IP package, and the ToS field can be a DSCP value.

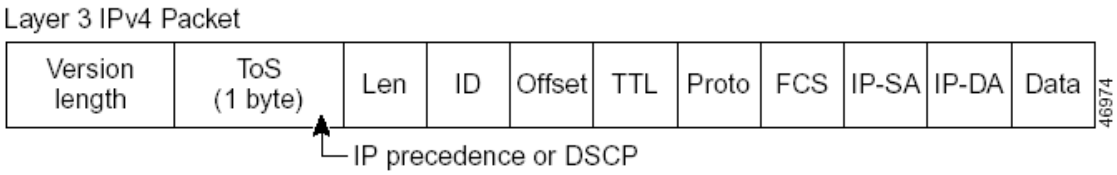


Diagram 10-2 ToS Priority

DSCP：Differentiated Services Code Point , L3 IP packet header carrying information, a total of 6bits, ranging from 0 to 63, backward compatible with IP Precedence.

Classification: QoS entry action, according to the packet to carry the classification of information

and ACLs, the packet traffic classification.

Supervise: QoS entry actions, develop regulatory policies, and monitor the rate of queues.

Rewriting: The export action of QoS, overriding the priority of the packet in the outbound direction.

Shaping: QoS export action, configure the rate of each queue.

Schedule: QoS export action, configure the export queue work.

8.2. QoS configuration

8.2.1. QoS Configure the task sequence

1. Configure the QoS port inbound direction
   Configure the port's trust mode, port inbound default CoS, DEI, PCP, DPL value, inbound direction priority classification
2. Configure QoS inbound supervision
   Configure the inbound direction rate control and configure the inbound queue rate supervision.
3. Rewrite the QoS outbound priority
4. Configure the rate of the QoS exit queue
5. Configure the queue queue work and weight
   Allocate the working mode of the queue to the strict priority mode or the WRR mode, and set the ratio of the 6 outgoing queue bandwidths.

1. Enter the QoS port inbound direction

Command	Explanation
Interface configuration mode	
qos trust [dscp |tag] **no qos trust**	Configure the port trust mode. The no operation of this command is to disable the current trust mode of the switch port.
qos cos {<*default-cos*> } **no qos cos**	Configure the default CoS value for the port. The no operation of this command is to restore the default.
qos dei <dei> **no qos dei**	Configure the port default DEI value. The no operation of this command is to restore the default.

qos dpl <dpl> **no qos dpl**	Configure the port default DPL value. The no operation of this command is to restore the default.
qos pcp <pcp> **no qos pcp**	Configure the port default PCP value. The no operation of this command is to restore the default.
qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl> **no qos map tag-cos pcp <pcp> dei <dei>**	Configure the port PCP-CoS mapping. The no operation of this command is to restore the default.
Command	Explanation
Global configuration mode	
qos map dscp-cos <dscp_num>cos <cos> dpl <dpl> **no qos map dscp-cos <dscp_num>**	Configure the port DSCP-CoS mapping. The no operation of this command is to restore the default.

2. Configure QoS inbound supervision

Command	Explanation
Global configuration mode	
qos policer <rate> [kbps | mbps | fps | kfps] [flowcontrol] **no qos policer**	Configure the inbound direction rate of the port. The no operation of this command is to restore the default configuration.
qos queue-policer queue <queue> <rate> [kbps | mbps] **no qos queue-policer queue <queue>**	Configure the port inbound queue rate control. The no operation of this command restores the default configuration.

3. Rewrite the QoS priority in the outbound direction

Command	Explanation
Global configuration mode	
qos tag-remark { pcp <pcp> dei <dei> | mapped } **no qos tag-remark**	Rewrite the port outbound priority; the no operation of

	this command is to restore the default configuration.

4. Configure the QoS exit queue rate

Command	Explanation
Global configuration mode	
qos queue-shaper queue <queue> <rate> [kbps | mbps] [excess] **no qos queue-shaper queue <queue>**	Configure the direction of the queue rate; the command no operation to restore the default configuration.

5. Configure the queue queue work and weight

Command	Explanation
Global configuration mode	
qos wrr <*weight0 weight1 weight2 weight3 weight4 weight5* > **no qos wrr**	Set the WRR weight of the switch port queue. The no operation of this command is to restore the default value.

8.2.2. QoS Configuration command

8.2.2.1. qos trust

Command: qos trust [dscp |tag]

no qos trust

Function: Configure the switch port trust status. The no operation of this command is to disable the current trust status of the switch port.

Parameters: dscp Configure the port trust status; dscp Configure the port to trust the DSCP value; tag Configure the port to trust the tag value.

Default: Do not trust any value.

Command mode: Interface configuration mode

Example: To configure the trusted dscp value on GigabitEthernet 1/1, that is, packets are classified by dscp.

(config)#interface GigabitEthernet 1/1

(Config-if)# qos trust dscp

8.2.2.2. qos cos

Command: qos cos {<*default-cos*> }

no qos cos

Function: Configure the default CoS value of the switch port. The no operation of this command is

to restore the default.

Parameters: <default-cos> The default CoS value for the switch port, in the range of 0 to 7.

Default: The default CoS value is 0.

Command mode: Interface configuration mode

user's guidance:

Example This example describes how to configure the default cos value to 5 on port GigabitEthernet 1/1. That is, if the packets coming from this port do not have a cos value, assign the default cos value to 5.

(config)#interface GigabitEthernet 1/1

(Config-if)# qos cos 5

8.2.2.3. qos dei

Command: qos dei <dei>

no qos dei

Function: Configure the default DEI value of the switch port. The no operation of this command is to restore the default.

Parameters: <DEI> The default DEI value for the switch port, in the range 0 to 1.

Default: The default CoS value is 0.

Command mode: Interface configuration mode

user's guidance:

Example: slightly

8.2.2.4. qos dpl

Command: qos dpl <dpl>

no qos dpl

Function: Configure the default dpl value of the switch port. The no operation of this command is to restore the default.

Parameters: <dpl> The default dpl value of the switch port, in the range of 0 to 1.

Default: The default dpl value is 0.

Command mode: Interface configuration mode

user's guidance:

Example: slightly

8.2.2.5. qos pcp

Command: qos pcp <pcp>

no qos pcp

Function: Configure the default pcp value of the switch port. The no operation of this

command is to restore the default.

Parameters: <pcp> The default pcp value of the switch port, in the range of 0 to 7.

Default: The default pcp value is 0.

Command mode: Interface configuration mode

user's guidance:

Example: slightly

8.2.2.6. qos map tag-cos

8.2.2.7. qos map tag-cos

Command: qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>

no qos map tag-cos pcp <pcp> dei <dei>

Function: Configure the port PCP-CoS mapping. The no operation of this command is to restore the default. The

Parameters: <pcp>: pcp value, range 0 to 7, <dei>: dei value, range 0 to 1, <cos>: cos value, range 1 to 7, <dpl>: dpl value, range 0 to 1 The

By default:

Command mode: Interface configuration mode

user's guidance:

Example: On port GigabitEthernet 1/1, map pcp 7 dei 1 to cos 7 dpl 0.

```
# con t
(config)# interface GigabitEthernet 1/1
(config-if)# qos map tag-cos pcp 7 dei 1 cos 7 dpl 0
(config-if)#
```

8.2.2.8. qos map dscp-cos

Command: qos map dscp-cos <dscp_num>cos <cos> dpl <dpl>

no qos map dscp-cos <dscp_num>

Function: Configure the port DSCP-CoS mapping. The no operation of this command is to restore the default. The

Parameters: <dscp_num>: dscp value, range 0 to 63, <cos>: cos, range 1 to 7, <dpl>: dpl value, range 0 to 1.

By default:

Command mode: global configuration mode

user's guidance:

Example: Mapping DSCP 7 to cos 0 dpl 1.

(config)# qos map dscp-cos 7 cos 0 dpl 0

8.2.2.9. qos policer

Command: qos policer <rate> [kbps | mbps | fps | kfps] [flowcontrol]

no qos policer

Function: Define a policy that defines the port bandwidth. The no operation of this command is to delete the specified policy.

Parameters: **<rate>** The average rate of traffic after classification, **[kbps | mbps | fps | kfps]**: unit, **[flowcontrol]**: flow control.

By default:

Command mode: Interface configuration mode

Usage Guidelines: This command configures the policy in interface mode.

Example: Create a policer on port GigabitEthernet 1/1, set to 20Mbit / s.
(config)# interface GigabitEthernet 1/1
(config-if)# qos policer 20 mbps

8.2.2.10. qos queue-policer

Command: qos queue-policer queue <queue> <rate> [kbps | mbps]

no qos queue-policer queue <queue>

Function: Define a policy that defines the queue bandwidth. The no operation of this command is to delete the specified policy.

Parameters: **<queue>**: Queue number, **<rate>** Average rate of traffic after classification, **[kbps | mbps]**: Units.

By default:

Command mode: Interface configuration mode

Usage Guidelines: This command configures the policy in interface mode.

Example: Create a policer on port GigabitEthernet 1/1 queue 0, set to 20M bits per second.
(config)# interface GigabitEthernet 1/1
(config-if)# qos queue-policer queue 0 20 mbps

8.2.2.11. qos tag-remark

Command: qos tag-remark { pcp <pcp> dei <dei> | mapped }

no qos tag-remark

Function: Rewrite the outbound direction of the port. The no operation of this command restores the default configuration.

Parameters: **<pcp>:** pcp value, **<dei>**: dei value, **mapped**: mapping

By default:

Command mode: Interface configuration mode

Usage Guidelines: This command configures the policy in interface mode.

Example: GigabitEthernet 1/1 outbound priority rewriting: pcp 7, dei 0.
(config)# interface GigabitEthernet 1/1
(config-if)# qos tag-remark pcp 7 dei 0

8.2.2.12. qos tag-remark

Command: qos queue-shaper queue <queue> <rate> [kbps | mbps] [excess]

no qos queue-shaper queue <queue>

Function: Configure the direction of the queue rate; the command no operation to restore the default configuration.

Parameters: **<queue>**: queue, <rate>: rate, **[kbps | mbps]:** unit, **[excess]**: allowed to exceed bandwidth.

By default:

Command mode: Interface configuration mode

user's guidance:

Example: The port GigabitEthernet 1/1 queue 1 rate is set to 200mbps and can exceed the bandwidth.

