Wi-Tek L2+ Managed Switches

CIL User Manual

www.wireless-tek.com

Catalogue

Catalogue

Chapter 1 CLI Command line introduction

This chapter describes the CLI command line interface in detail, mainly including the following contents：

- Accessing the CLI of the switch
- Introduction to CLI mode
- Introduction to command syntax
- Command line shortcuts
- Historical command

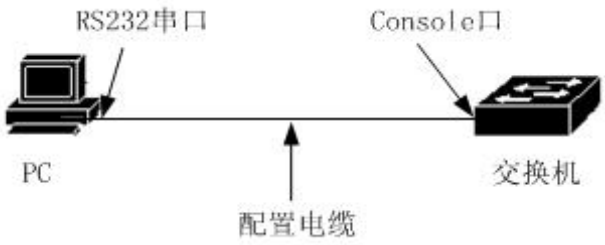
1.1 Accessing the CLI of the switch

The CLI command line interface of the switch provides an interface for users to manage the switch. Users can access the CLI command line interface of the switch through the console port and telnet terminals, which are described below。

1.1.1 Users access the CLI via Console port

The operation steps are as follows：

Step 1: connect the serial port of the PC with the console port of the switch through the configuration cable, as shown in the following figure：



Step 2: start the terminal emulator on the PC (such as windows super terminal) and configure the communication parameters of the terminal emulator. The communication parameters of the terminal are configured as follows：

Baud rate: 38400 (or 115200) (Note: subject to the actual product)

Data bit：8

Parity check： No

Stop bit：1

Data flow control： No

The communication parameter configuration of the super terminal is shown in the figure below：

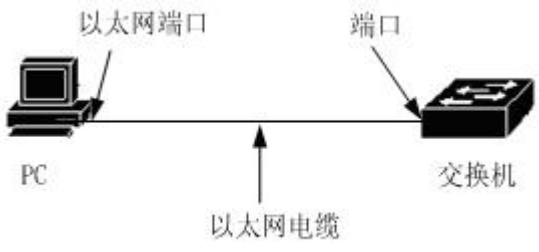
Step 3: start the switch. After the switch is started, the CLI prompt (Switch > by default) will be displayed on the terminal. Users can enter commands at this prompt, so that users can access the CLI of the switch。

1.1.2 Users access CLI via TELNET

Users can access the switch through the port of the switch。

The IP address of the port of the switch defaults to 192.168.0.1 (Note: subject to the actual product). The operation steps of accessing the switch through the port are as follows：

Step 1: connect the Ethernet port of PC and the port of switch through Ethernet cable. As shown below：



Step 2: set the IP address of the Ethernet port of the PC, which must be within 192.168.0.0/24 (such as IP address 192.168.0.100). Judge the connectivity between PC and switch by Ping 192.168.0.1。

Step 3: if the PC is connected with the switch, telnet 192.168.0.1 enters the telnet terminal interface. As shown below：

Step 4: if the system does not set a password, the telnet interface directly enters the CLI and a cli prompt appears (Switch > by default); If the system has set a password, you need to enter the password on the telnet interface before entering the CLI。

There are two points to pay special attention to：

- The IP address of the switch port is based on the VLAN layer 3 interface. Before accessing the switch, the IP address of a VLAN interface must be set. The default IP address of vlan1 is 192.168.0.1 (Note: subject to the actual product), which can be used directly. The IP address of VLAN interface can be configured through console port。
- Users can access the switch through the port. They can connect the PC and the port directly through the Ethernet cable or through a network. They only need to be able to communicate between the PC and a VLAN of the switch。

1.2 CLI Mode introduction

1.2.1 CLI Role of mode

The main functions of CLI mode are as follows：

- Facilitate the classification of users and prevent unauthorized users from illegally using cli。

Users can be divided into two levels: ordinary users and privileged users。

Ordinary users can only view some operating states of the switch and can only use display commands.

In addition to viewing the operation status of the switch, privileged users can also maintain and configure the switch and change the behavior of the switch。

- It is convenient for users to configure the switch

Switches have many configurations. If all configurations are put in one mode, it is very inconvenient for users to use them. Therefore, multiple modes are established on the CLI, and similar commands are placed in one mode, which is convenient for users to understand and use. For example, put VLAN related commands in VLAN configuration mode and interface related commands in interface configuration mode。

1.2.2 Identification of CLI mode

CLIThe CLI prompt is the identification of the CLI mode. When using the CLI, the user can know the current cli mode by looking at the CLI prompt.

The CLI prompt consists of two parts, one identifying the host and the other identifying the mode.

The host part of the CLI prompt uses the host name of the system. The host name of the system is configurable and the default is switch. Therefore, the CLI prompt starts with switch by default. The CLI descriptor mentioned later generally uses the default host name.

The mode part in the CLI prompt is not configurable. Each mode has its own corresponding mode string. Some mode strings are fixed and some mode strings are variable. For example, the mode string of VLAN configuration mode is fixed, and the mode string of interface configuration mode is variable.

For example:

The CLI prompt switch # identifies the privileged mode, switch identifies the host, and # identifies the mode.

The CLI prompt switch (config-ge1 / 1) # identifies the interface configuration mode and configures the GE1 / 1 port. Switch identifies the host and (config-ge1 / 1) # identifies the mode.

The CLI prompt switch (config-vlan2) # identifies the interface configuration mode, and the vlan2 interface is configured. Switch identifies the host and (config-vlan2) # identifies the mode.

1.2.3 Classification of CLI modes

CLI modes are divided into four categories: normal mode, privileged mode, global configuration mode and configuration sub mode, and configuration sub mode is composed of many cli modes.

Ordinary users can only access normal mode, and privileged users can access all cli modes.

The console and telnet terminals first enter the normal mode. Enter the enable command in the normal mode and enter the privileged mode after successfully verifying the password. On telnet terminal, ordinary users can only stay in normal mode and cannot enter privileged mode. Enter configure terminal in privileged mode and enter global configuration mode in cli mode. In the global configuration mode, enter relevant commands to enter each configuration sub mode。

The following table lists the main cli modes of the switch：

Mode	Description	Prompt	Command to enter mode	Exit mode command
Normal mode	Provides a display command to view the status information of the switch.	Switch>	The mode that the terminal first enters.	If there is no command to exit the mode on the console terminal, use the exit or quit command on the telnet terminal to exit the telnet terminal.
Privileged mode	In addition to providing display commands to view the status information of the switch, it also provides commands such as debugging, version upgrade and	Switch#	In addition to providing display commands to view the status information	Use the disable command to return to normal mode. Use the exit or quit command on the console

	configuration maintenance.		of the switch, it also provides commands such as debugging, version upgrade and configuration maintenance.	terminal to return to the normal mode, and use the exit or quit command on the telnet terminal to exit the telnet terminal.
whole situation mode of configuration	t provides general commands that cannot be implemented in the configuration sub mode, such as the configuration static routing command.	Switch(config)#	Enter the configure terminal command in privileged mode.	Use the exit, quit, or end command to exit to privileged mode
Interface configuration mode	Provides commands for configuring ports and VLAN interfaces。	Port： Switch(config-ge1/1)# VLAN port： Switch(config-vlan1)#	Enter the < if name > command in global configuration mode.	Use the exit or quit command to exit the global configuration mode, and use the end command to exit the privileged mode.
VLAN mode of configuratio	Provides commands for configuring VLANs. For example, commands to create and delete VLANs.	Switch(config-vlan)#	Enter in global configuration mode vlan	Use the exit or quit command to exit the global configuration mode, and use

n			database order。	the end command to exit the privileged mode.
MSTP configuration mode	Provides commands for configuring MSTP. For example, commands to create and delete MSTP instances.	Switch(config-mst)#	Enter the spaning tree MST configuration command in global configuration mode。	Use the exit or quit command to exit the global configuration mode, and use the end command to exit the privileged mode.
Terminal configuration mode	Provides commands to configure console and telnet terminals, such as the command to configure the timeout time of the terminal.	Switch(config-line)#	Enter the line vty command in global configuration mode.	Use the exit or quit command to exit the global configuration mode, and use the end command to exit the privileged mode.

1.3 Introduction to command syntax

1.3.1 Command composition

CLI commands are composed of keywords and parameters. The first word must be keywords, and the following words can be keywords or parameters. Keywords and parameters can appear alternately. A command must have keywords, but can have no parameters. For example, the command write has only one keyword and no parameters; The command show version has two keywords and no parameters; The command VLAN < VLAN ID > has a keyword and a parameter; The command instance < instance ID > VLAN < VLAN ID > has two keywords and two parameters, and the keywords and

parameters appear alternately。

1.3.2 Parameter type

The parameters of CLI commands are divided into two types: required parameters and optional parameters. When entering a command, the required parameters must be entered, while the optional parameters can be entered or not. If the parameter in the command VLAN < VLAN ID > is a required parameter, this parameter must be entered when entering the command; The parameter in the command show interface [if name] is optional. This parameter can be entered or not when entering the command。

1.3.3 Command syntax rules

When describing commands in text, the following rules must be met:

1) Keywords are directly expressed in words.

Such as the command show version.

2) Parameters must be enclosed with < >.

Such as the command VLAN < VLAN ID >

3) If it is an optional parameter, the parameter must be enclosed by [].

For example, the command show VLAN [< VLAN ID >]

In this case, the parameter < > can be omitted and changed to:

Command show VLAN [VLAN ID]

That is, the parameter VLAN ID can be entered or not.

If it is a required parameter, the parameter cannot have []。

4) If you must select one of multiple keywords or parameters, use {} to enclose multiple keywords or parameters. Multiple keywords or parameters are separated by | and a space is required before and after |

If multiple keywords are required:

spanning-tree mst link-type {point-to-point | shared}

You must choose between point to point and shared.

Command with multiple parameters required：

no arp {<ip-address> | <ip-prefix>}

Keywords and parameters are mixed. Required commands：

Show spanning-tree mst {none|instance <0-15>}ng

5) If one of the keywords or parameters can be selected, use [] to enclose the keywords or parameters. The keywords or parameters are separated by |, and a space is required before and after |。

The command is as follows：

debug ip tcp [recv | send]

The keywords recv and send can be selected or not。

show ip route [<ip-address> | <ip-prefix>]

show interface [<if-name> | switchport]

6) If there is a keyword or parameter or a group of keywords or parameters, you can select and input repeatedly, and add the symbol "*" after this (Group) keyword or parameter。

Example ping commad：

ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*

-j <count> <ip-address>* --- Multiple IP addresses can be entered repeatedly

-k <count> <ip-address>* --- Multiple IP addresses can be entered repeatedly

The entire option can also be entered repeatedly。

6) The parameter is represented by the descriptor of one or more words. If there are multiple words, separate each word with the symbol "-" and each word is lowercase。

Correct parameter representation：<vlan-id>，<if-name>，<router-id>， <count>。

Wrong parameter representation：<1-255>，<A.B.C.D>，<WORD>，<IFNAME>。

1.3.4 Command abbreviation

When the user enters a command on the CLI interface, the keyword of the command can be abbreviated. The CLI supports the prefix matching function of the command. As long as the input word uniquely matches the keyword prefix, the CLI parses the input word into a matching keyword. This is very convenient for users to use the CLI. Users can type a few characters to complete a command. For example, the show version command can only type sh ver。

1.3.5 Grammar help

Syntax help is set in the CLI command line interface, which supports the help function of commands and parameters at each level, as described below:

1) Enter directly in a cli mode? Key, the first keyword and its description of all commands in this mode will be listed on the terminal. For example, switch (config) #?.

2) Enter the first part of a command, then enter a space, and then enter? Key, all keywords or parameters of the next level and their descriptions will be listed on the terminal. For example, switch #show?.

3) Enter an incomplete keyword and enter it directly? Key, all keywords matching this input prefix and their descriptions will be listed on the terminal. For example, switch #show ver?.

4) Enter the front part of a command, then enter a space and then enter the tab key. All keywords of the next level will be listed on the terminal. If the next level is a parameter, it will not be listed.

5) After entering an incomplete keyword, enter the tab key directly. If only one keyword matches the input prefix, it will be supplemented directly. If multiple keywords match the input prefix, all matching keywords will be listed on the terminal。

1.3.6 Command line error message

If the command entered by the user fails to pass the syntax check, an error message will be displayed on the terminal. The common error messages are shown in the table below。

Error message	Error reason
Invalid input or Unrecognized command	No matching keywords were found. Incorrect parameter input. Too many keywords or parameters entered.
Incomplete command	The command input is incomplete, and there are keywords or parameters that have not been entered.
Ambiguous command	The keyword input is incomplete. There are multiple keywords matching the input prefix.

1.4 Command line shortcuts

1.4.1 Row edit shortcut

The CLI command line interface supports the function of line editing shortcut keys, which can facilitate the input and editing of CLI commands. When you enter or edit a command, you can use the line edit shortcut to speed up the input of the command. The following table lists all the row editing shortcut keys and their functions：

Shortcut key	Function
Ctrl+p or ↑ key	Previous command
Ctrl+n or↓key	Next command
Ctrl+u	Delete entire row
Ctrl+a	Mouse back to the beginning of the line
Ctrl+f or→key	Move the mouse one grid to the right
Ctrl+b or←key	Move the mouse one grid to the left
Ctrl+d	Delete the character of the mouse
Ctrl+h	Delete the previous character of the mouse
Ctrl+k	Delete all characters at the mouse and behind the cursor
Ctrl+w	Delete all characters in front of the mouse
Ctrl+e	Move the mouse to the end of the line
Ctrl+c	Interrupt without executing the command line. If the CLI is in global configuration mode or configuration sub mode, the CLI returns to privileged mode; If the CLI is in normal mode or privileged mode, the CLI mode remains unchanged, but the CLI starts a new line。
Ctrl+z	Same function as Ctrl + C。
Tab	Use this key after entering an incomplete keyword. If a keyword matches the entered prefix, supplement this keyword; If more than one keyword matches the entered prefix, all matching keywords will be listed; If there is no keyword match, the key is invalid。

Note: some console terminals↑、↓、→、←key without function。

1.4.2 Show command shortcuts

The commands starting with the show keyword are all display commands. Some display commands cannot be displayed in one screen due to many displayed contents. The terminal provides the function of split screen display. After one screen is displayed, the terminal waits for user input to determine the subsequent processing. The following table lists the display command shortcuts and their functions。

Shortcut key	Function
Space	Show next screen
Enter	Show next row
Ctrl+c	Interrupt the execution of the command and exit to cli mode.
Other key	Same function as Ctrl + C.

1.5 Historical command

The CLI command line interface supports the command history function. It can remember the 20 historical commands recently used by the user and save the commands recently typed by the user. You can use show history to display the commands you have entered, or you can use Ctrl + P, Ctrl + n or ↑, ↓ keys to select historical commands. The historical command function can facilitate users to enter commands.

Chapter 2 System management configuration

Before learning the relevant function configuration of the switch, users need to master some basic configurations of the system management and maintenance of the switch. This chapter describes the basic configurations of these system management and maintenance, mainly including the following contents：

- System security configuration
- System maintenance and commissioning
- Monitoring system
- Profile management
- Software version upgrade

1.6 System security configuration

In order to prevent illegal users from invading the switch, the system provides several system management security measures, mainly including：

- Multi user management control
- Enable Password control
- TELNET service control
- SNMP service control
- HTTP service control

1.6.1 Multi user management control

Multi user management not only ensures the security of the switch system, but also provides the ability of multiple users to manage and maintain the switch at the same time. Multi user management ensures the security of the system by giving each user a user name, password and authority. Users need to verify the user name and password when accessing the switch. They can pass the verification only when the user name and password are correct and consistent. The user can access the switch after passing the authentication, but the user's permission limits the scope of the user's access to the switch.

Multi-user management divides the permissions of users into two levels: ordinary users and privileged users. Ordinary users can only stay in the ordinary mode of CLI command line interface, and can only use the display command to query the information of the switch. Privileged users can access all modes of the CLI command line interface and use all commands provided by the CLI. They can not only query the information of the switch, but also maintain and manage the switch.

The multi-user management function is only applied to the telnet terminal and does not control the console terminal. When using the console terminal to access the switch, the user does not need to verify the user name and password, and the user can directly access the CLI. When accessing the switch through telnet terminal, the user name and password need to be verified. The CLI can be accessed only after the user name and password are verified.

The default user name and password of the switch are admin. The admin user must be an administrator, that is, a privileged user. It cannot be configured as an ordinary user, and the admin user cannot be deleted。

The commands related to multi-user management are shown in the following table：

Command	Description	CLI mode
username <user-name> password <key> {normal | privilege}	Add a user. If the specified user already exists, modify the password and permission of the user. The first parameter is the user name, the second parameter is the password, and the optional option indicates the permission, normal indicates the ordinary user, and privilege indicates the privileged user.	Global configuration mode
no username [user-name]	Delete a user with a specified user name.	Global configuration mode

show running-config	View the current system configuration, and you can view the configuration of multi-user management.	Privileged mode

1.6.2 Enable password control

Enable password is used to control the switching from normal mode to privileged mode. Before enable password authentication, users can only view the information of the switch. After enable password authentication, users may configure and maintain the switch.

The enable password is not attached to the user. Any user who logs in to the console terminal or telnet terminal must verify the enable password if he wants to enter the privileged mode. If the verification is unsuccessful, he can only stay in the normal mode.

Enter the enable command in the normal mode, and the terminal will prompt the user to enter the password. At this time, the user can enter the enable password. If the password is verified successfully, the terminal will enter the privileged mode. Otherwise, it will stay in the normal mode, and ordinary users will not enter the privileged mode regardless of whether the password is verified successfully or not.

When the command is "enable", the terminal will not enter the password in the normal mode by default.

The relevant commands of enable password are shown in the following table：

Command	Description	CLI mode
enable password <key>	Set the enable password of the system。	Global configuration mode
no enable password	Clear the enable password of the system. The enable password is empty.	Global configuration mode
show running-config	View the current system configuration, and you can view the configuration of enable password.	Global configuration mode
enable	Interactive command to	Global configuration

	verify the enable password of the system. After successful verification, the terminal enters the privileged mode.	mode

Note: for system security, the administrator needs to set the enable password of the system.

1.6.3 TELNET service control

In some cases, the administrator does not need to manage the switch remotely, but only needs to manage the switch locally through the console terminal. At this time, in order to improve the security of the system and prevent illegal users from logging in to the telnet terminal remotely, the administrator can turn off the telnet service. Telnet service is on by default.Telnet

The relevant commands of service control are as follows:

Command	Description	CLI mode
security-manage telnet enalbe	Open telnet service。	Global configuration mode
security-manage telnet disable	Close telnet service。。	Global configuration mode
security-manage telnet number <1-100>	The number parameter ranges from 1 to 100 and defaults to 5.	Global configuration mode
security-manage telnet access-group <1-99> (Note: subject to the actual product)	Specify an ACL group and turn on source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address will not be controlled。	Global configuration mode
no security-manage telnet access-group	turn off source IP address control.	Global configuration

		mode
show security-manage	You can view the configuration of service control.	Privileged mode

1.6.4 SNMP Service control

SNMP service control can turn on / off SNMP service and control the IP address of the access switch through ACL.

The relevant commands of SNMP service control are shown in the following table：

Command	Description	CLI mode
security-manage snmp enalbe	Open the SNMP service.	Global configuration mode
security-manage snmp disable	Close the SNMP service.	Global configuration mode
Security-manage snmp access-group <1-99> (Note: subject to the actual product)	Specify an ACL group and turn on source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address will not be controlled.	Global configuration mode
no security-manage snmp access-group	Turn off source IP address control.	Global configuration mode
show security-manage	You can view the configuration of service control.	Privileged mode

1.6.5 HTTP Service control

HTTP service control can turn on / off HTTP services and control the IP address of the access switch through ACL.

The commands related to HTTP service control are shown in the following table：

Command	Description	CLI mode
security-manage http enalbe	Open HTTP service。	Global configuration mode
security-manage http disable	Close HTTP service。	Global configuration mode
security-manage http access-group <1-99> (Note: subject to the actual product)	Specify an ACL group and turn on source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address will not be controlled.	Global configuration mode
no security-manage http access-group	Turn off source IP address control.	Global configuration mode
show security-manage	You can view the configuration of service control.	Privileged mode

1.6.6 HTTPS Service control

HTTPS service control can turn on / off HTTPS service and control the IP address of access switch through ACL。

The relevant commands of HTTPS service control are shown in the table below：

Command	Description	CLI mode
security-manage https enalbe	Open HTTP service。	Global configuration mode
security-manage https disable	Close HTTP service。	Global configuration mode
security-manage https access-group <1-99> (Note: subject to the actual product)	Specify an ACL group and turn on source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address will not be controlled.	Global configuration mode
no security-manage https access-group	Turn off source IP address control.	Global configuration mode
show security-manage	You can view the configuration of service control.	Privileged mode

1.6.7 SSH Service control

Traditional network service programs, such as FTP, pop and Telnet, are inherently insecure, because they transmit passwords and data in plaintext on the network. People with ulterior motives can easily intercept these passwords and data. Moreover, the security verification methods of these service programs also have their weaknesses, that is, they are vulnerable to the attack of "man-in-the-middle". The so-called "middleman" attack means that the "middleman" pretends to be a real server to receive the data you send to the server, and then pretends to be you to send the data to the real server. After the data transmission between the server and you is tampered with by the "middleman", there will be serious problems. By Using SSH, you can encrypt all the transmitted data, so

that the "man in the middle" attack can not be realized, and it can also prevent DNS spoofing and IP spoofing. Another additional advantage of Using SSH is that the transmitted data is compressed, so it can speed up the transmission speed. SSH has many functions. It can not only replace Telnet, but also provide a safe "channel" for FTP, pop and even PPP。

The commands related to SSH are shown in the following table：

Command	Description	CLI mode
security-manage ssh enalbe	Open ssh service。	Global configuration mode
security-manage ssh disable	Close ssh service。	Global configuration mode
security-manage ssh access-group <1-99>	Specify an ACL group and turn on source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address will not be controlled.	Global configuration mode
no security-manage ssh access-group	SSH turns off source IP address control.	Global configuration mode
ip sshd auth-retries < times>	Set the maximum number of verifications that the client can attempt	Global configuration mode
ip sshd silence-period < seconds>	Set the waiting time after the client exceeds the maximum number of verifications	Global configuration mode
show ip sshd	View the configuration information of sshd	Privileged mode
show security-manage	You can view the configuration of service control.	Privileged mode

1.7System maintenance and commissioning

The basic system maintenance and debugging functions mainly include the following contents：

- Configure the system clock
- Configure terminal timeout attribute
- System reset
- View system information
- Network connectivity debugging
- Traceroute debugging

1.7.1 Configure the system clock

The switch provides the function of real-time clock. You can set and view the current clock through commands. The clock of the system is internally powered to ensure the continuous operation of the real-time clock when the system is powered off. There is no need to reset the clock after the system is started.

The switch has set the clock before leaving the factory. The user does not need to set it again. If the user finds that the time is inaccurate, the user can reset the clock.

The relevant commands of the system clock are as follows:

Command	Description	CLI mode
set date-time <year> <month> <day> <hour> <minute> <second>	To set the current clock of the system, you need to enter the parameters of year, month, day, hour, minute and second.	Privileged mode
show date-time	Displays the current clock of the system.	Normal mode. privileged mode

1.7.2 Configure terminal timeout attribute

For the safety of the terminal, when the terminal has no key input, the terminal will exit after a certain time. The exit processing of the console terminal is different from that of the telnet terminal. For the console terminal, when the terminal times out, the CLI mode

returns to the normal mode. For the telnet terminal, when the terminal times out, the telnet connection is interrupted and the telnet terminal exits.

The timeout time of the terminal is 10 minutes by default. The user can also set the terminal never to timeout.

The relevant commands of terminal timeout are shown in the table below：

Command	Description	CLI mode
exec-timeout <minutes> [seconds]	Set the terminal timeout. If the parameters are all 0, it means that the terminal will never timeout.	Global configuration mode
no exec-timeout	Set the terminal timeout to return to the default, i.e. 10 minutes.	Global configuration mode
show running-config	View the current configuration of the system, and you can view the configuration of terminal timeout.	Privileged mode

1.7.3 System reset

The system provides a reset method：

- Reset the switch

The relevant commands for system reset are shown in the table below：

Command	Description	CLI Mode
reset	Reset the switch	Privileged mode

1.7.4 View system information

The system provides a wealth of display commands to view the operation status and

information of the system. Only a few commonly used display commands for system maintenance are listed here, as shown in the table below：

Command	Description	CLI mode
show version	Displays the version number of the system and the time of executing the file compilation connection.	Normal mode. privileged mode
show snmp system information	Display the basic information of the system, including how long the system has been running after startup.	Normal mode. privileged mode
show history	Displays a list of recently entered commands on the CLI command line.	Normal mode. privileged mode

1.7.5 Network connectivity debugging

In order to debug the connectivity between the switch and another device in the network, it is necessary to realize the ping command on the switch and Ping the IP address of the other party on the switch. If the switch receives the Ping response from the other party, it indicates that both ends are connected, otherwise it indicates that both ends cannot communicate.

The switch not only realizes the ping command, but also supports many options on the ping command. Users can use these options for more accurate and complex debugging.

The ping command is shown in the following table：

Command	Description	CLI mode
ping <ip-address> [-n <count> | -l <size> | -w <timeout>]*	It can be used without any options or with one or more options. Without any options, it is the simplest ping command. When the command is executed, you can type Ctrl + C to interrupt the execution of the	Privileged mode

	command.	

1.7.6 Traceroutedebugging

In order to debug which intermediate devices the switch passes through when communicating with another device in the network, it is necessary to implement the trace route command on the switch. When using the trace route command on the switch, specify the IP address of the other party, and all the paths in the middle will be displayed during the execution of the command.

The switch not only implements the trace route command, but also supports many options on the trace route command. Users can use these options for more accurate and complex debugging.

The trace route command is shown in the following table：

Command	Description	CLI mode
trace-route <ip-address> [-h <maximum-hops> | -j <count> <ip-address>* | -w <timeout>]*	It can be used without any options or with one or more options. Without any options, it is the simplest trace route command. When the command is executed, you can type Ctrl + C to interrupt the execution of the command.	Privileged mode

1.7.7 Telnet Client

The switch provides telnet client function, and users can remotely access other devices through telnet client.

Command	Description	CLI mode
telnet <ip-address>	The parameter is the IP address of the target device	Privileged mode

1.7.8 ssh Client

Series switches provide SSH client function, and users can remotely access other devices through SSH client.

Command	Description	CLI mode
ssh <ip-address> [user-name]	SSH client can access other devices remotely	Privileged mode

1.8 Profile management

There are two configurations: current configuration and initial configuration. The current configuration refers to the configuration during system operation, which is stored in the memory of the system, while the initial configuration is the configuration used during system startup, which is stored in the flash of the system, that is, the configuration file. When the user executes relevant commands, the current configuration of the system is modified. Only after executing the Save command, the current configuration is written into the initial configuration for the next startup of the system. After the system is started, the current configuration information of the system is the same as the initial configuration information without any configuration.

The current configuration and the initial configuration adopt the same format, which is the format of command line text, which is very intuitive and easy for users to read. The format of configuration file has the following characteristics：

- The configuration file is a text file.
- All saved are commands.
- Only the non default configuration is saved, and the default configuration is not saved.
- Commands are organized according to the CLI mode. Commands in the same cli mode are organized together to form a segment, with "!" between segments separate. For commands in the global configuration mode, organize the commands with the same function or similar functions into a section with "!" separate.
- For commands in configuration sub mode, there is a space before the command, while for commands in global configuration mode, there is no space before the command.
- End the configuration with "end".

Configuration file management mainly includes the following contents：

- View configuration information
- Save configuration
- Delete configuration profile
- Download from configuration file

1.8.1 View configuration information

Viewing configuration information includes viewing the current configuration and initial configuration of the system. The initial configuration is actually the configuration file in flash. When there is no configuration file in flash, the default configuration is used when the system starts. At this time, if you view the initial configuration of the system, the system will prompt that the configuration file does not exist.

The commands for viewing configuration information are shown in the following table：

Command	Description	CLI mode
show running-config	View the current configuration of the system.	Privileged mode
show startup-config	View the initial configuration of the system.	Privileged mode

1.8.2 Save configuration

When the user modifies the current configuration of the system, these configurations need to be saved to the configuration file, so that these configurations still exist after the next startup. Otherwise, these configuration information will be lost after restart. Saving the configuration is to save the current configuration to the initial configuration.

The commands to save the configuration are shown in the following table：

Command	Description	CLI mode
write	Save current configuration	Privileged mode

Note: after configuring the switch, users need to use this command to save the configuration, otherwise the configuration will be lost after system restart.

1.8.3 Delete configuration file

When users want the initial configuration of the system to return to the default configuration, they can delete the configuration file. Deleting the configuration file has no impact on the current configuration. If they want the current configuration of the system to return to the default configuration, they need to restart the switch. Users must be careful when deleting the configuration file, otherwise the configuration will be lost.

The commands to delete the configuration file are shown in the following table

Command	description	CLI mode
delete startup-config	Delete configuration file。	Privileged mode

1.8.4 Download from configuration file

For the security of the configuration file, the user can use the command to upload the configuration file to the PC for backup. When the system configuration is abnormally lost or wants to return to the original configuration after modification, the original configuration file can be downloaded from the PC to the switch. After downloading the configuration file, it has no impact on the current configuration of the system, The configuration will take effect after the switch is restarted. You can also upload and download configuration files through the web. For specific operations, please refer to the web operation manual.

The commands downloaded from the configuration file are as follows：

Command	description	CLI mode
upload configure <ip-address> <file-name>	Upload the configuration file to the PC. the first parameter is the IP address of the PC, and the second parameter is the file name of the configuration file stored on the PC.	Privileged mode
download configure <ip-address> <file-name>	Download the configuration file to the PC. the first parameter is the IP address of the PC, and the second	Privileged mode

	parameter is the file name of the configuration file stored on the PC.	

Download the configuration file and use the TFTP protocol. Run the TFTP client software on the switch and the TFTP server software on the PC. The steps for downloading the configuration file are as follows：

Step 1: build a network environment.

Step 2: store the TFTP software configuration file on the PC.

Step 3: save the configuration on the switch.

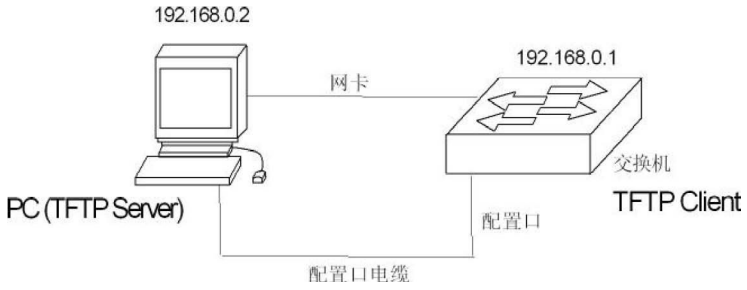
Step 4: execute the configuration file upload command on the switch to back up the configuration file to the PC.