(config)# interface GigabitEthernet 1/1
(config-if)#qos queue-shaper queue 1 200 mbps excess

8.2.2.13. qos wrr

Command: qos wrr ***<weight0 weight1 weight2 weight3 weight4 weight5 >***

no qos wrr

Function: Set the WRR weight of the queue of the switch port. The no operation of this command is to restore the default value.

Parameters: **<weight0 weight1 weight2 weight3 weight4 weight5> WRR** weight value

By default:

Command mode: Interface configuration mode

user's guidance:

Example: Set the bandwidth ratio of the 6 outgoing queues of port 1 to 1: 2: 4: 4: 8: 8.

(config)# interface GigabitEthernet 1/1
(config-if)# qos wrr 1 2 4 4 8 8

8.3. QoS example

Case 1:

Change the weight of the port GigabitEthernet 1/1 export queue to 1: 2: 4: 4: 8: 8, configure

the trusted dscp mode, and set the default cos value of this port to 5.

The configuration steps are as follows:

#CONFIG

(config)#interface GigabitEthernet 1/1

(config-if)#qos wrr1 2 4 4 8 8

(config-if)# qos trust dscp

(config-if)# qos cos 5

Configuration results:

The QoS of the interface GigabitEthernet 1/1 is 1: 2: 4: 4: 8: 8. When the packets coming from GigabitEthernet 1/1 are sampled with cos values, they are placed in different priority queues according to the mapping of cos values to exit queues. If the incoming packets do not have cos values, set their cos values to 5 , According to the corresponding relationship, into the priority queue.

Chapter 9 **RSTP Configuration**

9.1. Introduction

STP(Spanning Tree Protocol) is a protocol established by the 802.1D standard developed by the IEEE protocol to prevent broadcast storms and provide link backup in the LAN. The device that runs the protocol chooses to block the loop network into a loopless tree network by interacting with each other, thus avoiding the proliferation and infinite loop of the packets in the loop network. STP is the lack of fast migration, you must wait 2 times Forward Delay time delay, the port can be transferred to the forwarding state.

To address this flaw in the STP protocol, IEEE introduced the 802.1w standard as a complement to the 802.1D standard. The Rapid Spanning Tree Protocol (RSTP) is defined in the IEEE 802.1w standard. RSTP protocol on the basis of the STP protocol made the following improvements make the convergence speed is much faster: the root port and the designated port were configured to quickly switch the replacement port (Alternate Port) and backup port (Backup Port), when the root port fails, The replacement port enters the forwarding state without any delay.

9.2. Basic concept

- Root bridge: In the tree network structure similar to the role of the root, the root bridge in the whole network only one, and the root bridge will change according to the network topology changes, not fixed. The root bridge periodically sends BPDU configuration messages, and other devices forward the configuration messages to ensure topology stability.
- Root port: the best port from the non-root bridge to the root bridge, that is, the port with the lowest cost of the root bridge. The root port is responsible for communicating with the root bridge. The root bridge device has only one root port and the root bridge device has no root port.
- Specify port: Forward the configuration message to other devices or LANs;
- Replace the port: the root port of the backup port, the root port fails, replace the port will become the new root port;
- Backup port: Specifies the backup port of the specified port. After the specified port fails, the backup port will be forwarded to the new designated port forwarding data.

9.3. BPDU Configuration message

In order to make the communication link is not ring, all the bridges in the LAN together

to calculate a spanning tree. This process determines the topology of the network by passing BPDUs between the devices. The data structure of BPDUs is shown in the following table:

…	Root bridge ID	Root path cost	Specify bridge ID	Specify port ID	Message age	Max age	Hello time	Forward delay	…
…	8 byte	4 byte	8 byte	2 byte	2 byte	2 byte	2 byte	2 byte	…

- Root bridge ID: 2 bytes Root bridge priority +6 bytes Root bridge MAC address;
- Root path cost: the sum of all port costs in the root bridge path;
- Specify bridge ID: 2 bytes Specify bridge priority +6 bytes Specify bridge MAC address;
- Specify port ID: port priority + port number;
- Message age: BPDU configuration message in the network to spread the survival period;
- Max age: Maximum lifetime that BPDU configuration messages can be saved in the device. When Message age> Max age, the BPDU message is discarded.
- Hello time: The interval at which BPDU configuration messages are sent;
- Forward delay: discarding - learning - forwarding state transition delay.

9.4. Implementation process

Each bridge uses BPDU packets to calculate the spanning tree.

1, the initial state, each port of the device will generate a configuration message with its own root bridge. The root bridge ID is its own device ID, the root path cost is 0, the bridge ID is the ID of its own device, and the designated port is the port.

2, the optimal configuration of the message selection, the equipment are sent out their own configuration messages, but also received other equipment to send the configuration message. Each port receives a configuration message followed by a comparison of the configuration BPDU of this port:

- If the configuration BPDU of this port is of high priority, no processing is performed.
- If the configuration BPDU of this port has a low priority, the contents of the configuration BPDU of the port are replaced with the contents of the received configuration BPDU.
- The device compares the configuration BPDUs of all ports to select the best configuration BPDU. Configure Message Comparison Principle:
- The configuration error of the smaller root bridge ID is higher;
- If the root bridge ID is the same, compare the root path cost. Compare the method: use the root path cost in the configuration message and add the path

cost corresponding to the port. The smaller priority of the configuration message is higher.

- If the path cost is the same, the port ID is specified, the port ID is specified, the port ID of the configuration BPDU is received, and the configuration BPDU with the smaller value is higher.

3. The choice of the root bridge, the root bridge of the spanning tree is the bridge with the smallest bridge ID.

4, the root port of choice, non-root bridge equipment will receive the optimal configuration of the port as the root port.

5. Specify the specified port configuration BPDU for each port according to the configuration BPDU of the root port and the path cost of the root port.

- Root bridge ID is replaced with the root bridge ID of the configuration BPDU of the root port;
- Root path cost is replaced by the root path cost of the root port configuration message plus the path cost corresponding to the root port;
- The specify the bridge ID to replace the ID of its own device;
- The specified port ID is replaced with its own port ID.

6. the specified port selection, if the above calculation of the configuration message is excellent, then the device will be designated as the port port, the port configuration message is calculated to replace the configuration message and forward; if the port configuration message is excellent, then The device does not update the configuration BPDU of the port and blocks the port. The blocked port can only receive RSTP packets. It can not receive and forward other data packets.

9.5. RSTP Configuration

9.5.1. RSTP configuration task

1. Enable the RSTP protocol.
2. Set the RSTP bridge priority.
3. Set the RSTP hello time.
4. Set the RSTP forward delay time.
5. Set the maximum lifetime of RSTP.
6. Set the RSTP version.
7. Enable the RSTP port.
8. Set the port priority.
9. Set the port path cost.
10. View RSTP information

1. Enable RSTP protocol

Command	Explanation
Interface configuration mode	
spanning-tree no spanning-tree	Set the RSTP protocol on / off.

2. Set the RSTP bridge priority

Command	Explanation
Interface configuration mode	
spanning-tree rstp bridge priority <prio>	Set the RSTP bridge priority. <Prio> is the bridge priority value. The default value is 32768, in the range of 0 to 65535.

3. Set RSTP hello time

Command	Explanation
Global configuration mode	
spanning-tree rstp hello-time < hello-time >	Set the RSTP hello time. <Hello-time> is the hello time value, in seconds. The default value is 2, in the range of 1 to 10.

4. Set RSTP forward delay time

Command	Explanation
Global configuration mode	
spanning-tree rstp forward-time <fwdtime>	Set the RSTP forward delay time. <Fwdtime> is the forward delay time value, in seconds. The default value is 15, in the range of 4 to 30.

5. Set RSTP maximum lifetime

Command	Explanation
Global configuration mode	
spanning-tree rst max-age <maxage>	Set RSTP maximum lifetime. <Maxage> is the maximum lifetime value in seconds. The default value is 20, in the range of 6 to 40.

6. Set the STP version

Command	Explanation
Global configuration mode	
spanning-tree mode { stp | rstp | mstp }	Set the STP version. <Stp | rstp | mstp> for the STP version

	number, select rstp mode, in the mode behind the input rstp

7. Enable the RSTP port

Command	Explanation
Global configuration mode	
spanning-tree no spanning-tree	Enable RSTP port or turn off RSTP port.

8. Set the port priority

Command	Explanation
Interface configuration mode	
spanning-tree rstp <instance> port-priority <prio>	Set the port priority. <Instance> is the port number, and <prio> is the priority value. The step is 16, in the range of 0 to 255.

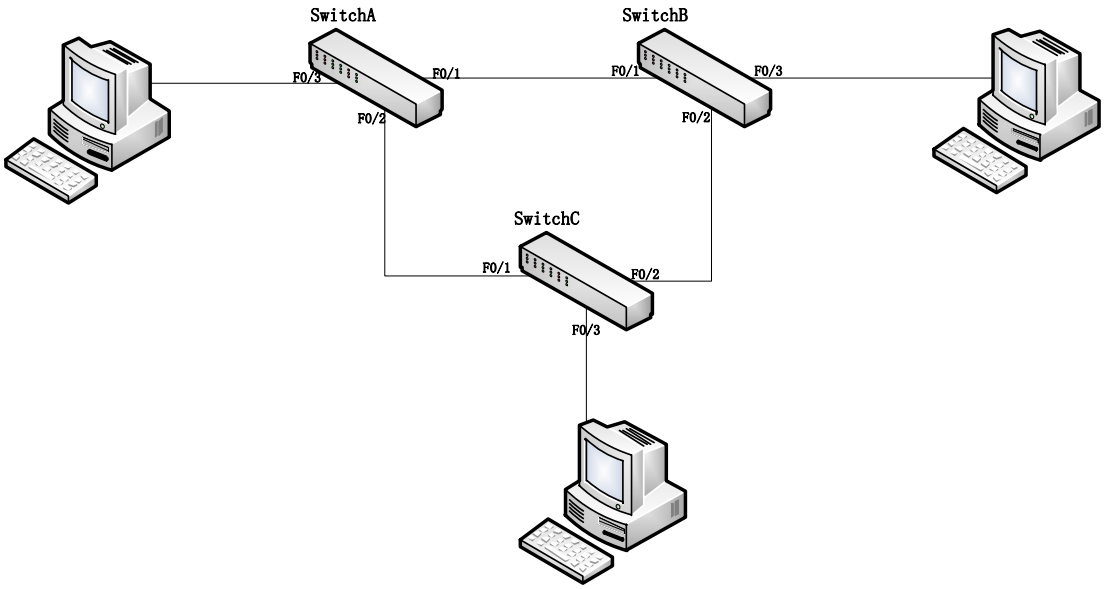
9. Set the cost of port path

Command	Explanation
Interface configuration mode	
spanning-tree rstp <instance> cost {<cost>|auto }	Set the port path cost value, <instance> for the port number, auto that automatically calculated. <Cost> is the cost of the path, the default is automatic calculation, the value range: 0 ~ 200000000.

10. View the RSTP information

Command	Explanation
Privilege mode	
show spanning-tree	View RSTP information.

9.6. Configuration example



Basic configuration of Switch A、B、C

#configure terminal

(config)#hostname SwitchA

(config)#interface GigabitEthernet 1/3

(config-if)#switchport access vlan 1

(config-if)#exit

(config)#interface GigabitEthernet 1/1-2

(config-if)#switchport mode trunk

(config-if-range)#exit

When configured for B / C switches, the corresponding A can be changed to B / C.

Switch A configures the spanning tree protocol

#configure terminal

(config)# spanning-tree mode rstp

(config)# interface GigabitEthernet 1/1

(config-if)# spanning-tree

(config-if)#exit

(config)# interface GigabitEthernet 1/2

(config-if)#spanning-tree

Switch B configures the spanning tree protocol

#configure terminal

(config)# spanning-tree mode rstp

(config)# interface GigabitEthernet 1/1

(config-if)#spanning-tree

(config-if)#exit

(config)# interface GigabitEthernet 1/2

(config-if)#spanning-tree

Switch C configuration spanning tree and A, B the same

Chapter 10 HSTW-Ring Configuration

10.1. Introduction

HSTW-Ring is the company with independent intellectual property rights,the use of distributed ring protection program. In the event of a link failure within 20ms can quickly switch to the network back to normal, to ensure stable and reliable communication.

10.2. Concept

INIT: the initial state of the switch;

Root: There is only one root in a ring network. Root is added by the switch. After joining the switch, it is determined that the election will change according to the change of the network topology. It is not fixed. Root periodically sends an Announce message, and the other device forwards the message to ensure that the topology is stable;

B-Root: has a ring port Link-down, or a ring port degradation (that is, the number of CRC packets exceeds the threshold) of the switch;

Normal: The remaining switches in the normal communication ring network except Root and B-Root;

Backup port: A communication port between the HSTW-Ring ring and the ring. You can configure multiple backup ports. All backup ports must exist in the same ring ring. First, the backup port of Link Up is the primary backup port. The primary backup port is in Forward State, the remaining backup ports are from the backup port, and the backup port is in the block state;

Forward state: port can receive, forward data;

Blocking state: A port can receive forwarding ring protocol packets and can not receive and forward other data packets.

10.3. Implementation

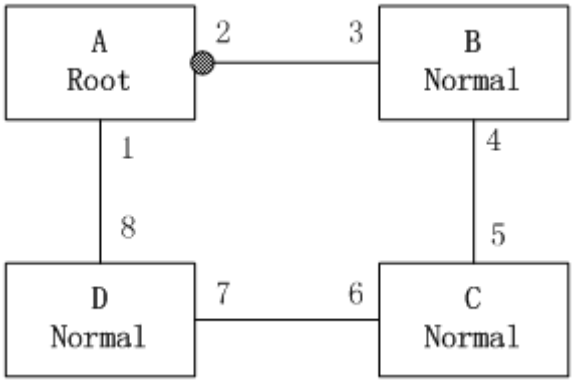
The HSTW-Ring protocol determines the role of the switch by forwarding Announce data packets to ensure that the redundant network is not ringing.

HSTW-Ring configuration meets the following conditions:

- All switches in the same ring must be configured with the same domain number;
- There is only one root in a ring, which can have multiple B-roots or Normal;
- Only one ring is allowed for each switch in a ring;

- For the two rings connected, the backup port can only be configured in one of the rings;
- Allow multiple backup ports to be configured in a ring;
- A switch can only be configured with one backup port in a ring

As shown in the following figure, the A, B, C, D switches work:

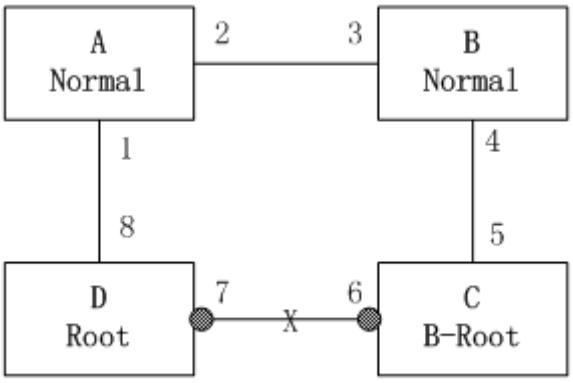


1. In the initial state, all switches are in INIT state;

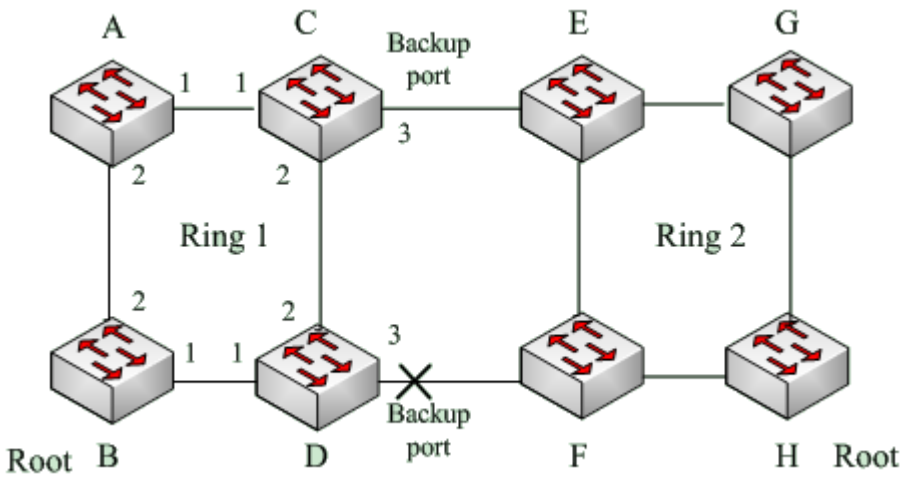
2, the switch connected to the ring network is configured to compare the forwarded Announce messages to select the optimal switch A as Root, Root first Link up ring port 1 is Forward state, and another ring port 2 is Block state ; The remaining switches are B-Root or Normal, B-Root or Normal two ring ports are in Forward state;

3, when the link CD fails, as shown in the following figure, switch A immediately from Root to Normal state, all devices re-election Root, then switches C and D have a selected Root, such as D, then C is B-Root, ports 6 and 7 are in the Block state.

Note: Changes in link status affect the status of all ring ports.



The HSTW-Ring protocol can also provide backup between two ring rings. As shown in the following figure, each switch can be configured with a backup port. The primary backup port is in Forward and the remaining backup ports are in the block state. If the primary backup port or link fails, it will re-select a data from the backup port to ensure that the redundant ring can not ring the normal communication.



10.4. HSTW-Ring configuration

10.4.1. HSTW-Ring configuration task

1. Perform the HSTW-Ring configuration.
2. View the HSTW-Ring information.
3. Remove the HSTW-Ring configuration.

1. **Perform the HSTW-Ring configuration**

Command	Explanation
Global configuration mode	
ring <id> port0 <port_type> <port0> port1 <port_type> <port1> [backup-port <port_type> <bport>] [priority <priority>] [crc-thre <crc_thre>]	Execute the ring configuration. <Id> is the domain number, in the range of 1 to 32; <Port_type> is the port type, with the actual change; <Port0> <port1> <bport> selected port; Priority priority, in the range 0-255; Crc-thre threshold, in the range of 25-65535.

2. **View the HSTW-Ring information**

Command	Explanation
Privilege mode	
show ring <id>	View the ring information, <id> is in the range of 1 to 32

3. **Remove the HSTW-Ring configuration**

Command	Explanation
Global configuration mode	
no ring <id>	Delete the ring configuration, <id> is in the range of 1 to 32

10.4.2. Precautions

- The aggregation port and the ring port are mutually exclusive. The aggregation port can not be configured as a ring port. The ring port can not join the aggregation group.
- Mirroring destination port and ring port configuration are mutually exclusive. The mirroring destination port can not be configured as a ring port. The ring port can not be configured as a mirroring destination port.
- Backup port select the port other than the port;
- The aggregation port and the backup port are mutually exclusive. The aggregation port can not be configured as a backup port. The backup port can not join the aggregation group.
- Mirroring destination port and backup port configuration are mutually exclusive. The mirroring destination port can not be configured as a backup port. The backup port can not be configured as a mirroring destination port.

Chapter 11 ERPS（ Ethernet Ring Protection Switching）

ERPS（Ethernet Ring Protection Switching）：Ethernet multi-ring protection technology, is defined by ITU-T

The standard number is ITU-T G.8032 / Y1344, hence it is called G.8032. It defines the RAPS (Ring Auto Protection Switching) protocol message and the protection switching mechanism.