Step 5: when the switch needs the configuration file on the PC, execute the configuration file download command on the switch to download the configuration file on the PC to the switch.

Step 6: to make the configuration effective, you must restart the switch。

Example: for a switch that has been configured with VLAN and interface address, you need to upload and download the configuration file.

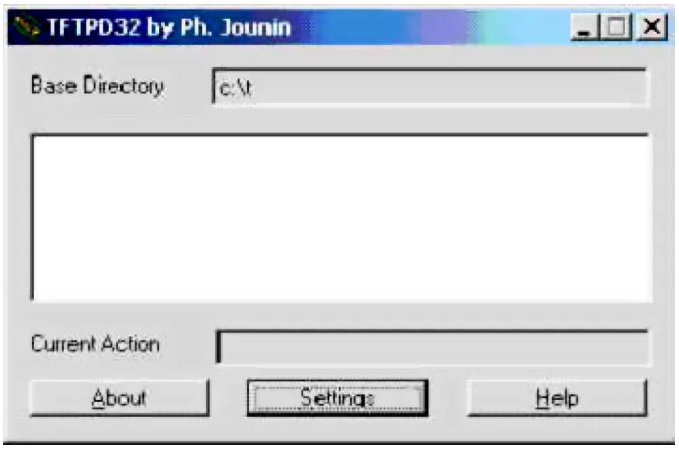
Step 1: build the following network environment。



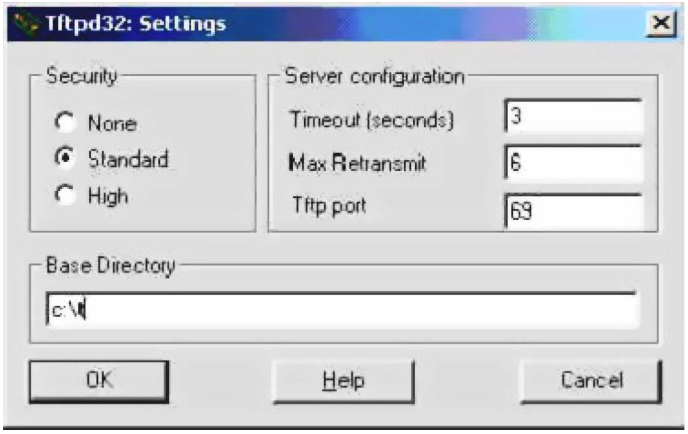
Connect the configuration port of the switch to a configuration terminal through cable and connect it to a PC through network cable. Install TFTP server on the PC and configure the IP address of the Ethernet port of the PC. here, it is assumed that the IP address of the PC is 192 168.0.2 。 Then, configure the IP address of the switch. Here, it is assumed that the IP address of the switch is 192.168 0 1. Ensure the connectivity between PC and switch

Step 2: start TFTP server and configure TFTP server parameters.

Run TFTP server, and the window interface is shown in the figure below：



Then, set the directory of the backup configuration file. Specifically, click the [settings] button to set the interface, as shown in the following figure：



Enter the file path in base directory. Click the [OK] button to confirm.

Step 3: execute the write command on the switch and save the current configuration to the configuration file.

Step 4: back up the file to the PC and execute the command switch#upload configuration 192.168.0.2 Beifen cfg。

Step 5: if necessary, download the backup file to the switch and execute the command switch#download configuration 192.168.0.2 Beifen cfg。

Step 6: if you want the downloaded configuration file to take effect, you must restart the switch and execute the command switch#reset.

1.9 Software version upgrade

The switch supports online upgrade of software version. The upgrade is done through the TFTP tool.

1.9.1 Software version upgrade command

Upgrade the switch file of the switch in the global configuration mode. The command is as follows:

download switch <ip-address> <file-name>

Where < IP address > is the IP address of the PC running the TFTP server and < file name > is the name of the switch file saved on the TFTP server.

Upgrade the kernel file of the switch in the global configuration mode. The command is as follows:

download kernel <ip-address> <file-name>

Where < IP address > is the IP address of the PC running the TFTP server and < file name > is the name of the kernel file saved on the TFTP server.

Upgrade the patch file of the switch in the global configuration mode. The command is as follows:

download patch <ip-address> <file-name>

Where < IP address > is the IP address of the PC running the TFTP server and < file name > is the name of the patch file saved on the TFTP server.

Upgrade the uboot file of the switch in the global configuration mode. The command is as follows:

download uboot <ip-address> <file-name>

Where < IP address > is the IP address of the PC running the TFTP server and < file name > is the uboot file name saved on the TFTP server.

During the upgrade process, the power cannot be cut off, otherwise the file of the switch may be damaged and the switch cannot be started. After downloading, you need to restart the switch to run the newly downloaded corresponding file program. The whole upgrade process will take a few minutes. Please wait patiently.

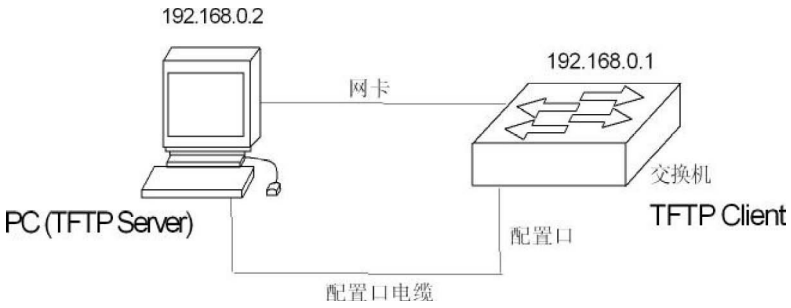
The software version can also be upgraded through the web. For specific operations, please refer to the web operation manual.

1.9.2 Software upgrade process

The steps to upgrade switch and other files are as follows:

Step 1: build an upgrade environment. As shown in the figure

Below.

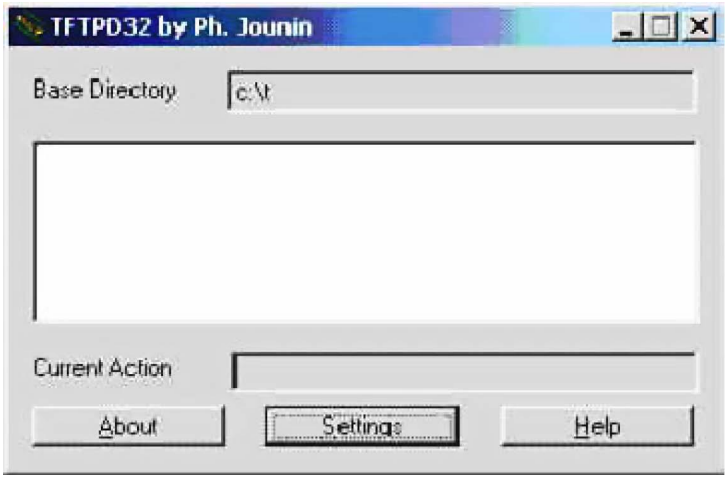


The construction process is as follows:：

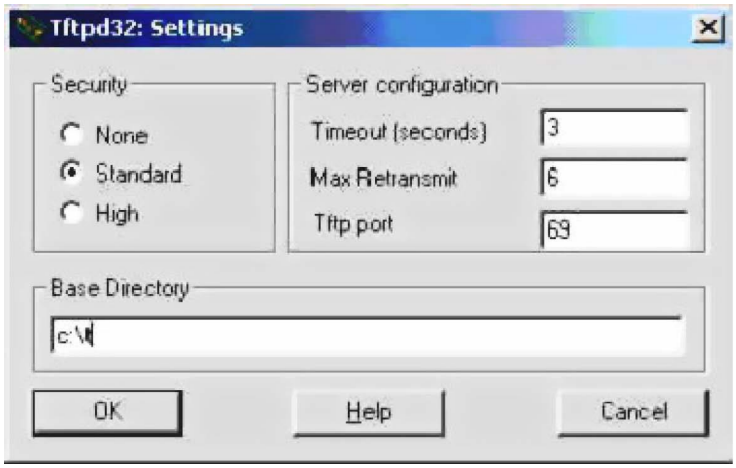
- Connect the console port of the switch to a configuration terminal (PC) through the cable.
- Install TFTP server on PC.
- Copy the new switch and other files to a path on the PC. here, it is assumed that the path is C: \ T;
- Configure the IP address of the Ethernet port of the PC. here, it is assumed that the IP address of the PC is 192.168.0.2.
- Configure the IP address of the switch. Here, it is assumed that the IP address of the switch is 192.168.0.1.

Step 2: run TFTP server and configure TFTP server.

First: run TFTP server. The tftpd32 window interface is shown in the following figure:



Then: set the TFTP server file directory. After starting the TFTP server, reset the TFTP server file directory and copy the switch and other files to be loaded into this directory. Specifically, click the [settings] button to open the tftpd32 setting interface, as shown in the following figure



Enter the file path in base directory. Click the [OK] button to confirm.

Step 3: upgrade the file.

First: connect the port of the switch with the PC running TFTP server program through Ethernet cable. The ping command is used to detect whether the host is connected with the switch.

Then: enter the command at the HyperTerminal switch# prompt:

Switch# download switch 192.168.0.2 switch.img，Press enter and wait for the upgrade file to complete.

Software is updating. Please wait and down’t powerdown!

……

Updating is completed. Do you wish to reset?[Y/N]

After the file transfer is completed, the system will prompt you whether you need to restart the switch; Generally, we suggest you choose "Y" to restart the switch, because the system upgrade can only take effect after restart; If your configuration file is not saved, you can select 'n' first and do not restart first; Restart the switch after completing other operations such as saving disk.Switch#

Note

交换机升级过程中，不能断电。

Step 4: restart the switch.Switch# reset

Configure port

This chapter introduces port related configurations, mainly including the following contents:

- General configuration of ports
  - Configure
  - Configure TORM-CONTROL
  - Configure LOW-CONTROL
- Configure port bandwidth
  - Configure truck

1.10 General configuration of ports

The administrator controls the users accessed under the port by configuring the port of the switch. If the users under the port are not allowed to access the network, the administrator can close this port. This section introduces the general configuration of ports, mainly including：

- Opening and closing of ports
- Port rate configuration
- Display port information

1.10.1 Opening and closing of ports

The port of the switch is open by default. If the administrator wants users under the port not to access the network, he can close this port.

The following command opens the management status of the port in the interface configuration mode:

no shutdown

For example, open the management status of port GE1 / 1

Switch(config-ge1/1)#no shutdown

The following command turns off the management state of the port in the interface configuration mode:

Shutdown

For example, close the management status of port GE1 / 1:

Switch(config-ge1/1)#shutdown

1.10.2 Port rate configuration

The default rate configuration of all ports is adaptive.

The following command configures the port rate in interface configuration mode：

speed {autonegotiate |full-1000 |full-100 |full-10 |half-100 |half-10 }

autonegotiate--- self-adaption

full-1000------- Full duplex Gigabit

full-100-------- Full duplex 100M

full-10 -------- Full duplex 10M

half-100-------- Half duplex 100M

half-10--------- Half duplex 10M

For example, the rate of port 1 / 1 is configured as full duplex 100M:

Switch(config-ge1/1)# speed full-100

1.10.3 Display port information

The following command displays information about one or more ports in normal mode or privileged mode:

show interface [if-name]

For example, display the information of port GE1 / 1:

Switch# show interface ge1/1

For example, display information for all ports：

Switch# show interface

1.11 Cofigure mirror

Port mirroring is a very useful function for monitoring the traffic of packets received and sent by one or more ports. It can use the mirrored port to monitor the packets received and sent by one or more ports. The switch supports port mirroring. The mirrored port can monitor the incoming data and outgoing data of other ports. A mirror port can listen to multiple ports at the same time. This section focuses on the configuration of

mirror, mainly including the following contents：

- Configure the listening port and monitored port of mirror
- Show mirror configuration

1.11.1 Configure the listening port and monitored port of mirror

When configuring the listening port, the administrator needs to enter this interface configuration mode to set the monitored port. For example, to set port GE1 / 1 and listening port GE1 / 2, enter port GE1 / 1 and type the command：

Switch(config-ge1/1)# mirror interface ge1/2 direction both

At this time, port GE1 / 1 is set as the listening port and GE1 / 2 is set as the listening port.

The commands for setting the monitored port are as follows：

Switch(config-ge1/1)#mirror interface <if-name> direction {both | receive | transmit}

At this time, port GE1 / 1 is set as the listening port, < if name > is set as the monitored port, and the following {both | receive | transmit} indicates the direction of monitoring: receive means to monitor the received data packet; Transmit monitors the transmitted data packets; Both monitors all packets sent and received. such as：

Switch(config-ge1/1)#mirror interface ge1/2 direction both

Indicates that port GE1 / 1 is set to listen for packets sent and received by port GE1 / 2.

If you want to set multiple monitored ports, you need to execute multiple commands.

In the interface configuration mode, the administrator can cancel the monitored port. The commands are as follows：

Switch(config-ge1/1)#no mirror interface <if-name>

At this time, < if name > is the port that is no longer monitored. such as：

Switch(config-ge1/1)# no mirror interface ge1/2

It indicates that setting port GE1 / 1 will no longer listen to the packets of port GE1 / 2.

When all monitored ports are cancelled, the monitored port will also be cleared。

1.11.2 Displays the configuration of mirror

The administrator can view the set mirror configuration through the following command in normal mode or privileged mode：

Switch# show mirror

Attention should be paid to the following points：

- One port cannot be set as both listening port and monitored port。
- There can only be one listening port, but there can be multiple listening ports.

1.12 Configure storm-control

In real life, a NIC card can send high-speed unicast, multicast and broadcast packets, which can cause network failure. In this case, the suppression function on the switch is particularly important. It can prevent data packets from flooding into the network and causing network congestion. All ports of the switch support the suppression function of broadcast packets, multicast packets and DLF packets.

This section describes the configuration of storm-control in detail, mainly including the following contents：

- Default configuration
- Broadcast suppression configuration
- Multicast suppression configuration
- DLF suppression configuration
- Displays the storm-control configuration

1.12.1 Default configuration

The switch supports setting broadcast, multicast and DLF switches for each port. The three settings share the same rate limit. The broadcast packet suppression on the default port is turned on, and the suppression rate is 64K. The purpose is to prevent the network from forming a broadcast storm. DLF packets and multicast packets are not suppressed by default。

1.12.2 Broadcast suppression configuration

The following commands configure the broadcast suppression of this port in the interface configuration mode:

storm-control broadcast

The following command cancels the configuration of broadcast suppression of this port in interface configuration mode:

no storm-control broadcast

1.12.3 Multicast suppression configuration

The following command configures the multicast suppression of this port in the interface configuration mode：

storm-control multicast

The following command cancels the multicast suppression configuration of this port in the interface configuration mode：

no storm-control multicast

1.12.4 DLF suppression configuration

The following command configures DLF suppression for this port in interface configuration mode：

storm-control dlf

The following command cancels the configuration of DLF suppression for this port in interface configuration mode：

no storm-control dlf

1.12.5 Suppression rate configuration

The following command configures the suppression rate of this port in interface configuration mode：

storm-control ratelimit <1-1024000>

1.12.6 Displays the storm-control configuration

The following command displays the storm-control configuration in normal mode or privileged mode：

show storm-control

1.13 Configure storm-constraint

The port traffic threshold control function is used to control the message storm on the Ethernet. The port with this function enabled will regularly detect the unicast message traffic, multicast message traffic and broadcast message traffic arriving at the port. If a certain type of message traffic exceeds the preset upper limit threshold, the user can decide whether to block or close the port through configuration, and whether to record log information.