11.1. ERPS Function configuration

1、create a new protection group, add port

2、configure the ERPS MEP

3、set the ERPS port role

4、set the ERPS version

5、set the ERPS protection VLAN

6、set the ERPS protection time

7、set the ERPS hysteresis time

8、Set whether the link is reversible and time-out

1、Create a new protection group, add port

Command	Explanation
Global configuration mode	
erps <group> major port0 interface <port_type> <port0>port1 interface <port_type> <port1> [interconnect] **no erps <group>**	Set / delete ERPS protection group ID, add port 0 and port 1

2、Configure ERPS MEP

Command	Explanation
Global configuration mode	
erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps <p1_aps> **no erps <group> mep**	Set / delete Signal Fail and APS MEP

3、Set the ERPS port role

Command	Explanation

Global configuration mode	
erps <group> rpl { owner | neighbor } { port0 | port1 } **no erps <group> rpl**	Set / remove port roles

4、Set the ERPS version

Command	Explanation
Global configuration mode	
erps <group> version { 1 | 2 } **no erps <group> version**	Set / delete ERPS version

5、set the ERPS protection VLAN

Command	Explanation
Global configuration mode	
erps <group> vlan { none | [add | remove] <vlans> } **no erps <group> vlan**	Set / remove ERPS protected VLANs

6、Set ERPS protection time

Command	Explanation
Global configuration mode	
erps <group> guard <guard_time_ms> **no erps <group> guard**	Set / delete ERPS protection time

7、Set ERPS hysteresis time

Command	Explanation
Global configuration mode	
erps <group> holdoff <holdoff_time_ms> **no erps <group> holdoff**	Set / delete ERPS hysteresis time

8、Set whether the link is reversible and time-out

Command	Explanation
Global configuration mode	
erps <group> revertive <wtr_time_minutes> **no erps <group> revertive**	Set / delete ERPS protection link is reversible and timeout

11.2. ERPS Configuration command

1、erps group port0 port1

Command: erps <group> major port0 interface <port_type> <port0>port1 interface <port_type> <port1> [interconnect]

no erps <group>

Function: Configure / delete ERPS protection group ID, add port 0 and port 1.

<Port_type>: port type; <port0> <port1>: Port mapping port for ports 0 and 1.

Command mode: global configuration mode

User Guide: Users need to configure according to the scene

Example: Add protection group 1, port 0 is switch port 1/1, port 1 is switch port 1/2.

con t

(config)#erps 1 major port0 interface GigabitEthernet 1/1 port1 interface interface GigabitEthernet 1/2

2、erps mep

Command：erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps <p1_aps>

no erps <group> mep

Function: Set / delete the Signal Fail and APS MEP

<P0_sf>: port 0 signal fail MEP; <p0_aps>: port 0 aps MEP; <p1_sf>: port 1 signal fail MEP; <p1_aps>: port 1 aps MEP.

Command mode: global configuration mode

User Guide: Users need to configure according to the scene

Example: Port 0 signal fail MEP 1, port 0 aps MEP 1, port 1 signal fail MEP 2, port 1 aps MEP 2.

con t

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

3、rpl

Command: erps <group> rpl { owner | neighbor } { port0 | port1 }

no erps <group> rpl

Function: Sets / deletes the port role

Parameters: owner | neighbor: port role; port0 | port1: the port corresponding to the role

Command mode: global configuration mode

User Guide: Users need to configure according to the scene

Example: The port 0 role is rpl owner

con t

(config)# erps 1 rpl owner port0

4、version

Command：erps <group> version { 1 | 2 }

no erps <group> version

Function: Set / delete ERPS version

Parameters: <group>: ERPS protection group ID; {1 | 2}: ERPS version

Command mode: global configuration mode

User Guide: Users need to configure according to the scene

Example: Set the ERPS version to 1

con t

(config)#erps 1 version 1

5、vlan

Command：erps <group> vlan { none | [add | remove] <vlans> }

no erps <group> vlan

Function: set / delete ERPS protection vlan

Parameters: <group>: ERPS protection group ID; {none | [add | remove] <vlans>}: add or remove vlan

Command mode: global configuration mode

User Guide: Users need to configure according to the scene

Example: Add VLAN1

con t

(config)# erps 1 vlan add 1

6、guard

Command：erps <group> guard <guard_time_ms>

no erps <group> guard

Function: Set / delete ERPS protection time

Parameters: <guard_time_ms>: ERPS protection time, default 500ms

Command mode: global configuration mode

User Guide: Users need to configure according to the scene

Example: Set the protection time to 400ms

con t

(config)# erps 1 guard 400

7、holdoff

Command：erps <group> holdoff <holdoff_time_ms>

no erps <group> holdoff

Function: Set / delete ERPS hysteresis time

Parameters: <holdoff_time_ms>: ERPS hysteresis time, default 500ms

Command mode: global configuration mode

User Guide: Users need to configure according to the scene

Example: Set the hysteresis time to 100ms

con t

(config)# erps 1 holdoff 100

8、revertive wtr

Command：erps <group> revertive <wtr_time_minutes>

no erps <group> revertive

Function: Set / delete ERPS to protect the link from reversible and time-out

Parameters: <wtr_time_minutes>: ERPS timeout time, default 1min

Command mode: global configuration mode

User Guide: Users need to configure according to the scene

Example: Set the timeout time to 2s

con t

(config)# erps 1 revertive 2

12. L3 Routing protocol

12.1 L3 forwarding

This switch supports Layer 3 forwarding. Layer 3 forwarding is three layer protocol packet forwarding (IP message) across the VLAN, the forwarding address is to use the IP address, when one interface of switch that receives the IP packet, according to their own routing table retrieval and then decided to the operation of the data packet according to the results, if the destination address of IP packets is another subnet connected with the switch, then it will be sent out this message from the switch to the corresponding interface. The switch can use the hardware to forward the IP packet, and the forwarding chip has the host routing table and the default routing table. Among them, the host routing table is used to store the host routing directly linked to the switch, and the default routing table storage (via the aggregation algorithm) network segment routing.

When forwarding unicast flow need routing（host routing or segment routing ）exist in the forwarding chip, flux is forwarded by hardware completely, not like a router or the CPU, thus greatly improve the efficiency of forwarding, can achieve Link-speed forwarding.

12.2 Layer3 interface introduction.

You can create a Layer3 interface on the switch. The Layer3 interface is not an actual physical interface, it is a virtual interface. The three layer interface is created on the basis

of a VLAN. A three layer interface could contain one or more two layer interfaces (they belong to one same VLAN), and it also could not contain two-layer interfaces. At least one of the two-layer interfaces is UP state, then the three-layer interface could be UP state, otherwise it is DOWN state. All three layer interfaces in the switch use the same MAC address by default, which is selected from the MAC address reserved by the switch when the three-layer interface is created. Three layer interface is the basis of three layer protocol, you can configure the IP address on a three layer interface, the switch can be configured in three layers of the IP address of the interface, and other equipment for the transmission of the IP protocol. Switches can also forward IP protocol messages between different layer 3 interfaces.

Command：interface vlan <vlan-id>

no interface vlan <vlan-id>

Function：Create a VLAN interface that creates a three-layer interface for a switch; The no operation of this command is to delete the three-layer interface specified by the switch.

Parameter：<vlan-id> Is the VLAN ID of the established VLAN.

By default：There is no three-layer interface by default.

Command mode：Global configuration mode

Use guide：Before creating the VLAN interface (three-layer interface), you need to configure the VLAN first, and see the VLAN section for details. Use this command to enter the VLAN interface (three layer interface) configuration mode while creating the VLAN interface (three-layer interface). After the VLAN interface (three-layer interface) is created, you can still use the interface VLAN command to enter the three-layer interface mode.

For example：Create a VLAN interface (three-layer interface) on VLAN 1.

switch (config)#interface vlan 1

12.3 Routing protocol

In an Internet network, one host must choose a suitable path through a series of routers or a three-layer switch to access the remote host.

The router or the Layer 3 switch calculated the path by the CPU. The difference is

that the path of the Layer 3 switch is added to the switching chip and link-speed forwarded by the chip. The router starts by storing the calculated path in the routing table and the routing cache region, and the CPU is responsible for the data forwarding. It can be seen that both routers and Layer 3 switches can choose the path, and Layer 3 switch has a strong advantage in data forwarding. Here is a brief description of the basic principles and methods of path selection for a three-layer switch.

In the process of path selection, each layer 3 switch is only responsible to choose a right in the middle of the path according to the destination address of the received packets, then sends the packet to next layer 3 switch, until the last Layer 3 swith on the end of the path sends the packets to the destination host. The path chosen by each three-layer switch for transferring packets to the next three-layer switch is called routing. Routing can be divided into direct routing, static route and dynamic routing.

Direct routing is the path to the network connected to the three-layer switch directly , and the three-layer switch can obtain it without calculation.

Static routing is the path to a network or a particular host which are specified manually, and static is not allowed to change at will. The advantages of static routing are simple and easy to match, stable and restrict illegal routing changes, so as to realize load sharing and facilitate routing backup. However, because of the artificial setting, the routing for large networks is too large and complex, so static routing is not suitable to be used for medium and large networks.

Dynamic routing refers to the path to some network or specific host, and this path is calculated dynamically based on the initiated routing protocol by a three-layer switch. If a three-layer switch cannot be reached by next hop in the path, the three-layer switch can automatically discard the path through that three-layer switch and select the path through the other three-layer switch.

Dynamic routing protocols are generally divided into two categories: internal gateway routing protocol (IGP) and external gateway routing protocol (EGP). The internal gateway routing protocol (IGP) is the protocol used to calculate the routing of the destination within an autonomous system. The internal gateway dynamic routing protocols supported by the Layer 3 switch have RIP and OSPF routing protocols, which can configure RIP and OSPF

routing protocols as needed. Layer 3 switches support running multiple internal gateway dynamic routing protocol at the same time, also can introduce other dynamic routing protocols and static routing in a dynamic routing protocol for linking multiple routing protocols

12.3.1 The routing table

As mentioned earlier, a Layer 3 switch is mainly used to establish the current routing from the current Layer 3 switch to a network or a specific host, and forward packets based on the routing. Each layer 3 switch has a routing table that records all the routes used by the Layer 3 switch. Each route in the routing table points that the packets to a subnet or host should be sent via which vlan interface of layer 3 switches to reach its destination or to the destination path to next layer 3 switches.

The routing table contains the following main contents:

1. Destination address: the destination address or destination network used to identify IP packets.

2. Network mask: to identify the network segment address of the destination host or the Layer 3 switch with the destination address. The network mask consists of a number of consecutive "1" , usually marked with a decimal mark (typically address constitute by 1-4 groups of 255). After the destination address and network mask "and", you can get the network address of the destination host or the network segment of the Layer 3 switch. For example, the destination address is 200.1.1.1, and the network address of the host or Layer 3 switch whose mask code is 255.255.255.0 is 200.1.1.0.

1. Output interface: specifies which interface of the IP packet will be forwarded from the three layer switch.

2. Next layer 3 switch (next hop) IP address: specifies the next layer3 switch which the IP packets will be routed through.

3.Routing priority: There might be several different next hop routes for the same destination. These routes may be found by different dynamic routing protocols, or may be static routing by artificial configuration. The high priority (small number) will become the current best route. Users can configure multiple routes with different priority to the

same destination, and the layer 3 switch will select the only route for IP packet forwarding in priority order.

To prevent routing tables from being too large, could set a default route. Once failed to looking the routing table, the default route will be selected to forward the packet.

12.3.2 Static routing

（1） Static route introduction.

As mentioned earlier, static routing refers to the path that is assigned manually to a network or a particular host. The advantages of static routing are simple and easy to match, stable, and can prohibit illegal routing changes, and it could facilitate load sharing and routing backup. However, it also has many disadvantages. Static routing is static. Once the network fails and cannot automatically modify the route, It must be manually configured, it is not suitable for the medium and large network.

Static routing is mainly used in two situations: 1) for stable networks, static routing can be used to reduce the load of routing and routing data streams. For example, routing to a STUB network can be a static route. 2) for routing backup, static routing can be used (static routing is configured on the backup line, and the routing priority is lower than the main road).

Static and dynamic routing can exist at the same time, and the layer 3 switch chooses the highest priority route according to the priority of routing protocol. At the same time, in the dynamic routing can add the static routing into dynamic routing by reintroducing to the static routing (redistribute), and change the introduction of the static routing priority according to the need.

（2） Default route introduction.

The default route is also a static route, which is used only when no matching route is found. In the routing table, the representation of the default route is 0.0.0.0 for the destination address, and the network mask is also the route of 0.0.0.0. If there are no packets in a routing table to reach the destination, also does not have a default route, the packet will be discarded, and return an ICMP message to the source address and pointed out that the destination address or network inaccessible.

12.3.2.1 Static routing configuration.

1. Enable routing function.
2. Static routing configuration.
3. Default routing configuration.

1. Enable routing function

Command	Explain
Global configuration mode	
ip routing **no ip routing**	Enable/disable routing capabilities.

2. Static routing configuration.

Command	Explain
Global configuration mode	
ip route <*ipv4_addr*> < *ipv4_netmask*> < *ipv4_gateway*> [<*distance*>] **no ip route <*ipv4_addr*> < *ipv4_netmask*> < *ipv4_gateway*> [<*distance*>]**	Configure static routing; The no operation of this command is to remove the static route.

3. Default routing configuration

Command	Explain
Global configuration mode	
ip route 0.0.0.0 0.0.0.0 < *ipv4_gateway*> [<*distance*>] **no ip route 0.0.0.0 0.0.0.0 < *ipv4_gateway*> [<*distance*>]**	Configure the default route; The no operation of this command is to delete the default route.

12.3.2.2 introduction of static routing configuration commands.

- **ip route**
- **show ip route**

ip route

Command：ip route <*ipv4_addr*> < *ipv4_netmask*> < *ipv4_gateway*> [<*distance*>]

no ip route <*ipv4_addr*> < *ipv4_netmask*> < *ipv4_gateway*> [<*distance*>]

Function：Configure static routing; The no operation of this command is to remove the

static route.

Parameter：*<ipv4_address> and <ipv4_mask>* are respectively destination IP address and subnet mask, dot decimal format; ***<ipv4_gateway>***For the next hop IP address, point decimal format;***<distance>***is the routing priority. The range:1～255，The smaller the distance, the higher the priority.

By default：。

Static routing of a three-layer switch has a default priority of 1

Command mode： Global configuration mode

Use guide: When configuring the next hop of a static route, you can assign the way routing packet sending to the next hop IP address.

The default distance of the various routing types of the layer 3 switch is:

Routing type	Preference Value
Direct routing	0
Static routing	1
OSPF	110
RIP	120
IBEP	200
EBGP	20

Without changing various routing priority values, direct routing has the highest priority, followed by static routing, EBGP, OSPF, RIP, and IBGP.

For example

Example 1．Add a static routing

Switch(config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1

Example 2．Add a default routing

Switch(config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1

show ip route

Command：show ip route [<*ipv4_addr*>] [*ipv4_netmask*] [{connected | static | rip| ospf | bgp | isis}] [<*vlan-id*>]

Function：Show routing table

Parameter：***<ipv4_addr>is target network ad***；**[*ipv4_netmask*] means** mask of destination network,**connected means direct routing**；**static means static routing**；**rip means RIP routing**；**ospf means** OSPF routing； **bgp means** BGP routing；**isis means** isis routing；***<vlan-id>* means** vlan identifier.

Command mode：Privileged user configuration mode.

User guide：Display the contents of the core routing table, including: routing type, destination network, mask, next hop address, interface, etc.

For example：

switch#show ip route

Codes: K - kernel route, C - connected, S - static, R - RIP,

O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,

> - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo

C>* 192.168.0.0/24 is directly connected, VLAN1

S 192.168.3.0/24 [1/0] via 192.168.2.0 inactive

Show information	Explain
C - connected	Direct connection route, which is directly connected with the three-layer switch;
S – static	Static routing, manually configured by the user.
R - RIP	RIP routing, three-layer switch obtained through RIP protocol;
O - OSPF	OSPF routing, the three-layer switch is obtained through the OSPF protocol.
B- BGP	BGP routing, routing through BGP protocol.
Destination	Target network;
Mask	The mask of the target network
Next hop	Next hop IP address

12.3.3 Configuration cases.

As showing in the below picture, this is a simple network constituted by 3 sets of layer 3 switches, each layer 3 switch's and PC's IP address network mask are 255.255.255.0, SWITCH-1 and SWITCH - 3 are configured by static routing to enable the communication between PC1 and PC3, the communication between PC3 to PC2 is realized throgh the static routing which is configured between SWITCH-3 to SWITCH -2, the communication between PC2 and PC3 is realized by the default routing which is configured on SWITCH-2.

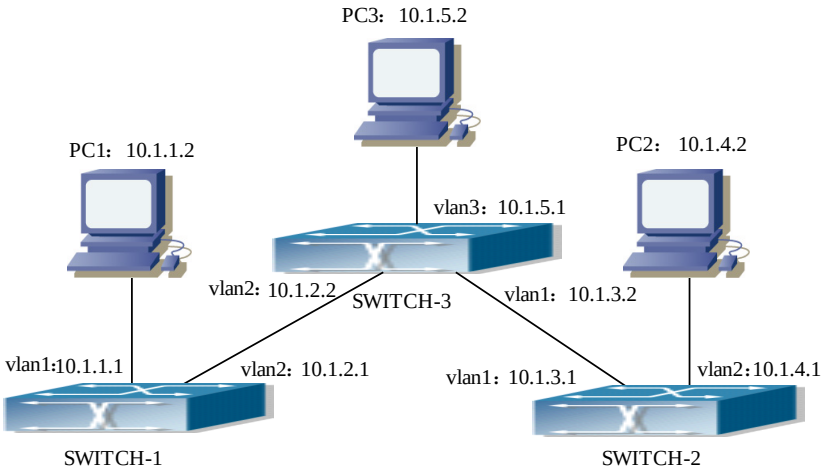


Figure 3-1　Static routing configuration diagram.

Configuration steps:

Layer 3 SWITCH-1 configuration

switch#config

switch(config)#ip route 10.1.5.0 255.255.255.0 10.1.2.2

switch(config)#ip route 10.1.4.0 255.255.255.0 10.1.2.2

Layer 3 SWITCH-3configuration

switch#config

！ The next hop takes the end-to-end IP address.

switch(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.1

！ The next hop takes the end-to-end IP address.

switch(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.1

Layer 3 SWITCH-2 configuration

switch#config

switch(config)#ip route 0.0.0.0 0.0.0.0 10.1.3.2

In this way, PC1 and PC3, PC2 and PC3 both of them can be pinged.

12.4 RIP introduction

RIP protocol was used in ARPANET network in the earliest time, and was dedicated in small and simple network. RIP protocol is a distance vector routing protocol based on Bellman - Ford algorithm. The network device which run distance vector routing protocol sends two kinds of information to adjacent devices regularly.

The number of hops that arrived at destination network, it is called metric, or the number of network.

What is the next hop, or the direction(vector)to be used to arrive at the destination network.

The distance vector Layer 3 switch regularly sends its entire routing table to adjacent layer 3 switches. The Layer 3 switch establishes its own routing information table based on the information received from the adjacent layer3 switch. Then the information is passed to its adjacent Layer 3r switch. The result is that the routing table is founded based on the second hand information, and the route that costs more than 15 jumps will be considered inaccessible.

The RIP protocol is an optional routing protocol, based on UDP, the host using RIP send and receive datagarm on the UDP 520 port. All layer 3 switches that run RIP protocol send routing table updated information to all neighbour Layer 3 switches every 30 seconds. If not receiving information from the opposite side within 180 seconds, then that device should be considered broken or can not connect with the network. But the route to that Layer 3 switch will still remain in the routing table for 120 seconds before being deleted.

Due to the Layer 3 switch that runs the RIP protocol set up the routing table by using the second hand information, there will be at least one problem -- the infinite number of counts.

For the network running RIP routing protocol , when a RIP routing become inaccessible, RIP layer 3 switches usually do not send a routing update message immediately, but waiting until the update cycle time interval (every 30 seconds) to send the update

datagram contains that routing information. Before receiving the update message, if the neighbor switch send the layer 3 switches a datagram contains neighbor layer 3 switches its routing table information, then it will cause "infinite number" phenomenon, which appear to inaccessible layer 3 switches routing metric fixed increasing phenomenon. This greatly affects routing selection and routing aggregation time.

To avoiding the "infinite number" phenomenon, the RIP protocol provides "horizontal segmentation" and "trigger update" and other mechanisms to solve the routing looping problem. The principle of "horizontal segmentation" is to avoid sending the routing to the same gateway which the routing is learned from, it includes "a simple horizontal segmentation" - deleting the routing which is learned from or sent to neighbour gateway, and the "reverse toxicity horizontal segmentation" - not only remove the routing mentioned above, but also set the cost of these routing to infinity. The "trigger update" mechanism defines that whenever the gateway changes the routing metric, it will immediately update the datagram and send it in a broadcast format without considering the status of a 30-second update timer.