When the flow of a certain type of message exceeds the preset upper limit threshold of this type of message, the system provides two processing methods:

(1) Block mode: if the traffic of unicast, multicast or broadcast messages on the port is greater than the upper threshold, the port will suspend forwarding messages, and the port is blocked, but the port still counts the traffic of such messages. When the traffic of this kind of message is less than the preset lower threshold, the port will resume forwarding the message.

(2) Shutdown mode: if the unicast, multicast or broadcast message traffic on the port is greater than the upper threshold, the port will be closed and the system will stop forwarding all messages. You can restore the port state by executing the no shutdown command or by canceling the port traffic threshold configuration.

Note: for a certain type of message traffic, it can be suppressed through this function or the storm suppression function of Ethernet port, but these two functions cannot be configured at the same time, otherwise the suppression effect is uncertain. For example, the unicast message flow threshold control function and unicast storm suppression function of the port cannot be configured at the same time.

CLI configuration commands are as follows：

Command	Description	CLI mode
storm-constrain (broadcast|multicast|unicast)	Storm control of broadcast, multicast or	Interface configuration

min-rate <1-1488100> max-rate <1-1488100>	unknown unicast messages under the interface	mode
no storm-constrain (broadcast|multicast|unicast|all)	Cancel storm control	Interface configuration mode
storm-constrain action (block|shutdown)	Configure the action of storm control. By default, the message will not be storm controlled	Interface configuration mode
no storm-constrain action	Cancel the configured storm control action	Interface configuration mode
storm-constrain enable (trap)	Turn on the switch for logging during storm control	Interface configuration mode
no storm-constrain enable (log)	Turn off the switch for logging during storm control	Interface configuration mode
storm-constrain interval <6-180>	Configure the detection interval of storm control. By default, the detection interval of storm control is 5 seconds	Interface configuration mode
no storm-constrain interval	Restore the detection interval of storm control to the default value	Interface configuration mode
no storm-constrain	Delete the storm control function of the interface	Interface configuration mode
show storm-constrain	View storm control information for all interfaces	Privileged mode
show storm-constrain interface IFNAME	View the storm control information of the interface	Privileged mode

Configuration description：

(1) View the storm control information description table of the interface

	Description
interface	Interface name
type	Message type (1) broadcast broadcast message; (2) Multicast multicast message; (3) Unicast unicast message
rate	Min - low threshold; Max high threshold
action	Actions of storm control, including (1) block blocking message; (2) Shutdown - close the interface
punish-status	Message status of the current interface, including (1) block - when the rate is greater than max rate and the storm control action is blocking message, the status is blocking message; (2) Normal - normal forwarding; (3) Shutdown - when the rate is greater than max rate and the storm control action is to close the interface, the status is to close the interface
log	Log switch status, on / off
interval	The detection interval of storm control. The unit is seconds. The default value is 5 seconds
last-punish-time	Time for the final implementation of the storm control penalty

(2) By executing the storm - constraint action command to configure the action of storm control and the storm - constraint command to configure the high and low threshold of storm control, the storm message can be controlled to prevent flooding. During the storm control detection interval, when the average rate of receiving broadcast, multicast or unicast messages on the interface is greater than the specified high threshold, the storm control will block the message or close the interface according to the configured action. When the storm control action is blocking message, if the flow is lower than the minimum threshold, the interface will return to the normal forwarding state; When the storm control action is to close the interface, the interface cannot be recovered automatically. You need to manually execute the no shutdown command to recover. You can recover by canceling the configuration of port storm control shutdown action。

(3) The port traffic exceeds the upper threshold or falls back from the upper threshold to the lower threshold. Log / trap information is output

1.14 Configure flow-control

Flow-control is used to prevent packet loss when the port is blocked. In half duplex mode, flow control is realized by back pressure technology, which makes the information source reduce the transmission rate. In full duplex mode, flow control complies with ieee802.1 3x standard, the blocking port sends a "pause" packet to the information source to suspend sending.

This section describes the configuration of flow-control in detail, mainly including the following contents：

- Default configuration
- Set port flow control
- Close port flow control
- Display flow control information

1.14.1 Default configuration

The switch supports setting the flow control of sending and receiving for each port. The default port does not turn on the flow control function。

1.14.2 Set port flow control

The following command configures port flow control on in interface configuration mode：

flowcontrol

1.14.3 Close port flow control

The following command closes the flow control on the sending and receiving side of the port in the interface configuration mode：

no flowcontrol

1.14.4 Display flow control information

The following command displays the flow control information of all ports in normal mode or privileged mode：

show flowcontrol

The following command displays the flow control information of a port in normal mode or privileged mode：

show flowcontrol interface <if-name>

Where, < if name > is the name of the port to query the flow control information.

1.15 Configure port bandwidth

Port bandwidth control is used to control the sending and receiving rate of the port.

This section describes the configuration of port bandwidth in detail, mainly including the following contents：

- Default configuration
- Set the port sending or receiving bandwidth control
- Cancel port send or receive bandwidth control
- Displays the bandwidth control of the port configuration

1.15.1 Default configuration

The switch supports setting the sending and receiving bandwidth for each port. The default port has no bandwidth control.。

1.15.2 Set the port sending or receiving bandwidth control

The following commands set the port sending or receiving bandwidth control in the interface configuration mode:

portrate {egress | ingress} <rate>

Egress means to control the bandwidth of the transmitted packets.

Ingress means to control the bandwidth of received packets.

< rate > indicates the value of the bandwidth to be set. The range is 1-1024000, and the unit is kbits.

1.15.3 Cancel port send or receive bandwidth control

The following command cancels the bandwidth control of the port in the interface configuration mode:

no portrate {egress | ingress}

Egress means to cancel the bandwidth control of sending packets.

Inress means to cancel the bandwidth control of receiving packets.

1.15.4 Displays the bandwidth control of the port configuration

The following command is used to view the bandwidth control of port configuration in normal mode or privileged mode:

show portrate interface <if-name>

Where < if name > is the name of the port to query bandwidth control information.

1.16 Configure trunk

Trunk aggregates multiple ports into one logical port. It can be used to increase bandwidth, provide redundant backup connections, and load balancing. When trunk group is used as the output logical port, the switch will select a port from the port group to send the packet according to the aggregation policy set by the user. The port and aggregation strategy of trunk group are configured by software, but the forwarding of data flow is completed by hardware.

All ports in trunk group must be configured at the same speed and in full duplex mode. The switch can support up to 32 groups of trunk and up to 8 trunk members in each group. It should be noted that each port can only belong to one trunk group.

LACP is a protocol based on IEEE802 3aD standard protocol. LACP protocol interacts with the opposite end through lacpdu (link aggregation control protocol data unit).

The interface in the aggregation group enables LACP protocol. The interface will notify the opposite end of its own system LACP protocol priority, system Mac, LACP protocol priority of port, port number and operation key by sending lacpdu. After receiving the lacpdu, the opposite end compares the information in it with the information received by other interfaces to select the interface that can be in the selected state, so that both parties can reach an agreement on the interface in the selected state.

Operation key is a configuration combination automatically generated by aggregation control according to some configurations of member ports during link aggregation, including port rate, duplex mode, up / down status, VLAN allowed on the port, default VLAN ID of the port, link type of the port (i.e. trunk, hybrid, access type), etc. In the aggregation group, the member ports in the selected state have the same operation key.

This section describes the trunk configuration in detail, mainly including the following contents：

- LACPP protocol configuration
- TRUNK Group configuration
- TRUNK Member port configuration
- TRUNK Load balancing policy configuration
- TRUNK Display

1.16.1 LACP protocol configuration

Command	Description	CLI mode
lacp system-priority <1-65535>	Set LACP system priority	Global configuration mode
no lacp system-priority	Restore system priority defaults 32768	Global configuration mode
lacp max-active-link-number <1-8>	Set the upper limit of LACP activation aggregation port	Global configuration mode
no lacp max-active-link-number	Restore LACP activation aggregate port default upper limit 8	Global configuration mode
lacp port-priority <1-65535>	Set LACP port priority	Interface configuration mode
no lacp port-priority	Restore port priority defaults 32768	Interface configuration mode
lacp timeout (short|long)	Set LACP port timeout,	Interface

	missing governor timeout	configuration mode
show lacp summary	Displays a simple overview of all LACP aggregations	Privileged mode
show lacp detail	Displays all LACP aggregations	Privileged mode
show lacp <1-8>	Display LACP aggregation details	Privileged mode
show lacp port IFNAME	Displays the details of the LACP port	Privileged mode
show lacp system-id	Display LACP system status	Privileged mode
show lacp counter <1-8>	Displays the statistics of LACP aggregation ports	Privileged mode
show lacp counter	Display statistics of all LACP aggregation ports	Privileged mode
clear lacp <1-8> counters	Clear the statistics of LACP aggregation port	Privileged mode
clear lacp counters	Clear statistics of all LACP aggregation ports	Privileged mode

1.16.2 TRUNK Group configuration

The following command creates a manual trunk group in global configuration mode:
trunk <trunk-id>
Create a trunk group. The < trunk ID > value range is 1-32, indicating the ID number of the trunk group to be created. Up to 8 groups of trunk can be configured; After successful creation, the interface name of the trunk group is trunk + ID number. For example, the interface name of the trunk group with group ID number 1 is trunk 1. You can use the command "interface trunk + ID number" to enter the interface configuration mode in the configuration mode, and then operate the trunk group. For example, use the command interface trunk 1 to enter the interface mode of trunk 1 and configure trunk 1。

The following command creates a static LACP trunk group in global configuration mode:

trunk <1-32> dynamic

The following command deletes a trunk group in global configuration mode:

no trunk <trunk-id>

When deleting a trunk group, you must ensure that the trunk group has no member ports。

1.16.3 TRUNK Member port configuration

The following command adds a trunk group member port in the interface configuration mode:

trunk interface IFNAME (passive|)

< if name > is the name of the port to be added to the trunk group. It must be a layer-2 interface. Each group of trunk can add up to 8 layer-2 interfaces. If the trunk group is a static LACP trunk group, the added interface defaults to the active state or can be configured to the passive state.

The following command deletes all member ports of the trunk group in the interface configuration mode:

no trunk interface

The following command deletes the specified trunk group member port in interface configuration mode:

no trunk interface <if-name>

You can use this command multiple times to delete multiple member ports of the trunk group。

1.16.4 TRUNK Load balancing policy configuration

The following command sets trunk's load balancing policy in interface configuration mode:

trunk load-balance {dst-mac | dst-ip | src-dst-mac | src-dst-ip | src-mac | src-ip}

DST MAC ------- equalization strategy based on destination MAC

DST IP ---------- balancing strategy based on destination IP

SRC DST MAC ---- equalization strategy based on source MAC and destination MAC

SRC DST IP ---- the balancing strategy based on source IP and destination IP

SRC MAC -------- source MAC based equalization strategy

SRC IP ---------- source IP based equalization strategy

The following command sets the default trunk load balancing policy in the interface configuration mode:

no trunk load-balance

Mac SRC MAC port is the default load balancing policy based on MAC source port.

1.16.5 TRUNK Display

The following commands view all trunk group configurations in normal mode or privileged mode:

show trunk

The following command views the configuration of the specified trunk group in normal mode or privileged mode:

show trunk <trunk-id>

Where < trunk ID > is the ID number of the trunk group to be queried.。

1.17 Configure extra large frames

1.17.1 Introduction to super large frame

In order to realize that the port can receive super large frames, the port can be set to support specific super large frame length.

1.17.2 Configure extra large frames

Configure the port to support super large frame length. In config mode, enter the port configuration mode, such as interface GE1 / 1, and execute the following commands:

Switch(config-ge1/1)#jumbo frame 2000

Displays the extra large frame length supported by the port

Switch#show jumbo frame ge1/1

Port	Jumbo frame(bytes)
ge1/1	2000

1.18 Configure redundant ports

In some special cases, for example, it is necessary to focus on ensuring the stability of some servers linked to the network. The redundant port of the switch can provide two ports to link to the server, and ensure that there is only one link up port linked to the network at one time. When one port is linked down, the system will immediately enable the other port.

When a port is in link up in the redundant port group, we call it active; Conversely, if a port is in link down in a redundant port group, we call it disable.

This section focuses on the configuration of redundant ports, mainly including the following contents：

- Configuration of redundant ports
- Display of redundant ports

1.18.1 Configuration of redundant ports

The switch can be configured with 8 groups of redundant ports, and one group of redundant ports can only be configured with 2 ports; A port can only be configured into one redundant port group.

A redundant port group can be configured with a primary port and a secondary port. When configuring and enabling redundant port groups:

1. When the two ports are in the link up state at the same time, the primary port will be set to the active state and the secondary port will be set to the disable state;

2. If only one port is in the link up state, set the current link up port to the active state and the other port to the disable state;

3. Otherwise, both ports are in the disable state.

If a link down event occurs on a port in the active state, another port will be tried to set to the active state.

Another configuration parameter is force switch. When the secondary port is active and the primary port is disabled, if a link up event occurs on the primary port, decide whether to switch back to the active primary port and the disabled secondary port. If force switch is configured as enable, the switch will be forced. Otherwise, the port state of the original redundant port group will be retained.

Command	Description	CLI mode

redundant-port <1-8> primary-port IFNAME secondary-port IFNAME [force-switch]	Configure a set of redundant ports < 1-8 > is the group number Primary port ifname is the name of the primary port interface, Secondary port ifname is the name of the alternate port interface, Whether force switch is enabled	Global configuration mode
redundant-port <1-8> force-switch	Enable the forced switch of redundant ports.	Global configuration mode
no redundant-port <1-8>	Delete redundant port group.	Global configuration mode
no redundant-port <1-8> force-switch	Turn off the forced switch of the redundant port.	Global configuration mode

1.18.2 Display of redundant ports

Display of redundant ports

Command	Description	CLI mode
show redundant-port	Displays the configuration of all redundant port groups in the system	Privileged mode

1.19 UDLD configuration

UDLD (unidirectional link detection): it is a layer-2 protocol used to monitor the physical configuration of Ethernet links connected by optical fiber or twisted pair. UDLD can detect this situation when unidirectional links occur (only in one direction, for example, I can send data to you and you can receive it, but I can't receive the data you send to me), Close the corresponding interface and send a warning message. Unidirectional links may cause many problems, especially spanning trees, which may cause loopback. Note: UDLD needs the support of devices at both ends of the link to operate normally.

UDLD supports two working modes; Normal mode (default) and aggressive mode.

Normal mode: in other words, normal mode will shut down a port only if it can explicitly determine that the associated link is fault for an extended period of time

Aggressive mode: in this mode, UDLD can detect by unidirectional link. It will try to rebuild the link and send UDLD messages for 8 seconds. If there is no UDLD echo response, the port will be placed in errdisable state。

Command	Description	CLI mode
udld enable	Global enable UDLD function	Global configuration mode
udld message time <time>	UDLD message sending interval	Global configuration mode
udld port	Port enable UDLD	Interface configuration mode
udld aggressive	Enable port radical mode, default normal mode	Interface configuration mode
show udld <ifname>	View port UDLD information	Privileged mode

1.20 Configure LLDP

At present, there are more and more kinds of network devices and their configurations are complex. In order to enable the devices of different manufacturers to find and interact with each other's system and configuration information in the network, a standard information exchange platform is needed.