The RIP protocol includes version 1 and version 2: RFC1058 introduces the RIP-I protocol; RFC2453 introduces the RIP-II protocol, which is compatible with RFC1723 and RFC1388. RIP-I sends routing updates by sending a broadcast datagram, which does not support subnet masks and authentication. There are some fields in the RIP-I datagram are not used, and the requirements are guaranteed to be full "0", so if the RIP-I is used for full "0" field checks, if these fields are not "0", then the RIP-I datagram is discarded. RIP - II version is better than RIP - I version, it adopts the way of multicast datagrams send routing updates datagram (multicast address for 224.0.0.9), it adds the subnet mask and RIP authentication domains (support simple text passwords and MD5 password authentication), support variable-length subnet mask. RIP-II uses part of full "0" domain in RIP - I, so no need to do full "0" field check .The Layer 3 switch send the RIP-II datagram in multicast way and receive the RIPI and RIP-II datagram by default.

Every layer 3 switch running RIP protocol has a routing database, it contains the routing items that layer 3 switch for all the the accessible destination, and the routing table is established based on this database. When layer 3 switch that support RIP protocol sends

routing updates to its adjacent devices, the routing update datagram contains the entire routing table set up by the layer 3 switch based on the routing database. Therefore, for the larger network system, each layer 3 switch needs to transmit and process large routing data and have heavy burden, which greatly affects the network performance.

At the same time, RIP protocol supports the introduction of routing information found by other routing protocols into the routing table.

The operation process of RIP protocol is described as follows:

1.Start the RIP, sending the request datagram in the form of broadcast to the adjacent layer 2 switch, after the adjacent equipment receive the request datagram, then the adjacent equipment response the request and send back the response data which contains local routing information.

2.After the layer 3 switch receives the response datagram, it changes the local routing table, and sends the trigger update datagram to the adjacent device at the same time, and the broadcast route updated information. After the adjacent three-layer switch receives the triggering update datagram, it sends the trigger update datagram to its neighboring layer 3 switch. After a series of broadcasts that trigger the update, each of the Layer 3 switches gets and maintains the latest routing information.

At the same time, the RIP layer 3 switch broadcasts the local routing table to its adjacent devices every 30 seconds. After receive the datagram to the local routing maintenance, the adjacent equipment mentains local routing and chooses the best route to broadcast the updated information to their equipment, make the updated routing finally achieve global effectively. In addition, RIP adapts the timeout mechanism and dispose the obsolete routing with timeout handler, which means if a layer 3 switches does not receive the periodic update data from one of its neighbors in a certain time interval (invalid timer interval), then that neighbour switch’s routing should be considered as invalid routing, then this neighbour switch’s routing could exist in the routing table for a certain time interval (hold down timer interval), then is deleted finally..

12.4.1 RIP configuration

1. Start RIP protocol
2. Configure RIP protocol parameters.

（1） Configure the RIP forward mechanism.

（2） Configure routing introduced.

（3） Configure the RIP protocol update, timeout, suppression and other timers.

（4） Configuration verification mode and password.

3. Configure the RIP version mode.

（1） Configure RIP version for all interfaces

（2） Configure the RIP version sent/received by the configuration interface

1. Start RIP protocol

Running on layer 3 switches RIP routing protocol of the basic configuration is simple, usually just need to open RIP switch, make it could send and receive RIP datagram, namely according to RIP the default configuration to send and receive RIP a datagram (layer 3 switches the default send RIP - receive RIP - I and II RIP - II).

Command	Explain
Global configuration mode	
[no] router rip	Open RIP protocol; The no operation of this command closes the RIP protocol.

2. Configure RIP protocol parameters.

（1） Configure the RIP distribution mechanism.

Command	Explain
Interface configuration mode	
[no]multicast	Indicates that the RIP three-layer switch allows all interfaces to broadcast packets or multicast packages; The no operation of this command sends a broadcast packet to the interface without sending a multicast package.

（2） Introduced Routing

Command	Explain

RIP protocol configuration mode.	
default-metric <*value*> **no default-metric**	Set the default routing weight of the incoming route; The no operation of this command resumes the default Settings.
redistribute { static | ospf | bgp} **[metric <*value*>]** **no redistribute { static | ospf | bgp }**	Introduce static, OSPF protocol or BGP protocol routing in RIP datagram; The no operation of this command cancels the route of the corresponding protocol introduced.

（3） Configure the RIP protocol update, timeout, suppression and other timers

Command	Explain
RIP protocol configuration mode.	
timer basic <*update_timer*> **<*info_timer*> <*collection_timer*>** **no timer basic**	Adjust the time when the RIP timer is updated, expired and suppressed; The no operation of this command responds to the default Settings.

（4） Configuration verification mode and password.

Command	Explain
Interface configuration mode	
ip rip authentication mode *{text| md5* ***{value }}*** **no ip rip authentication mode**	Set the type of validation to use; The no operation of this command is set to the default value and does not use validation.
ip rip authentication key-chain **<*name-of-chain*>** **no ip rip authentication key-chain**	Set the key to be used for validation; The no operation of this command is set to not use the authentication key.

3. Configure RIP version mode

（1） Configure RIP version for all interfaces.

Command	Explain

RIP protocol configuration mode.	
version { 1 | 2 } **no version**	Set all three layer switch interfaces to send/receive the RIP datagram version; The no operation recovers the default Settings, which is to send version 2 and receive the datagram of version 1 and 2.

（2） Configure the RIP version of the interface sent/received

Command	Explain
Interface configuration mode	
ip rip send version { 1 | 2 | 1 2 } **no ip rip send version**	Set interface to send RIP datagram version; The no operation of this command resumes the default setting, which is to send version 2.
ip rip receive version {1 | 2 | 1 2} **no ip rip receive version**	Set the interface to receive the RIP datagram version; The no operation of this command resumes the default Settings, which is the RIP datagram of version 1 and version 2.

12.4.2 RIP configuration command introduction.

1. Command：default-metric <*value*>

no default-metric

Function： Set the default routing weight of the incoming route; The no operation of this command is to restore the default value.

Parameters：<*value*>is the routing weight value, the value range is 1-16.。

Default: the default routing weight is 1.

Command mode: RIP protocol configuration mode.

Use guide: Default-metric command is used to set the default routing value, when introducing other routing protocols into RIP routing, when using the redistribute command to introduce other protocols routing, the default route weight is introduced specified by default-metric, if there is no

specific routing weight value.

For example：Set the default routing value is 3 when introduce other routing protocols in RIP routing

Switch(config-router-rip)#default-metric 3

Related command：redistribute

2. Command：ip rip authentication key-chain <*name-of-chain*>

no ip rip authentication key-chain

Function：Set the key used by RIP authentication；“No”operation command means cancel RIP authentication

Parameters：*<name-of-chain> character string*，not longer than 16 characters.

By default：The system do not perform RIP authentication.

Command mode：Interface configuration mode

User guide：” no operation” command is to cancel RIP authentication instead of deleting the key used in RIP authentication.

Related command：ip rip authentication

3. Command：ip rip authentiaction mode {text|md5 mode {text| md5 {value }}}

no ip rip authentication mode

Function：Set the type of authentication; the“no”operation command means restore the default authentication type, text verification.

Parameters：text means text verification；md5 meansMD5 verification.

Default: Text verification is used by default.

Command Mode: Interface Configuration Mode

Usage Guide: RIP-I does not support authentication. RIP-II supports two kinds of authentication: text verification (namely Simple verification) and datagram verification (MD5 verification).

For example: Set MD5 authentication for RIP packets on interface vlan1. Verify that the used key is 123.

switch(config-If-Vlan1)#ip rip authentication mode md5

switch(config-If-Vlan1)#ip rip authentication string 123

Related command：ip rip authentication key-chain

4. Command：default-metric <*value*>

no default-metric

Function：Set the default route weight for redistributed routes. “no” operation command means restore the value by default.

Parameters：<*value*>is the value of the route to be set. The value ranges from 1 to 16.

Default: The default route weight value is 1.

Command mode: RIP protocol configuration mode

Usage guide: Default-metric command is used to set the default routing value, when introducing other routing protocols into RIP routing, when using the redistribute command to introduce other protocols routing, the default route weight is introduced specified by default-metric, if there is no specific routing weight value.

For example：Set the default routing value is 3 when introduce other routing protocols in RIP routi

Switch(config-router-rip)#default-metric 3

Related command：redistribute

5. Command：ip rip receive version {1 | 2 | 1 2}

no ip rip receive version

Function：Set the interface to receive version information of RIP message. RIP version 1 and 2 are received by default. The “no” operation command restores the default value.

Parameters：1 and 2 respectively means RIP version 1 and RIP version 2； 1 2 means RIP version 1 and 2.

Default: The default value is 12, which means both RIP version 1 and 2.

Command mode: Interface Configuration Mode

6. Command：ip rip send version { 1 | 2 | 1 2}

no ip rip send version

Function: Setting the version of RIP massage sent by interface. “no” operation of this command is to recover the default data.

Parameter: v1 | v2 are both the version no of RIP. When configuration is sending v2 version of RIP massage, interface default will send the v2 version RIP massage by multicast way, only after closing the multicast, this interface could send broadcast massage.

Default situation: interface default send v2 version RIP massage.

Command mode: interface configuration mode

use guide: when interface configuration send v2 version RIP massage, default sending mode is multicast way, only after shut down the multicast way, this interface could send broadcast massage.

7.Command：ip split-horizon

no ip split-horizon

Function: setting allow split horizon, no operation of this command is disabling split horizon

Default situation: under default situation, allow split horizon

Command Mode: Interface Configuration Mode

Use guide:Split horizon is used to avoiding Routing Loops, it means to prevent Layer3 Ethernet Swtich broadcasts the routing through the same interface where the routing is learned from.

For example: Disabling split horizon on the vlan1 interface

Switch(config)#interface vlan1

Switch(config-If-Vlan1)#no ip split-horizon

8. Command：redistribute { static | ospf | bgp} [metric <value>]

no redistribute { static | ospf | bgp }

Function: importing the route of other routing protocol into RIP routing, no operation of this command is cancelling importing.

Parameter: static dicate introduce static route, ospf dicate introduce OSPD route,bgp dicate introduce BGP route,

<value> specified introducing route by how many routing metric, range 1-16.

Default situation: RIP default do not import other routing. If introducing other routing protocol but not assigned it's metric data,then introduce as per default-metric.

Command mode: RIP configuration mode

Use guide: adopt this command could introduce other routing as RIP own routing, in order to improve RIP function.