Lldp (Link Layer Discovery Protocol) came into being under this background. It provides a standard link layer discovery method, which can organize the main capabilities, management address, device identification, interface identification and other information of local devices into different TLV (type / length / value), It is encapsulated in lldpdu (Link Layer Discovery Protocol Data Unit) and released to its directly connected neighbors. After receiving these information, the neighbors save them in the form of standard MIB (management information base) for the network management system to query and judge the communication status of the link..

This section focuses on the configuration of lldp, mainly including the following contents:

- LLDP configuration
- LLDP dispaly

1.20.1 LLDP configuration

There are four working modes of lldp port:

TXRX: send and receive lldp message.

TX: only send but not receive lldp message.

Rx: only receive but not send lldp message.

Disable: neither send nor receive lldp message.

When the lldp working mode of the port changes, the port will initialize the protocol state machine. In order to avoid the frequent change of port working mode leading to the continuous initialization operation of the port, the port initialization delay time can be configured. When the port working mode changes, the initialization operation can be delayed for a period of time。

Command	Description	CLI mode
lldp global enable	Lldp global enable command	Global configuration mode
lldp hold-multiplier <num>	Lldp TTL multiple.	Global configuration mode
lldp timer [<reinit-delay><time>][< tx-delay><time>][< tx-interval ><time>]	Configure lldp various timers.	Global configuration mode
lldp enable	Enable interface lldp	Interface configuration mode
lldp admin-status{ disable| rx|tx|rxtx}	Configure lldp port working mode.	Interface configuration mode
lldp check-change-interval <time>	Configure refresh interface information interval	Interface configuration mode
lldp management-address <A.B.C.D>	Configure lldp management address of interface	Interface configuration

		mode
lldp tlv-enable{ dot1-tlv| dot3-tlv|med-tlv }	Configure interface lldp extension capability set switch	Interface configuration mode

1.20.2 LLDP display

LLDP command

Command	Description	CLI mode
show lldp configuration [ifname]	Display lldp configuration information	Privileged mode
show lldp local-information [ifname]	Display lldp local information	Privileged mode
show lldp neighbor-information [ifname]	Display lldp neighbor information	Privileged mode
show lldp statistics [ifname]	Display lldp message statistics	Privileged mode
show lldp status [ifname]	Display lldp status information	Privileged mode

Configure port based security

This chapter introduces the port based MAC security configuration, mainly including the following contents:

- Introduction
- MAC Binding configuration
- MAC Filter configuration
- Port learning restriction configuration
- Protection port configuration

1.21 Introduction

Port based MAC security can provide four functions: MAC binding, MAC filtering, port learning control and port protection to improve the security performance of layer 2 forwarding of the switch.

Mac binding can bind Mac and port together, and restrict a specified MAC address to access the network only on a specified port; At the same time, this port can only allow these bound MAC addresses to access the network; One port can bind multiple MAC addresses at the same time. Mac binding can be applied to a specified port at the same time as 802.1x. This function is very useful for some devices that do not have 802.1x function or devices that are inconvenient to use 802.1x, such as printers, file servers, etc.

Mac filtering can prevent some specified MAC addresses from accessing the network. The main purpose is to prevent some illegal devices from accessing the network. When a MAC address is configured as MAC filtering, the MAC address cannot access the network at any port of the switch, nor can it receive packets whose destination MAC is these specified MAC addresses. Like MAC binding, a port can configure multiple MAC filtered MAC addresses at the same time. In the application, if some virus software attacks the network through forged MAC address, in addition to ACL, it can also access and control the attack of these forged data packets through MAC filtering.

Port learning control can control the number of MAC addresses that a port can dynamically learn. If a port specifies the number of MAC addresses it can dynamically learn, when the number of MAC addresses learned by the port is equal to the number configured by the port, the new MAC addresses will not be learned, and the packets of these new MAC addresses will be discarded.

It should be noted that the MAC address referred to here is actually MAC + vid, and the description later in this chapter will not be repeated. In addition, MAC binding function and 802.1x can be configured on one port at the same time; Mac filtering and port learning restrictions can be configured on one port at the same time; Mac binding function, 802.1x and MAC filtering, and port learning restrictions cannot be configured to the same port at the same time.

1.22 MACBinding configuration

Mac binding configuration supports manual binding of MAC address and automatic binding of MAC address. Manually binding MAC addresses means that the user inputs

MAC addresses one by one through commands to bind with ports. Automatic MAC address binding is to read out the existing entries of the port in the layer 2 hardware forwarding table and bind the MAC address directly. The command to read the L2 hardware table is show bridge FDB。

Configuration command

Command	Description	CLI mode
switchport-security mac-bind HHHH.HHHH.HHHH vlan <1-4094> qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7}	Manually bind a MAC address to an interface and configure the priority queue of the table item.	Interface configuration mode
switchport-security mac-bind auto-conversion number <1-8191> qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7}	Automatically convert the specified number of MAC addresses of an interface into MAC binding configuration, and configure the priority queue of the table item.	Interface configuration mode
switchport-security mac-bind auto-conversion vlan <1-4094> qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7}	Automatically convert the MAC address of the specified VLAN of an interface into MAC binding configuration, and configure the priority queue of the table item.	Interface configuration mode
show port-security mac-bind [IFNAME]	Display MAC binding configuration	Privileged mode

Note:

The reasons for invalid or failed MAC address binding may be as follows:

The port has been configured with 802.1x

The port has been configured with MAC filtering or port learning restrictions;

The MAC address has been bound to other ports or configured with MAC filtering;

The L2 table of the switch is full.。

1.23 MACFilter configuration

Mac filtering configuration supports manual binding of MAC address and automatic binding of MAC address. To manually configure MAC filtering, the user inputs the Mac to be filtered one by one through the command and binds it with the port. Automatic configuration of MAC filtering is to read out the existing entries of the port in the layer 2 hardware forwarding table and directly configure MAC filtering. The command to read the layer 2 hardware table is Show bridge fdb。

Configuration command

Command	Description	CLI mode
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Manually configure MAC filtering of an interface	Interface configuration mode
switch port-security mac-filter auto-conversion number <1-8191>	Automatically convert the specified number of MAC addresses of an interface into MAC filtering configuration	Interface configuration mode
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Automatically convert the MAC address of the specified VLAN of an interface into MAC filtering configuration	Interface configuration mode
show port-security mac-filter [IFNAME]	Display MAC binding configuration	Privileged mode

Note：

The reasons for the invalid or failed MAC filtering configuration may be as follows:

The port has been configured with MAC binding or enabled with 802.1x protocol function;

The MAC address has been bound to other ports, or Mac binding is configured;

The L2 table of the switch is full。

1.24 Port learning restriction configuration

The switch can configure the maximum number of dynamic learning addresses per port. If a port is configured to dynamically learn the number of MAC addresses, the port can only learn the corresponding number of MAC addresses. When the number of MAC addresses exceeds this number, it cannot learn and forward on this port.

When the learning limit is not configured, a port can learn up to 8191 MAC addresses。

Configuration command

Command	Description	CLI mode
switchport port-security learn-limit <0-8191>	Configure the number of MAC addresses that an interface can learn.	Interface configuration mode
no switchport port-security learn-limit	Delete the number of MAC addresses that an interface can learn.	Interface configuration mode
show port-security learn-lmit [IFNAME]	Display port learning configuration	Privileged mode

Configuration example

Configuring port GE1 / 5 can only learn 7 MAC addressesSwitch#configure terminal

Switch(config)interface ge1/5

Switch(config-ge1/5)switchport port-security learn-limit 7

Note：

The reasons for invalid or failed port learning settings may be as follows:

The port has been configured with MAC binding or enabled with 802.1x protocol function。

1.25 Protection port configuration

1.25.1 Introduction to protection port

In order to realize the two-layer isolation between data packets, ports can be divided

into different VLANs, but VLAN resources will be wasted. Configuring ports as protection ports can realize the isolation of ports in the same VLAN and provide users with a safer and more flexible networking scheme.

Each port can be configured as a protected port. The protected ports cannot communicate with each other, but can only communicate with non protected ports. There are two application modes:

1. Only one port is not configured as a protection port, and all other ports are isolated;

2. Prevent some insecure ports from sniffing the data of other ports (even the server), and set these ports as protection ports。

1.25.2 Protection port configuration

Configure the port as a protected port. In the config mode, enter the port configuration mode, such as interface GE1 / 1, and execute the following commands：

Switch(config-ge1/1)#switchport port-security protect

Displays the ports configured as protection portsSwitch#show port-security protect

Port Port protected

----- --------------

ge1/1 ON

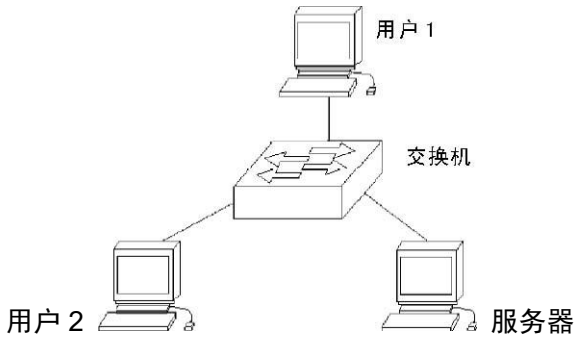
Typical configuration example of protection port

Networking requirements

The user 1 and user 2 servers are respectively connected to the ports GE1 / 1, GE1 / 2 and GE1 / 3 of the switch

User 1 and user 2 servers belong to the same VLAN. It is required that user 1 and user 2 cannot communicate with each other, but can communicate with the serve。

Networking diagram



Configuration stepsSwitch>enable

Switch#config terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport port-security protect

Switch(config-ge1/1)#interface ge1/2

Switch(config-ge1/2)#switchport port-security protect

Switch(config-ge1/2)#exit

Switch(config)#exit

Switch#show port-security protect

Port Port protected

----- --------------

ge1/1 ON

ge1/2 ON

Configure port IP and MAC binding

This chapter introduces the binding configuration of port IP and MAC, mainly including the following contents：

- Introduction
- IP and MAC binding configuration
- Configuration example
- Configuration troubleshooting

`

1.26 Introduction

Configuring IP and MAC binding on layer 2 switch port is a static defense measure against ARP attack. ARP attackers attack users by sending ARP messages with false MAC addresses, causing the user's local ARP cache table to be overwritten by the attacker's MAC address, so that normal data flows to the attacker. Configure the command on the switch port to statically bind the user's IP address and MAC address, which can effectively filter ARP attack packets.

In addition to the function of preventing ARP spoofing, the IP MAC binding function can also ensure the one-to-one mapping relationship between IP and MAC, that is, an IP can only correspond to one MAC, and a Mac can only correspond to one IP. If the access device modifies this mapping relationship, it will not be able to communicate in this network. 802.1x anti ARP Spoofing function and DHCP snooping protocol are the dynamic implementation of this function.

The four functions of IP MAC binding, ACL, 802.1x anti ARP Spoofing and DHCP snooping all use the same system resources CFP. Pay attention to whether the CFP resources are exhausted during configuration. In the design, we formulated the compatibility relationship between them. The following table：

	IP MACbinding	ACL	802.1x	DHCP SNOOPING
IP MACbinding	compatible	incompatible	compatible	compatible
ACL	incompatible	compatible	incompatible	incompatible
802.1x	compatible	incompatible	compatible	incompatible
DHCP SNOOPING	compatible	incompatible	incompatible	compatible

CFP is a limited hardware resource. On average, only 16 IP MAC binding entries can be configured for each port. Therefore, in a network with many access hosts, if only a few ports or a few IP and MAC addresses need to be controlled, the static IP MAC binding function can be adopted. Avoid data forwarding failure caused by CFP function exhaustion.

In addition, whether to use 802.1x or DHCP snooping protocol depends on the current situation. If you use static IP address configuration and use 802.1x protocol to access the network, you need to use 801.1x anti ARP Spoofing to be effective. If you use dynamic IP address acquisition, you need to use DHCP snooping protocol。

1.27 IP and MAC binding configuration

IP and MAC binding configuration

Configure port IP and MAC binding

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#ip mac-bind A.B.C.D MAC

Delete port IP and MAC binding

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no ip mac-bind A.B.C.D MAC

Display configuration

Show binding table entries for all ports

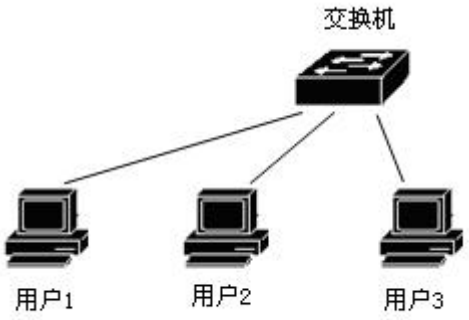
show ip mac-bind

Displays the binding table entry of an interface

show ip mac-bind IFNAME

1.28 Configuration example

There are user 1, user 2 and user 3 in the network. Bind the user's IP and MAC on the port to defend against ARP attacks。




```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#ip mac-bind 192.168.1.100 0011.5b34.42ad
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#ip mac-bind 192.168.1.101 0011.6452.135d
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#ip mac-bind 192.168.1.102 0011.804d.a246
Switch(config-ge1/3)#end
Switch#show ip mac-bind
[ge1/1] sum: 1
        MAC                 IP
        0011.5b34.42ad      192.168.1.100
[ge1/2] sum: 1
        MAC                 IP
        0011.6452.135d      192.168.1.101
```

```
[ge1/3] sum: 1
        MAC                 IP
        0011.804d.a246      192.168.1.102
Switch#show ip mac-bind ge1/1
[ge1/1] sum: 1
        MAC                 IP
        0011.5b34.42ad      192.168.1.100
Switch#show running-config
!
spanning-tree mst configuration
!
Interface vlan1
 ip address 10.10.10.1/24
!
interface ge1/1
 ip mac-bind 192.168.1.100 0011.5b34.42ad
!
interface ge1/2
 ip mac-bind 192.168.1.101 0011.6452.135d
!
interface ge1/3
 ip mac-bind 192.168.1.102 0011.804d.a246
!
line vty
!
end
```

1.29 Configuration troubleshooting

If the IP MAC binding configuration fails, it may be caused by the following reasons：

1. System CFP resources are exhausted.
2. The ACL filtering function is configured for the current interface.
3. The configured interface is a layer 3 interface or trunk interface。

Port loop detection

This chapter mainly includes the following contents：

- Introduction
- Protocol principle
- Configuration introduction

1.30 Introduction

When a loop appears under a port of the switch, it will cause a broadcast storm under this port, and learn the source MAC address of all broadcast packets to this looped port, which will cause the device forwarding to fail normally。

1.31 Protocol principle

Ethernet loopback detection (ELD) can detect the loop through the interaction of data packets and block the port where the loop occurs. Eld protocol is a protocol based on port calculation. It can only detect the loop of this port。

1.31.1 Detection process

When the eld protocol is enabled on a port, a timer will be enabled on this port. When the timer expires, the loop detection packet will be sent. If the loop detection packet sent by yourself is received within a timer cycle, it is considered that there is a loop on this port, the operation of blocking the loop on this port will be performed, and the FDB table of this port will be cleared.

If a port belongs to a port member of multiple VLANs, the port will automatically send loop detection packets to all VLANs. In other words, this port will automatically detect whether there are loops in all VLANs it belongs to。

1.31.2 Recovery mode

As mentioned above, when a port loop appears, the of this port will be blocked. Eld protocol has two recovery modes that users can configure: automatic recovery and

manual recovery.

Automatic recovery means that when a port is blocked, the eld protocol enables a recovery timer. After the timer expires, it will perform a reverse operation of blocking the loop, and enable the loop detection timer again at this port.

Manual recovery means that after the port is blocked, the protocol will no longer enable the timer to recover the port. The user should input the command to perform the reverse operation of blocking the loop。

1.31.3 Protocol security

Eld protocol is vulnerable to attack in the network, that is, users can send eld protocol packets to a port that enables eld protocol according to the packet format of eld protocol, resulting in the port being blocked without loop, resulting in wrong decisions.

Eld protocol adopts two strategies to prevent similar attacks and minimize the error.

Decision 1: firstly, ELD protocol is a protocol without interaction, that is, it does not depend on other devices, so the data packet itself can be simply encrypted. Our operation here is to send an eld protocol package with a key. The user cannot disguise the protocol package without a key.

Decision 2 is mainly to prevent attackers from reflecting protocol packets through packet capture attacks. The format of data packets received by the switch in a certain cycle can be configured to prevent attacks. This needs to be configured by users。

1.32 Configuration introduction

Eld protocol is implemented based on port, and there is no unified enabling command。

1.32.1 Global configuration

Global configuration is a unified attribute of configuration protocol。

Command	Description	Mode
loop-detection detection-time <1-65535>	Configure the time period of loop detection. Twice this time must be less than the recovery time period. The default value is 5 seconds.	Global configuration mode
loop-detection resume-time <10-65535>	Configure the time period of automatic recovery. The time of automatic recovery must be greater than 2 of the loop check time. If automatic recovery is enabled, this configuration will take effect. The	Global configuration mode

	default recovery time is 600 seconds.	
loop-detection protocol-safety	Enable protocol security check. It is off by default.	Global configuration mode
loop-detection respond-packets	Configure the number of packets that must be received within a certain period of time. If protocol security check is enabled, this configuration will take effect. The default value is 10	Global configuration mode

1.32.2 Port configuration

Interface configuration is the configuration of each port.

Command	Description	Mode
Loop-detection enable	Enable eld protocol on a port.	Interface configuration mode
Loop-detection resume	Manually restore and restart the loop check.	Interface configuration mode
loop-detection resume-mode {automation | manual}	Configure the recovery mode and select manual recovery or automatic recovery. The default is automatic recovery.	Interface configuration mode
loopback-detection shutdown-mode {no-shutdown | shutdown}	The command configures whether the port is shut down when a loop occurs.	Interface configuration mode

1.32.3 Display configuration

Show loop-detection [ifname]

Displays all configurations of the protocol and the configuration of an interface。

Configure VLAN

VLAN is an important concept in switches. It is widely used in practical applications. It is the basis for internal division of multiple networks. VLAN is the abbreviation of virtual LAN. It is a network that logically organizes multiple devices together, regardless of the physical location of the devices. Each VLAN is a logical network, which has all the functions and attributes of the traditional physical network. Each VLAN is a broadcast domain. Broadcast packets can only be forwarded within one VLAN, not across VLANs. Data communication between VLANs must be forwarded through three layers.

This chapter mainly includes the following contents：

- VLAN introduction
- VLAN configuration
- VLAN configuration example

1.33 VLAN introduction

This section gives a detailed introduction to VLAN, mainly including the following contents：

- Benefits of VLAN
- VLAN ID
- VLAN Port member type
- Default VLAN for port
- VLAN mode of port
- VLAN relay
- Forwarding of data flow in VLAN
- Subnet of VLAN

1.33.1 Benefits of VLAN

VLAN greatly expands the scale of physical network. The traditional physical network can only have a very small scale, which can accommodate thousands of devices at most, while the physical network divided by VLAN can accommodate tens of thousands or even hundreds of thousands of devices. VLAN has the same functions and attributes as traditional physical networks.

Using VLANs has the following benefits：

- VLAN can effectively control the traffic in the network。

In traditional networks, whether necessary or not, all broadcast packets are transmitted to all devices, which increases the load of networks and devices. VLAN can organize devices in a logical network according to needs. A VLAN is a broadcast domain. Broadcast packets are only transmitted within the VLAN and will not cross the VLAN. By dividing VLANs, the traffic in the network can be effectively controlled。

- VLAN can improve the security of the network。

Devices in a VLAN can only communicate with devices in the same VLAN through layer 2. If you want to communicate with another VLAN, you must forward through layer 3. If layer 3 forwarding between VLANs is not established, VLANs cannot communicate at all, which can play the role of isolation and ensure the data security in each VLAN. For example, if the R & D Department of a company does not want to share data with the marketing department, the R & D department can establish a VLAN, the marketing department can

establish a VLAN, and there is no three-layer communication channel between the two VLANs。

- VLAN Make the movement of equipment convenient。

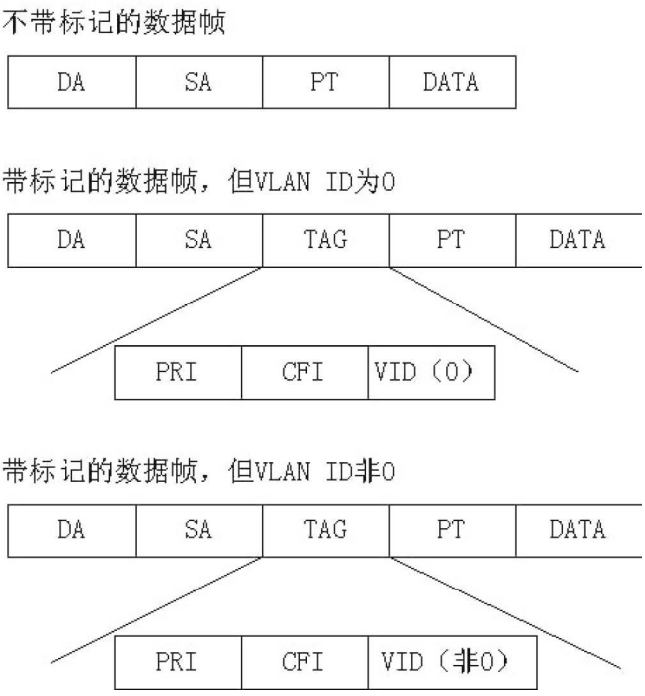
If a device in a traditional network moves from one location to another and belongs to a different network, it needs to modify the network configuration of the mobile device, which is very inconvenient for users. VLAN is a logical network, which can divide the devices not in the same physical location into the same network. When the devices move, they can also belong to this VLAN, so that the mobile devices do not need to modify any configuration。

1.33.2 VLAN ID

Each VLAN has an identification number called VLAN ID. the VLAN ID ranges from 0 to 4095, of which 0 and 4095 are not used. Only 1 to 4094 are actually valid. VLAN ID uniquely identifies a VLAN.

The switch supports 4094 VLANs. When creating VLANs, select a VLAN ID, ranging from 2 to 4094. The switch creates vlan1 by default, and vlan1 cannot be deleted.

There are three kinds of data frames transmitted in a VLAN in the network: data frames without tags, data frames with tags with vid 0 and data frames with tags with vid non-0. As shown in the figure below, there are three different data frame formats。



Inside the switch, all data frames are marked. If a data frame without tag is input into the switch, the switch will add a tag to the data frame, and select a VLAN ID value to fill in the marked vid. If a tagged data frame with vid 0 is input to the switch, the switch selects a VLAN ID value to fill in the tagged vid. If a data frame marked with vid non-0 is input to the switch, the frame remains unchanged。

1.33.3 VLAN Port member type

The switch supports port based VLAN and 802.1Q based VLAN. A VLAN includes two port member types: untagged member and tagged member. A VLAN can include both untagged and tagged port members.

A VLAN can have no port members or one or more port members. When a port belongs to a VLAN, it can be an untagged member or a tagged member of the VLAN.

A port can belong to tagged or untagged members of one or more VLANs. If a port belongs to tagged members of two or more VLANs, this port is also called VLAN relay port. A port can belong to untagged members of one or more VLANs and tagged members of another VLAN or VLANs at the same time。

1.33.4 Default port VLAN

The port has and has only one default VLAN. The default VLAN is used to determine the VLAN of the data packet without tag or with tag but vid 0 input from the port. The default VLAN is also called port vid or PVID. By default, the default VLAN of the port is 1。

1.33.5 VLAN mode of port

There are three VLAN modes on the port: access mode, trunk mode and hybrid mode. When configuring the VLAN of a port, the user must first specify the VLAN mode of the port.

The port of access mode is an access port that directly faces the user. This port can only belong to the untagged member of one VLAN. The default VLAN is the VLAN specified by the user. When a port belongs to an untagged member of only one VLAN, you can specify that the VLAN mode of the port is access mode.

The port in trunk mode is a relay port, which is directly connected to the switch. This port can belong to the tagged members of one or more VLANs, but cannot belong to the untagged members of any VLAN. The default VLAN of this port is 1 and cannot be changed.

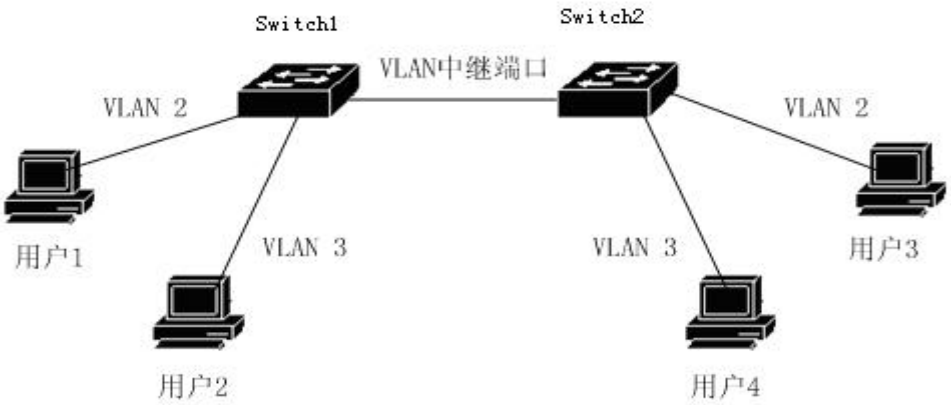
The port in hybrid mode is a relay port, which is directly connected to the switch. The port can belong to the tagged members of one or more VLANs and / or the untagged members of one or more VLANs. The default VLAN of this port can be changed.

In practical application, the user can select the VLAN mode of the port according to the specific situation。

1.33.6 VLAN RELAY

If a port belongs to a tagged member of two or more VLANs, it is also called a VLAN relay port. Two switches can be connected by VLAN trunk ports, so that two or more common VLANs can be divided between two switches.

The following figure is an example of VLAN relay. Two switches are connected by VLAN relay ports, which are the relay ports of VLAN 2 and VLAN 3. Each switch is divided into two VLANs, VLAN 2 and VLAN 3 respectively. There is one user in each VLAN. In this way, user 1 can communicate with user 3, user 2 can communicate with user 4, and user 1 and user 3 cannot communicate with user 2 and user 4。



1.33.7 forwarding of data flow in VLAN

When the switch receives a data packet from a port, carry out layer 2 forwarding according to the following steps：

- Determine the VLAN to which the packet belongs 。
- Judge whether the packet is broadcast packet, multicast packet or unicast packet。
- Determine the output port according to different data packets (it can be zero, one or more output ports). If there is no output port, discard the data packet。
- Determine whether the outgoing packet is marked according to the member type of the output port in the VLAN。
- Send from output port。

1) How to determine the VLAN of the packet:

If the received packet is tagged and the vid field in the tag is not 0, the VLAN to which the packet belongs is the V I d value in the tag.

If the received packet is not tagged or tagged, but the vid value in the tag is 0, the VLAN to which the packet belongs is the default VLAN of the port.

2) How to determine the type of data package:

If the destination MAC address of the received packet is FF: FF: FF: FF: FF: FF, the packet is a broadcast packet.

If the received packet is not a broadcast packet and the 40th bit of its destination MAC address is 1, the packet is a multicast packet.

If it is neither a broadcast packet nor a multicast packet, the packet is a unicast packet。

3) How to determine the output port of a packet:

If the input packet is a broadcast packet, all member ports of the VLAN to which the packet belongs are the output ports of the packet.

If the input packet is a multicast packet, first look up the layer-2 hardware multicast forwarding table according to the destination multicast MAC address and the VLAN. If a matching multicast entry is found, the common port (and operation) in the output port in the multicast entry and the member port in the VLAN is the output port of the packet. If there is no common port, the packet is discarded. If no matching multicast entry is found in the layer-2 hardware multicast forwarding table, the output port is determined according to the forwarding mode of layer-2 hardware multicast forwarding. If it is an unregistered multicast forwarding mode, the multicast packet is treated as a broadcast, and all member ports of the VLAN are the output ports of the data packet. If it is a registered forwarding mode, there is no output port, Packet drop.

If the input packet is a unicast packet, first look up the layer-2 hardware forwarding table according to the destination MAC address and the VLAN. If a matching entry is

found, the common port (and operation) between the output port in the entry and the member port of the VLAN is the output port of the packet. If there is no common port, the packet is discarded. If no matching entry is found in the layer 2 hardware forwarding table, the data packet is treated as a broadcast packet, and all member ports of the VLAN are the output ports of the data packet。

4) Send packet:

After determining the output port of the input packet, send the packet from all the output ports.

If an output port is an untagged member of the VLAN to which the packet belongs, the packet is sent from the output port without a tag.

If an output port is a tagged member of the VLAN to which the packet belongs, the packet is marked when it is sent from the output port, and the vid value in the tag is the value of the VLAN to which the packet belongs。

1.34 VLAN configuration

This section introduces VLAN configuration in detail, mainly including the following contents：

- Creating and deleting
- VLAN mode of VLANs configuration port
- VLAN configuration in access mode
- VLAN configuration in trunk mode
- VLAN configuration in hybrid mode
- VLAN subnet configuration
- View VLAN information

1.34.1 Creating and deleting VLANs

Before creating and deleting VLANs, users need to use the VLAN database command in the global configuration mode to enter the VLAN configuration mode, and create and delete VLANs in this mode.