For example: introducing SDPF protocol routing into RIP massage, the OSPD routing metric is 5, the static metric data is 8

Switch(Config-Router-Rip)#redistribute ospf metric 5

Switch(Config-Router-Rip)#redistribute static metric 8

9. /Command：router rip

no router rip

Function: open RIP routing and access RIP configuration mode, no operation of this command command is shut down RIP protocol routing

Default situation: not running RIP routing

Command mode: global configuration mode

User Guide: this command is the switch of opening RIP routing protocol, before processing other configuration of RIP protocol, the user should open this command firstly.

For example: start RIP protocol configuration mode.

Switch(Config)#router rip

Switch(Config-Router-Rip)#

10. **Command：timer basic <*update_timer*> <*info_timer*> <*collection_timer*>**

no timer basic

Function: adjust the update,expiry and restraint time of RIP timer, no operation of this command is to recovery each parameters' default data.

Parameter: <update> time interval of sending update massage, unit:s, data range 1～2147483647; <info_timer>declare RIP routing expired time slot, unit:s,data range1～2147483647；<collection_timer>declare the time slot which could be still existed in the routing table after one routing expired, unit:s, data range 1～2147483647.

Default situation:<update> default data 30,<info_timer> default data 180,<collection_timer> default data 120

Command mode: RIP protocol configuration mode

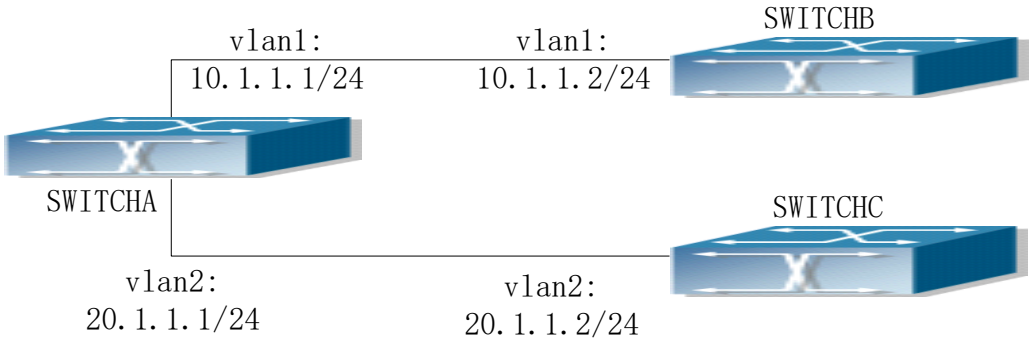
User Guide: under default situation, system will update broadcast RIP update massage every 30 seconds, system will decide the routing expired when it can not receive update massage after 180s, but this routing still could exist in routing table for 120 seconds, after 120 seconds, this routing will be deleted from routing table. When modulation all RIP timers, pls note, time for declaring RIP disabled must be longer than the time for RIP updating at least,<collection timer> time slot(which is the time from declaring RIP router disabled to deleting that router from routing table) should be longer than RIP updating time at least, and must be intergral multiple than it.

For example:

Setting RIP routing table update for 20s, declaring expired time for 80s, deleting router time is 60s.

switch(Config-Router-Rip)#timer basic 20 80 60

12.4.3 RIP configuration case



Picture 3-2 RIP Case

As showing in the picture, this is the network contributing by three layer3 Ethernet Switch, Layer 3 Switches SWITCHA,SWITCHB and SWITCHC connect with each other via vvlan1 and vlan2, these three switches run RIP protocol. Setting Layer3 SWITCHA only exchange update information with SWITCHB vlan1:10.1.1.2 via vlan1:10.1.1.1 and vlan2:20.1.1.1, not exchange Layer3 switch update information with SWITCHC vlan2:20.1.1.2.

Pls see Layer3 Ethernet Switch switcha,switchb and switchc's configuration as below:

a) Layer3 Ethernet Switch switch a：

Configuring the ip address of interface vlan1

switch#config

switch（config）#ip routing

switch(config)# interface vlan 1

switch(config-if-vlan)# ip address 10.1.1.1 255.255.255.0

！ Start rip protocol

switch(config-if-vlan)#router rip

switch (config-router-rip)#network vlan 1

switch (config-router-rip)#exit

! Configuring ip address of interface vlan2

switch(config)# interface vlan 2

switch(config-if-vlan)# ip address 20.1.1.1 255.255.255.0

！ Running rip protocol

switch(config-if-vlan)#router rip

```
switch (config-router-rip)#network vlan 2
switch (config-router-rip)#exit
```

b) Layer3 Ethernet Swich switchb

```
！Configure IP address of Interface vlan1.
switch#config
switch(config)# interface vlan 1
switch(config-if-vlan1)# ip address 10.1.1.2 255.255.255.0
！Running rip protocol, configuring ip address of neighbor Layer3 Ethernet Switch
switch(config-if-vlan)#router rip
switch (config-router-rip)#network vlan 1
switch(config-router-rip)#exit
switch(config)#exit
switch#
```

c) Layer3 Ethernet Switch switchc

```
! Configuring ip address of interface vlan2
switch#config
switch(config)# interface vlan 2
switch(config-if-vlan)# ip address 20.1.1.2 255.255.255.0
！ Running rip protocol
switch(config-if-vlan)#router rip
switch (config-router-rip)#network vlan 1
switch(config-router-rip)#exit
switch(config)#exit
switch#
```

12.5 OSPF introduction

12.5.1 Concept of OSPF

OSPF(Open shortest Path Firs) is one kind of typical Link-State protocol, is usually used in a routing domain. Routing domain means a Autonomous System, which called AS, it is a group network which have same routing policy or protocol and exchange routing information. In this AS, all OSPF router maintain a same database described AS structure,

this database keeps status information of corresponding Links,OSPF router calculate its OSPF routing table according to this database.

Considering one kind of Link-state router protocol, OSPF transmits Link State Advertisement(LSA) to all routers in one area, this point is different from Distance Vector Routing protocol. Running Distance Vector Routing protocol is that router transmits part or all of routing table to its neighbor routers.

Herebelow some basic concept of OSPF:

Hello protocol

1、 Using for finding neighbors

2、 Before being neighbors, must negociating some parameters in Hello Package successfully

3、 Impersonate role ”keepalive” between neighbors

4、 Allow bidirectional communication between neighbors

5、 Electing DR and BDR on NBMA(Nonbroadcast Multi-access) network

Neighbor and Adjacency:

1、 Neighbors are two routers which are connected to one same network segment by interface, the neighboring nodes is maintained by Hello protocol.

2、 Adjacency is the relationship elected from neighboring nodes for exchanging routing table information, not all neighboring nodes could be adjacency relationship, different type networks, different rules for building adjacency relationship. For example, in broadcast network, only routers, DR and BDR are adjacency relationship.

Router ID：

OSPF protocol used unique 32 bytes unsigned interger number which called Router ID to identify one router. Based on this purpose, each router runs OSPF need a Router ID. This Router ID need to be configurated manually usually, which always be configurated with the IP address of one interface of this router. Since IP address is unique, it is easy to keep the uniqueness of Router ID. Without configurating Router ID manually, some manufacture’s routers support electing the biggest IP address from all interfaces’ IP address automatically as Router ID.

DR and BDR：

Each broadcast network and NBMA Network ,which have two routers at least, have a Designated Router(DR) and Backup Designated Router(BDR).

1. Reducing adjacency relationships quantity, one router, which is not DR and not BDR either, only have adjacency relationship and exchange link-status information and router information with DR and BDR. This will reduce quantity of large broadcast network and quantity of adjacency relationship in NBMA network at most.

2. In the LSDB which describes topology, a NBMA network segment or broadcast segment is described by a unique LSA, this LSA is generated by DR of this network segment.

area：

OSPF support combing a group of network segments, this kind of combination is called area, which means area is a combination of a group network segments.

Area 0 is the backbone area, backbone area release the router information between the nonbackbone area, these router information are collected by ABR, and they are not detailed link-status information. To avoiding routing loops between areas, nobackbone area is not allowed release router information between area directly to each other. So all ABR have one interface belonging to Area 0, which means every area must be connected to backbone area.

Type of router:

IR: the router connected with all network segment in one area

ABR(Are Border Router): the router connected with multiple areas, ABR maintian a LSDB for each connected area.

Backbone Router: the router have one interface (or virtual connection) which is connected with backbone area at least, including all ABR and the router whose interfaces are all in backbone area.

AS Boundary Router: the router exchange routing information with the routers in other AS, this type of routers could release routing information external AS to AS. AS Boundary Router could be IR or ABR, could belong to backbone area or not.

Network type of OSPF

1、 Point to point network

Such as T1 line, is the network connected by a pair of router uniquely, on point to point network valid neighbor could built adjacency relationship, on this kind of network, OSPF package destination address is 224.0.0.5, this multicast address is called AllSPFRouters.

2、 Broadcast network

Like Ehternet Network, on this kind of network, there will be a DR and BDR, DR/BDR send OSPF package to target address 224.0.0.5, the frame send these OSPF package to target MAC address is 0100.5E00.0005, OSPF package out of DR/DBR are sent to target address 2240.0.6, this address is called AllDRouters.

3、 NBMA network

Such as X.25, Frame Relay and ATM, do not have broadcasting ability, so neighbor need to be designed manually, in order to electing DR and BDR on this type of network, OSPF package adopts unicast way.

4、 Point to Multipoint Network

This is the special configuration on NBMA network, it seems like the combination of point to point links, there's not DR or BDR on this type of network.

5、 Virtual link

OSPF package is transmitted bt unicast way. This type of network is the temporary circumvention method, if area could not connect with area 0 directly.

12.5.2 Configuration of OSPF

1. start OSPF protocol
2. configuration of OSPF protocol parameters

（1） Configuration of OSPF Router ID

（2） Configuration of routing

（3） Configuration of Area ID

（4） Configuration of timer

（5） configuration verification mode and pass code

1. start OSPF protocol

command	explanation
Global Configuration Mode	

[no] router ospf	Open OSPF protocol, “no” operation of this command is closing OSPF protocol

2. configurating OSPF protocol parameters

（1） Configurating OSPF Router ID

Command	Explanation
OSPF protocol configuration mode	
[no] router-id address <ipv4_addr>	Configuring Router ID is used to show the unique identification of this router.