The system has created VLAN 1 by default, and VLAN 1 cannot be deleted by the user. The commands for creating and deleting VLANs are shown in the following table：

Command	Description	CLI mode
vlan <vlan-id>	Create a VLAN. If the VLAN already exists, it will not be processed. Otherwise, this VLAN will be created. The parameters range from 2 to 4094.	VLAN configuration mode
no vlan <vlan-id>	Delete a VLAN. If the VLAN does not exist, it will not be processed. Otherwise, delete the VLAN. The parameters range from 2 to 4094。	V VLAN configuration mode

1.34.2 Configure VLAN mode of port

Before configuring the VLAN of a port, you need to specify the VLAN mode of the port. By default, the VLAN mode of the port is access mode. The commands for specifying the VLAN mode of the port are shown in the following table：

Command	Description	CLI mode
switchport mode access	The VLAN mode of the specified port is access mode. After executing this command, the port is an untagged member of vlan1, and the default VLAN of the port is 1。	Interface configuration mode
switchport mode trunk	The VLAN mode of the specified port is trunk mode. After executing this command, the port is a tagged member of vlan1, and the default VLAN of the	Interface configuration mode

	port is 1。	
no switchport trunk	The VLAN mode of the port is no longer trunk mode, but returns to the default, access mode.	Interface configuration mode
switchport mode hybrid	The VLAN mode of the specified port is hybrid mode. After executing this command, the port is an untagged member of vlan1, and the default VLAN of the port is 1。	Interface configuration mode
no switchport hybrid	The VLAN mode of the port is no longer the hybrid mode, but returns to the default mode, i.e. access mode.	Interface configuration mode

1.34.3 VLAN configuration in access mode

Before VLAN configuration of a port, you need to specify that the VLAN mode of the port is access mode. In this VLAN mode, the port defaults to the untagged member of vlan1, and the default VLAN of the port is 1. VLAN configuration commands in access mode are as follows:

Command	Description	CLI mode
switchport access vlan <vlan-id>	The configuration port is an untagged member of the specified VLAN, and the default VLAN of the port is the specified VLAN. The parameters range from 2 to 4094.	Interface configuration mode
no switchport access vlan	The VLAN configuration of the port returns to the default, that is, the port is an untagged member of vlan1,	Interface configuration mode

	and the default VLAN of the port is 1。	

1.34.4 VLAN configuration in trunk mode

Before VLAN configuration of a port, you need to specify that the VLAN mode of the port is trunk mode. In this VLAN mode, the port defaults to the tagged member of vlan1, and the default VLAN of the port is 1. VLAN configuration commands in trunk mode are shown in the following table：

Command	Description	CLI mode
switchport trunk native vlan <vlan-id>	Configure the default VLAN of the port, that is, PVID. The parameters range from 2 to 4094.	Interface configuration mode
switchport trunk allowed vlan all	The configuration port is the tagged member of all VLANs. For VLANs newly created in the future, the port is also the tagged member of these VLANs。	Interface configuration mode
switchport trunk allowed vlan none	Except vlan1, this port is no longer a tagged member of all other VLANs。	Interface configuration mode
switchport trunk allowed vlan add <vlan-list>	Configure the port to become a tagged member of one or more specified VLANs. The parameter < VLAN list > can be one VLAN, one VLAN range or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5".	Interface configuration mode
switchport trunk allowed vlan remove <vlan-list>	Clear the port from one or more specified VLANs and is no longer a tagged	Interface configuration mode

	member of these VLANs. The parameter < VLAN list > can be one VLAN, one VLAN range or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5".	

1.34.5 VLAN configuration in hybrid mode

Before VLAN configuration of a port, you need to specify that the VLAN mode of the port is hybrid mode. In this VLAN mode, the port defaults to the untagged member of vlan1, and the default VLAN of the port is 1. VLAN configuration commands in hybrid mode are shown in the following table：

Command	Description	CLI mode
switchport hybrid native vlan <vlan-id>	The configuration port is an untagged member of the specified VLAN, and the default VLAN of the port is the specified VLAN. The parameters range from 2 to 4094.	Interface configuration mode
no switchport hybrid native vlan	Clear the port from the default VLAN. It is no longer a tagged or untagged member of the default VLAN. The default VLAN of the port returns to 1.	Interface configuration mode式
switchport hybrid allowed vlan all	The configuration port is a tagged member of all VLANs (except vlan1). For VLANs newly created in the future, the port is also a tagged member of these	Interface configuration mode

	VLANs.	
switchport hybrid allowed vlan none	Except vlan1, the port is no longer a tagged or untagged member of all other VLANs, and the default VLAN of the port returns to 1.	Interface configuration mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged enable	Configure the port to become a tagged member of one or more specified VLANs. The parameter < VLAN list > can be one VLAN, one VLAN range or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5".	Interface configuration mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged disable	Configure the port to become an untagged member of one or more specified VLANs. The parameter < VLAN list > can be one VLAN, one VLAN range or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5".	Interface configuration mode
switchport hybrid allowed vlan remove <vlan-list>	Clear the port from one or more specified VLANs and is no longer a tagged or untagged member of these VLANs. If the default VLAN of the port belongs to the specified VLAN, the default VLAN returns to 1.	Interface configuration mode

1.34.6 View VLAN information

The commands for viewing VLAN information are shown in the following table：

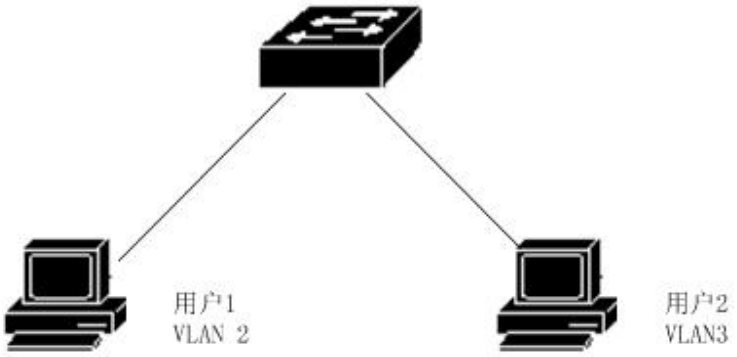
Command	Description	CLI mode
show vlan [vlan-id]	If you do not enter parameters, all VLAN information will be displayed. If you enter parameters, a specified VLAN information will be displayed. The parameters range from 1 to 4094.	Normal mode privileged mode
show interface	Displays VLAN related information of all ports of the system, such as VLAN mode, default VLAN, etc.	Normal mode privileged mode
show running-config	View the current system configuration, and you can view the VLAN configuration.	privileged mode

1.35 VLAN configuration example

1.35.1 Port based VLAN

1) configuration

There are two users, user 1 and user 2. The two users need to be in different VLANs due to different network functions and environments. Subscriber 1 belongs to vlan2 and connects to port GE1 / 1 of the switch. Subscriber 2 belongs to vlan3 and connects to port



GE1 / 2 of the switch.

The configuration of the switch is as follow：

Create VLAN

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Assign ports to VLANsSwitch#config t

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 2

Switch(config-ge1/1)#exit

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 3

2) Troubleshooting

If, after configuration, it is found that PCs between different VLANs cannot communicate, it is a normal phenomenon, because to communicate between different VLANs, they must go through three-layer routing and forwarding. If the PC in the same VLAN cannot communicate, the following verification must be performed：

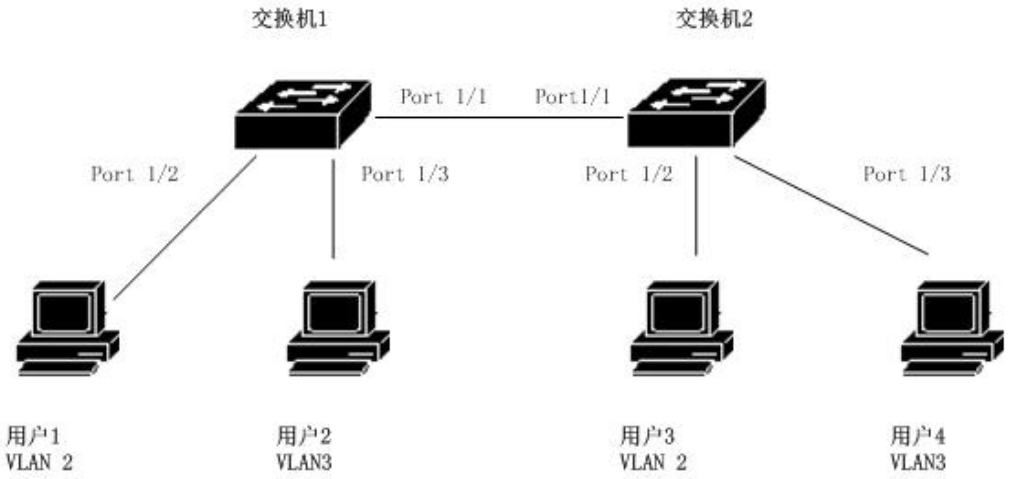
show vlan

View the member ports of all VLANsshow vlan <vlan-id>

Check whether the port connecting a specific PC is within the specified VLAN

1.35.2 802.1Q based VLAN

1) configuration



Two switches are connected to two users respectively：

User	Belong to VLAN	Connect port	Belong to switch	cascade port
User 1	2	1/2	switch 1	1/1
User 2	3	1/3	switch 1	1/1
User 3	2	1/2	switch 2	1/1
User 4	3	1/3	switch 2	1/1

It needs to be configured on two switches.

Switch 1 configuration：

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Switch#config t

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk allowed vlan add 2

Switch(config-ge1/1)#switchport trunk allowed vlan add 3

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 2

Switch(config-ge1/2)#exit

Switch(config)#interface ge1/3

Switch(config-ge1/3)#switchport mode access

Switch(config-ge1/3)#switchport access vlan 3

Switch 2 configuration：

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Switch#config t

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk allowed vlan add 2

Switch(config-ge1/1)#switchport trunk allowed vlan add 3

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 2

Switch(config-ge1/2)#exit

Switch(config)#interface ge1/3

Switch(config-ge1/3)#switchport mode access

Switch(config-ge1/3)#switchport access vlan 3

2) Troubleshooting

VLANs across switches and PCs in the same VLAN can communicate, if not. You must check the following：

- Whether the port connecting the PC belongs to the corresponding VLAN, and apply the access mode to join the VLAN。
- Cascade port 1 / 1 is added to each VLAN, and port 1 / 1 is trunk mode。

1.36 Mac, IP subnet, protocol VLAN

1.36.1 Introduction to Mac, IP subnet and protocol VLAN

The VLAN based on MAC is divided according to the MAC address of the message source. After receiving the untagged (or tag 0) message from the port, the device will

determine the VLAN to which the message belongs according to the source MAC address of the message, and then automatically divide the message into the specified VLAN for transmission;

VLAN based on IP subnet is divided according to the source IP address and subnet mask. After receiving the untagged message from the port, the device will determine the VLAN of the message according to the source address of the message, and then automatically divide the message into the specified VLAN for transmission. This feature is mainly used to transmit the message sent by the specified network segment or IP address in the specified VLAN;

Protocol based VLAN assigns different VLAN IDs to the packets according to the protocol type of the packets received by the port. The protocols that can be used to divide VLANs include IP, IPv6, IPX, etc。

1.36.2 Mac, IP subnet, protocol VLAN configuration

Before configuring VLANs based on MAC, IP subnet and protocol, you must first create corresponding VLANs。

Command	Description	CLI mode
mac-vlan mac WORD vlan <1-4094>	Create a VLAN based on the source MAC address	VLAN configuration mode
no mac-vlan mac WORD	Delete a VLAN based on the source MAC address	VLAN configuration mode
no mac-vlan	Delete all VLANs based on source MAC address	VLAN configuration mode
mac-vlan enable	Start the mac-vlan function of the interface	Interface configuration mode
mac-vlan disable	Turn off the mac-vlan function of the interface	Interface configuration mode
show mac-vlan	Displays all VLANs based on the source MAC address	Privileged mode
ip-subnet-vlan ip A.B.C.D	Create a VLAN based on	VLAN

A.B.C.D vlan <1-4094>	the source IP subnet	configuration mode
no ip-subnet-vlan ip A.B.C.D A.B.C.D	Delete a VLAN based on the source IP subnet	VLAN configuration mode
no ip-subnet-vlan	Delete all VLANs based on the source IP subnet	VLAN configuration mode
ip-subnet-vlan enable	Start the VLAN function based on the source IP subnet of the interface	Interface configuration mode
ip-subnet-vlan disable	Turn off the VLAN function based on the source IP subnet of the interface	Interface configuration mode
show ip-subnet-vlan	Displays all VLANs based on the source IP subnet	Privileged mode
protocol-vlan ether-type (ip|ipv6|ipx|…|<0-65535>) vlan <1-4094>	Create a protocol based VLAN	Interface configuration mode
no protocol-vlan ether-type (ip|ipv6|ipx|…|<0-65535>)	Delete a protocol based VLAN	Interface configuration mode
no protocol-vlan	Delete all protocol based VLANs	Interface configuration mode
show protocol-vlan	Displays all protocol based VLANs	Privileged mode
show vlan-partition interface IFNAME	Displays the status of enabling VLANs based on MAC and IP subnets on the interface	Privileged mode

1.37 Voice VLAN

1.37.1 Voice VLAN Introduction

Voice VLAN is a VLAN specially divided for users' voice data flow. By dividing voice VLAN and adding the port connecting voice equipment to voice VLAN, QoS (quality of service) parameters can be configured for voice data to improve voice data message priority and ensure call quality.

The device can judge whether the data stream is a voice data stream according to the source MAC address oui field in the data message entering the port. The message whose source MAC address conforms to the oui address of voice equipment set by the system is considered as voice data stream and is divided into voice VLAN for transmission.

The user can set the oui address in advance or use the default oui address as the judgment standard, as shown below

erial number	Oui address	Manufacturer
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3com phone

Manually add the IP phone access port to the voice VLAN. Then match the oui address by identifying the source MAC of the message. After the matching is successful, the system will issue ACL rules and configure the priority of the message。

1.37.2 Voice VLAN configuration

Before configuring voice VLAN, you must first create the corresponding VLAN。

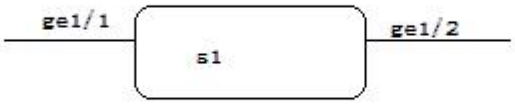
Command	Description	CLI mode
voice-vlan oui WORD mask WORD	Configure user oui	Global configuration mode
voice-vlan oui WORD mask WORD description WORD	Configure user oui and name it	Global configuration mode
no voice-vlan oui WORD	Delete user oui	Global

mask WORD	configuration through oui address and mask	configuration mode
no voice-vlan oui description WORD	Delete user oui configuration by naming	Global configuration mode
no voice-vlan oui	Delete all user oui configurations	Global configuration mode
no voice-vlan default-oui WORD mask WORD	Delete default oui configuration through oui address and mask	Global configuration mode
no voice-vlan default-oui description WORD	Delete the default oui configuration by naming	Global configuration mode
no voice-vlan default-oui	Delete all default oui configurations	Global configuration mode
voice-vlan default-oui resume	Restore all default oui configurations	Global configuration mode
show voice-vlan oui	Displays all default and user oui configurations	Privileged mode
voice vlan <1-4094> (enable|disable)	Interface enable voice VLAN	Interface configuration mode
voice vlan qos remark cos <0-7> dscp <0-63>	The interface is configured with QoS priority. The cos value is 6 and the DSCP value is 46	Interface configuration mode
no voice vlan qos	Restore interface QoS priority default configuration	Interface configuration mode
no voice vlan	Delete interface configuration voice VLAN	Interface configuration mode
show voice-vlan	Displays the configuration of	Privileged mode

	voice VLAN for all interfaces	

1.37.3 Voice VLAN configuration example

Configure the voice data stream (0009.ca00.0000) to flow in from port GE1 / 1 and out from port GE1 / 2 with tag 2, as shown in the following figure



The configuration of switch S1 is as follows：

```
Switch#con t
Switch(config)#vlan da
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#int ge1/1
Switch(config-ge1/1)#sw mod hy
Switch(config-ge1/1)#sw hybrid allowed vlan add 2 egress-tagged
disable
Switch(config-ge1/1)#voice vlan 2 en
Switch(config-ge1/1)#voice vlan 2 enable
Switch(config-ge1/1)#int ge1/2
Switch(config-ge1/2)#sw mod tr
Switch(config-ge1/2)#sw trunk allowed vlan add 2
Switch(config-ge1/2)#exit
Switch(config)#voice-vlan oui 0009.ca00.0000 mask ffff.ff00.0000
Switch(config)#
```

1.38 VLAN mapping

1.38.1 VLAN mapping introdution

The VLAN mapping function can modify the VLAN tag carried by the message and provide the following mapping relationship: 1:1 VLAN mapping: modify the VLAN ID in the VLAN tag carried by the message to another VLAN ID.