（2） Configuration of router introduction

Command	Explanation
OSPF protocol configuration mode	
redistribute (babel|connected|static|rip|bgp|isis)	Setting router introduction, “no” operation of this command is restoration of default configuration.
redistribute (babel|connected|static|rip|bgp|isis) metric **no redistribute { static | ospf | bgp }**	Introducing the metric of router from static, RIP protocol, BGP and other router protocols into OSPF datagram, “no” operation is canceling the router which is introduced by corresponding protocol.

（3） Area ID Configuration

command	explanation
Interface configuration mode	
ip ospf area address <ipv4_addr>	Configuring OSPF Area ID

（4） Configurations of Timer

Command	Explanation
Interface configuration mode	

ip ospf hello-internal / dead-internal / retransmit-internal / transmit-internal	configuring hello-internal / dead-internal / retransmit-internal / transmit-internal time interval

（5） Configuration verification mode and pass code

Command	Explanation
Interface configuration mode	
1. ip ospf authentication-key 123 **2. ip ospf authentication message-digest**	Setting Verification mode: 1. For Simple authentication, and setting password is 123 2. Indicate MD5 authentication
3. ip ospf message-digest-key KEYID md5 KEY	3. Setting password character of MDS verification

12.5.3 Command introduction of OSPF configuration

1. **Command:router-id address <ipv4_addr>**

   Function: Set the router-id of indicated router equipment

   Parameters: <ipv4_addr> is the address requested to set

   Default situation: the default address is 0.0.0.0

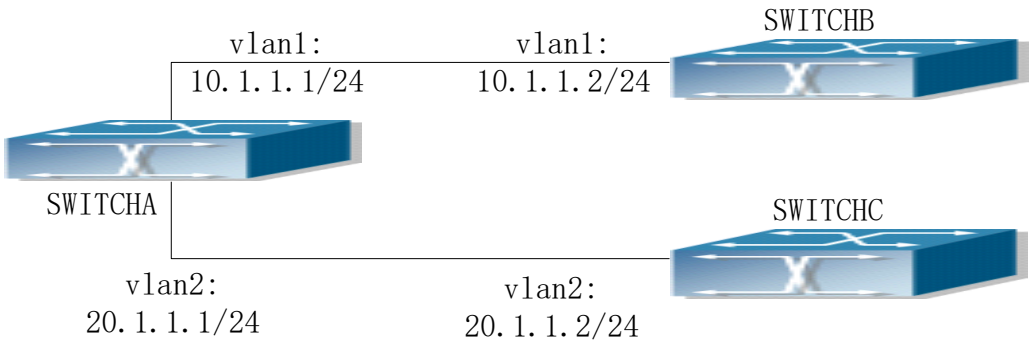
   Command mode: OSPF protocol configuration mode

   User Guide: **router-id address <ipv4_addr>** is used to indicated SOPF routing proccess ID, it is the unique identifier of router equipment.

   For example: setting the equipment address is 0.0.0.1

   Switch(config-router-ospf)# router-id address 0.0.0.1

12.5.4 OSPF configuration case



Picture 3-2 OSPF Case

The picture shows a network which is built by three layer3 switches, SWITCHA, SWITCHB and SWITCHC linked to each other through interface vlan1 and interface vlan2, all three switches run OSPF routing protocol, in order to sharing data.

Layer3 Switches, switch a, switch b, switch c, herebelow their configuration

a) Layer3 Switch switch a:

switch#config

！ Enable routing function

switch(config)#ip routing

！ Start OSPF protocol

switch(config)#router ospf

！ configuring Router ID

switch(config-router-ospf)#router-id address 0.0.0.1

switch(config-router-ospf)# exit

！ configuring the ip address of interface vlan1

switch(config)# interface vlan 1

switch(config-if-vlan)# ip address 10.1.1.1 255.255.255.0

！ configuring the ip address of interface vlan2

switch(config)# interface vlan 2

switch(config-if-vlan)# ip address 20.1.1.1 255.255.255.0

！ start ospf interface routing function

switch(config-if-vlan)#network address 10.1.1.1 netmask 255.255.255.0 area address 0.0.0.0

switch(config-if-vlan)#network address 20.1.1.1 netmask 255.255.255.0 area address 0.0.0.0

switch(config-router-ospf)#exit

b) Layer3 Switch switch b

switch#config

！Enable routing function

switch(config)#ip routing

！start OSPF protocol

switch(config)#router ospf

！ configuring Router ID

switch(config-router-ospf)#router-id address 0.0.0.2

switch(config-router-ospf)# exit

！ configuring the ips address of interface vlan1

switch(config)# interface vlan 1

switch(config-if-vlan)# ip address 10.1.1.2 255.255.255.0

！start ospf interface routing function

switch(config-if-vlan)#network address 10.1.1.2 netmask 255.255.255.0 area address 0.0.0.0

switch(config-router-ospf)#exit

c) Layer3 Switch switch c:

switch#config

！ Enable routing function

switch(config)#ip routing

！ start OSPF protocol

switch(config)#router ospf

！ configuring Router ID

switch(config-router-ospf)#router-id address 0.0.0.2

switch(config-router-ospf)# exit

！ configuring ip address of interface vlan1

switch(config)# interface vlan 2

switch(config-if-vlan)# ip address 20.1.1.2 255.255.255.0

！ start ospf interface routing function

switch(config-if-vlan)#network address 20.1.1.2 netmask 255.255.255.0 area address 0.0.0.0

switch(config-router-ospf)#exit

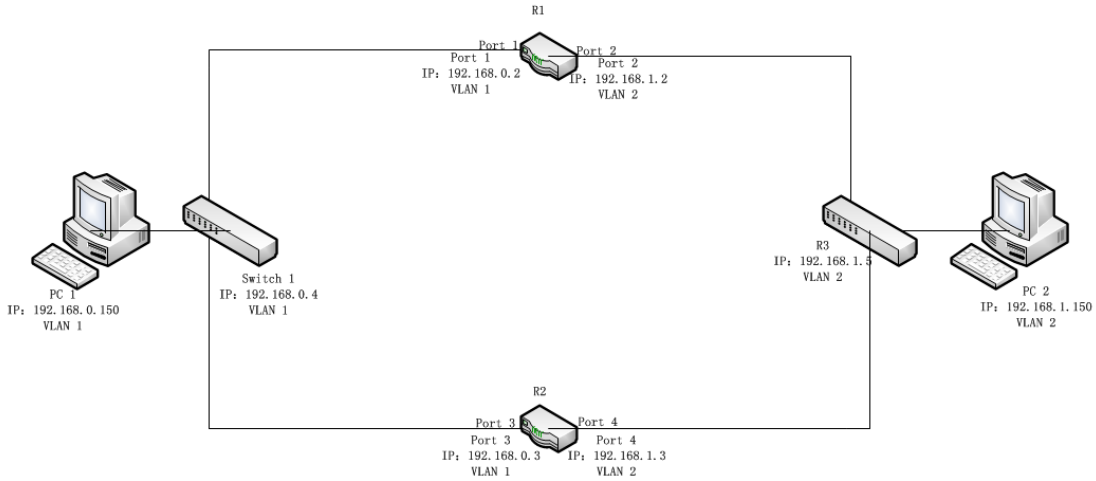
12.6 Introduction of VRRP

VRRP is one kind of error-tolerant protocol, when the next-hop router is broken, this protocol can guarantee that there is another router to replace the broken one in time, so that the communication could maintain continuity and reliability. For VRRP work, user need to configure virtual router number and virtual IP address and generate a virtual MAC address, so that a virtual router was added in the network. When the mainframe communicate with virtual router, there's no need to know the information of physical routers on this network. A virtual router is constituted by master router and several backup router, master router realize actual forwarder function. When master router is broken, a backup router will be the new master router and take over the job of broken one.

VRRP only defines one type of massage --VRRP massage, this is one kind of multicast massage, master router send this kind of massage periodically to inform its existence, using these massages also could test the parameters of virtual router, and could be used for master router electing.

VRRP defines three status mode: Initialize, Master, Backup. Only Master could serve for the forwarder request to virtual address.

12.5.1 VRRP Configuration Case



Configuring R1:R1

switch#config

！Enable routing function

switch(config)#ip routing

！Configuring the ip address of interface vlan1

switch(config)# interface vlan 1

switch(config-if-vlan)# ip address 192.168.0.2 255.255.255.0

switch(config-if-vlan)#router rip

switch (config-router-rip)#network vlan 1

switch (config-router-rip)#exit

switch(config)# interface vlan 1

！ Configuring virtual IP, using VRRP routing function

switch(config-if-vlan)# vrrp 1 ip 192.168.0.1

switch(config-if-vlan)# vrrp 1 track vlan 2

！ Configuring ip address of interface vlan2

switch(config)# interface vlan 2

switch(config-if-vlan)# ip address 192.168.1.2 255.255.255.0

switch(config-if-vlan)#router rip

switch (config-router-rip)#network vlan 2

switch (config-router-rip)#exit

switch(config)# interface vlan 2

！Configuring virtual IP, using VRRP routing function

switch(config-if-vlan)# vrrp 2 ip 192.168.1.1

switch(config-if-vlan)# vrrp 2 track vlan 1

Configuring R2:R2

switch#config

！Enable routing function

switch(config)#ip routing

！Configuring ip address of interface vlan1

switch(config)# interface vlan 1

switch(config-if-vlan)# ip address 192.168.0.3 255.255.255.0

switch(config-if-vlan)#router rip

switch (config-router-rip)#network vlan 1

switch (config-router-rip)#exit

```
switch(config)# interface vlan 1
！ Configuring vitrual IP,using VRRP routing function
switch(config-if-vlan)# vrrp 1 ip 192.168.0.1
switch(config-if-vlan)# vrrp 1 track vlan 2
！Configuring ip address of interface vlan2
switch(config)# interface vlan 2
switch(config-if-vlan)# ip address 192.168.1.3 255.255.255.0
switch(config-if-vlan)#router rip
switch (config-router-rip)#network vlan 2
switch (config-router-rip)#exit
switch(config)# interface vlan 2
！ Configuring vitrual IP, enable VRRP routing function
switch(config-if-vlan)# vrrp 2 ip 192.168.1.1
switch(config-if-vlan)# vrrp 2 track vlan 1
```