Before configuring VLAN mapping, you must first create the corresponding VLAN。

1.38.2 VLAN mapping configuration

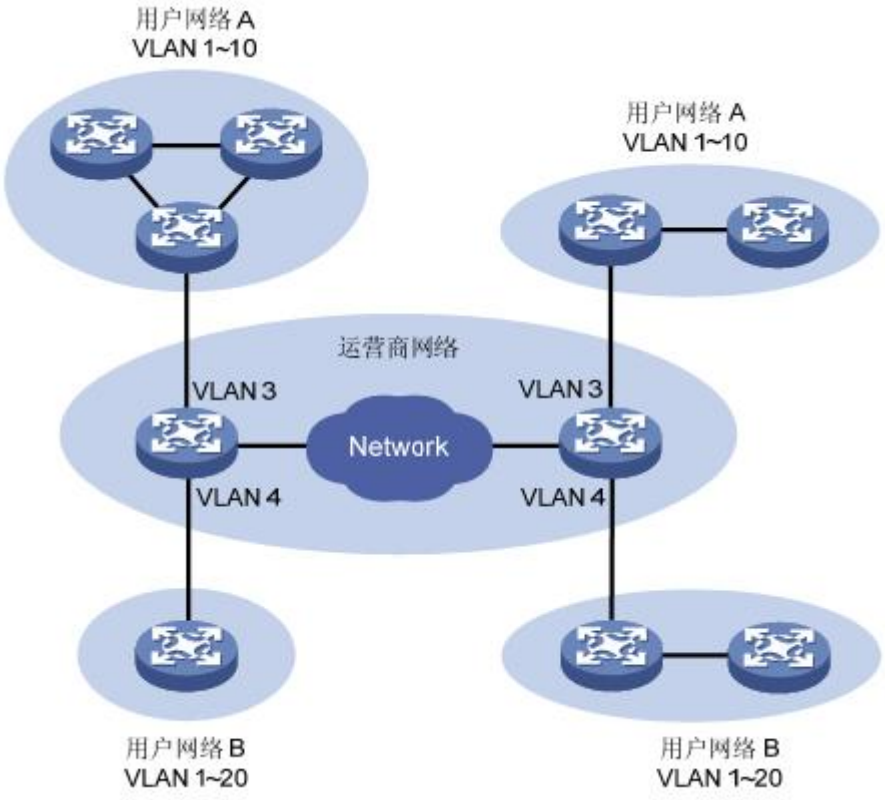
Command	Description	CLI mode
vlan-mapping vlan <1-4094> map-vlan <1-4094>	Configure a VLAN mapping relationship of ports	Interface configuration mode
no vlan-mapping vlan <1-4094>	Delete a VLAN mapping relationship of the port	Interface configuration mode
no vlan-mapping	Delete all VLAN mapping relationships of ports	Interface configuration mode
vlan-mapping enable	VLAN mapping relationship of startup port	Interface configuration mode
vlan-mapping disable	Close the VLAN mapping relationship of the port	Interface configuration mode
show vlan-mapping	Displays all configured VLAN mappings	Privileged mode

1.39 QinQ

1.39.1 Qinq introduction

The port QinQ feature provided by the device is a simple and flexible two-layer VPN technology. It encapsulates the outer VLAN tag for the user's private network message on the operator's network edge device, so that the message carries the two-layer VLAN tag through the operator's backbone network (public network). In the public network, the device only forwards the message according to the outer VLAN tag, and learns the source MAC address table item of the message into the MAC address table of the VLAN where the outer tag is located, while the user's private VLAN tag will be transmitted as the data part of the message in the transmission process.

QinQ feature enables operators to use one VLAN to serve user networks with multiple VLANs. As shown in the figure below, the private VLAN of user network a is VLAN 1 ~ 10, and the private VLAN of user network B is VLAN 1 ~ 20. The VLAN assigned by the operator to user network a is VLAN 3, and the VLAN assigned to user network B is VLAN 4. When the message with VLAN tag of user network a enters the operator's network, a layer of VLAN tag with VLAN ID 3 will be encapsulated outside the message; When the message of VLAN tag 4 of the operator enters the network with the tag ID of VLAN B. In this way, the messages of different user networks are completely separated during public network transmission. Even if the VLAN ranges of the two user networks overlap, there will be no confusion during public network transmission。



The QinQ feature enables the network to provide 4094x4094 VLANs at most, which meets the demand of man for the number of VLANs. It mainly solves the following problems

(1) Alleviate the increasingly scarce public network VLAN ID resources.

(2) Users can plan their own private VLAN ID, which will not conflict with the public VLAN ID.

(3) It provides a relatively simple two-layer VPN solution for small man or enterprise network.

QinQ can be divided into two types: basic QinQ and flexible QinQ.

(1) Basic QinQ: basic QinQ is implemented based on port mode. After opening the basic QinQ function of the port, when the port receives a message, the device will mark the VLAN tag of the default VLAN of the port for the message. If a message with VLAN tag is received, the message will become a double tag message; If a message without VLAN tag is received, it will become a message with port default VLAN tag.

(2) Flexible QinQ: flexible QinQ is a more flexible implementation of QinQ, which is based on the combination of port and VLAN. In addition to realizing all basic functions of QinQ, messages received at the same port can also take different actions according to different VLANs, and add different outer VLAN tags to messages with different inner VLAN IDs。

1.39.2 Qinq configuration

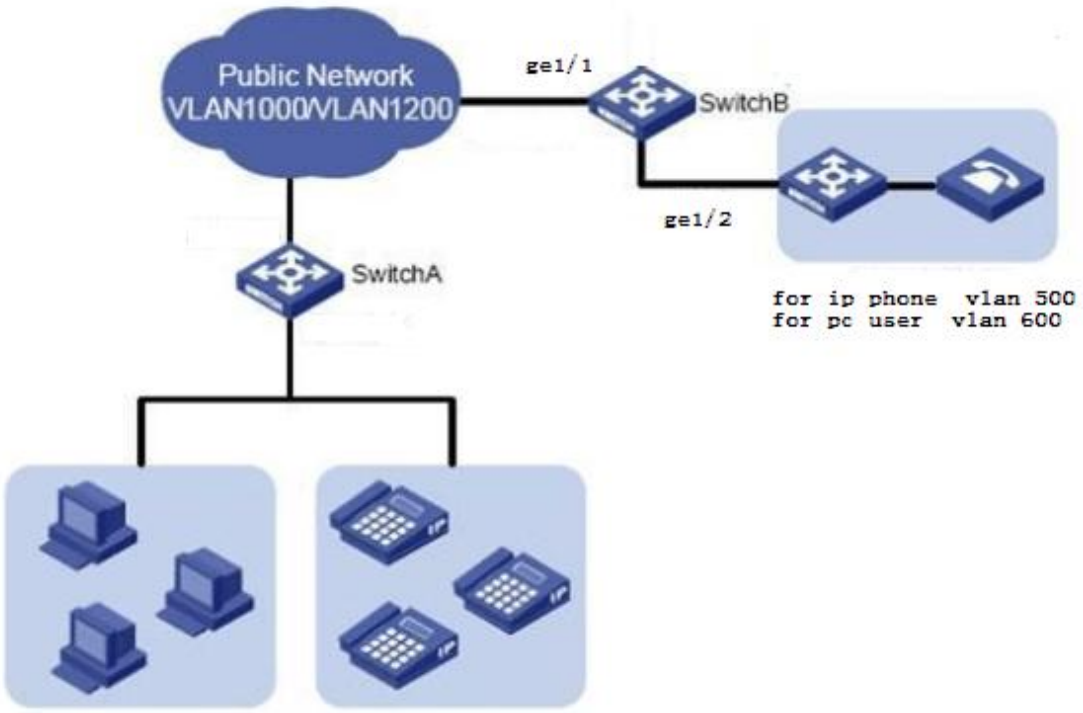
Command	Description	CLI mode
qinq tpid WORD	The default value carried in the VLAN is 0xtpid 8100	Interface configuration mode
no qinq tpid	Restore port default TPID	Interface configuration mode
qinq uplink	Configure the port as an uplink port	Interface configuration mode
no qinq uplink	Unlink port configuration	Interface configuration mode
qinq customer	Configure the port as customer port	Interface configuration mode
no qinq customer	Cancel customer configuration of port	Interface configuration mode
qinq outer-vid <1-4094> inner-vid VLAN_ID	Configure a VLAN conversion of the interface	Interface configuration mode
no qinq outer-vid <1-4094> [inner-vid VLAN_ID]	Delete a VLAN conversion of the interface	Interface configuration mode
show qinq	Displays the QinQ status of all configurations	Privileged mode

1.39.3 Qinq configuration

Port GE1 / 1 of switchb is connected to the public network, and port GE1 / 2 is connected to the PC and telephone server. The VLAN used by the PC is 600 and the VLAN used by the IP phone is 500. VLAN 100 and VLAN 200 messages are allowed to pass through the public network. In order to make the user data of the PC transmitted on the public network

through VLAN 200, the data of the IP phone is transmitted on the public network through VLAN 100.

The networking diagram is as follows:



The configuration of switch B is as follows：

Switch#con t

Switch(config)#vlan da

Switch(config-vlan)#vlan 100

Switch(config-vlan)#vlan 200

Switch(config-vlan)#exit

Switch(config)#int ge1/1

Switch(config-ge1/1)#sw mod tr

Switch(config-ge1/1)#switchport trunk allowed vlan add 100

Switch(config-ge1/1)#switchport trunk allowed vlan add 200

Switch(config-ge1/1)#qinq uplink

Switch(config-ge1/1)#int ge1/2

Switch(config-ge1/2)#switchport mode hybrid

Switch(config-ge1/2)#switchport hybrid allowed vlan add 100 egress-tagged dis

Switch(config-ge1/2)#switchport hybrid allowed vlan add 200 egress-tagged dis

Switch(config-ge1/2)#qinq customer

```
Switch(config-ge1/2)#qinq outer-vid 100 inner-vid 500
Switch(config-ge1/2)#qinq outer-vid 200 inner-vid 600
Switch(config-ge1/2)#
```

```
Switch#show qinq
ifname      tpid      dtag-mode      outer-vid      inner-vid
ge1/1       0x8100    uplink           -              -
ge1/2       0x8100    customer         100            500
ge1/2       0x8100    customer         200            600
Switch#
```

Configure QoS

This chapter describes QoS and its configuration, mainly including the following contents：

- QoS introduction
- QoS configuration
- QoS configutation example

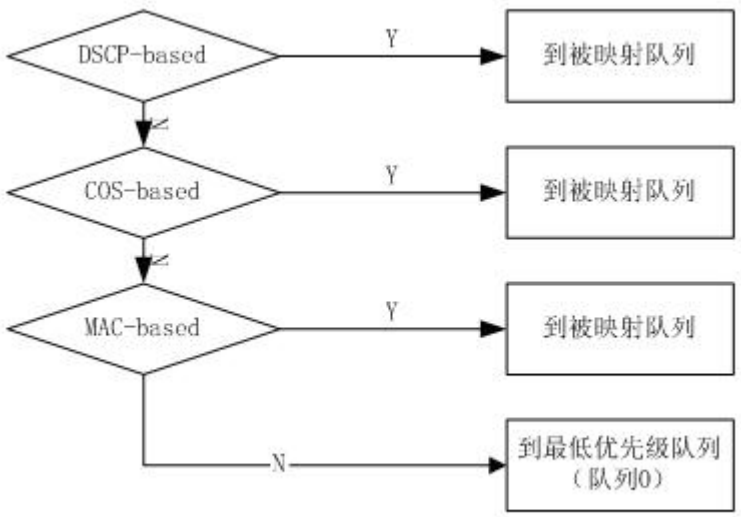
1.40 QoS Introduction

Using the QoS function of the switch, you can give priority to the important data streams forwarded through the switch, make the bandwidth utilization of your network more reasonable and the network performance more predictable.

In the switch, the queue of the data packet at the output end is determined according to the priority information of the data packet at the input end.

The switch realizes QoS based on cos (802.1p), QoS based on DSCP (DiffServ) and QoS based on Mac. DSCP based QoS can be configured on one physical port; The physical ports start cos based QoS by default. The MAC based QoS function is configured in the MAC binding function. Each physical port can only be configured with one QoS function.

The following figure shows the packet forwarding process with QoS enabled：



The switch supports eight priority queues from 0 to 7. Queue 7 has the highest priority and queue 0 has the lowest priority. There are four scheduling modes of priority queue: SP, RR, WRR and wdrr. SP is a strict priority scheduling, that is, it always forwards the packets of queue 7 first. It does not start forwarding the packets of queue 6 until the packets of queue 7 are forwarded. It does not forward the packets of queue 5 until the packets of queue 6 are forwarded. Finally, it forwards the packets of queue 0. RR is a polling scheduling method. When forwarding packets, the switch polls and forwards packets from high priority queue to low priority queue, and each queue forwards one packet. WRR refers to weighted priority polling. When forwarding packets, the switch polls and forwards packets from the high priority queue to the low priority queue according to the weight configuration. First, the packets with the number of weights are forwarded from the high priority queue, and then the packets with the number of weights of the next high priority are forwarded until the lowest priority queue is forwarded, and then the packets are forwarded from the high priority queue. Wdrr is a weighted arrears polling scheduling method, that is, if the weight of queue 3 is 4, it can forward 5 packets in one round, while in the next round, it can only forward 3 packets. This flexible adaptability is more suitable for highly aggregated network environment.

In order to facilitate user configuration, we introduce the concept of qosprofile. Qosprofile is an attribute that configures the mapping relationship between 802.1p and priority queue. This attribute cannot be configured by users. Their mapping relationship is shown in the following table:

QosProfile	802.1p(CoS) value	Priority queue
Qp0	0	0
Qp1	1	1
Qp2	2	2
Qp3	3	3
Qp4	4	4
Qp5	5	5
Qp6	6	6
Qp7	7	7

1.40.1 QoS based on cos

Cos based QoS is enabled on the port by default. The exchange opportunity obtains the priority value of VLAN tag in the packet entering the port, and determines the output queue of the packet according to the mapping relationship between the user configured cos value and the queue. If the packet has no VLAN tag or the vid of VLAN tag is 0, the switch will fill the packet according to the default vid of the port configured by the user and the default priority of the port, and then determine the output queue of the packet according to the default priority。

1.40.2 QoS based on DSCP

If a port enables DSCP based QoS, the exchange opportunity obtains the DSCP value in the IP packet entering the port, and determines the output queue of the packet according to the mapping relationship between the user configured DSCP value and the queue。

1.40.3 Mac based QoS

When a packet enters the switch, the switch will look up the layer-2 forwarding table of the switch according to the destination MAC of the packet and the vid of the packet VLAN tag. If a target table entry is found, the output queue of the packet will be

determined according to the queue mapping relationship configured by the target table entry。

1.40.4 Policy based QoS

QoS policies include classes, policies, and actions. Class is used to identify the flow. Users can define a series of rules through commands to classify data packets; The policy action is used to define the QoS action of the message matching the rule. If policy based QoS is enabled for a port, the switch will classify the data packets entering the port. For the data packets that meet the classification requirements, the switch will process the data packets of the port according to the corresponding policy actions. For the data packets that do not meet the classification requirements, it will not process them, and then determine the output queue of the data packet according to the priority mapping relationship。

1.41 QoS configuration

1.41.1 QoS default configuration

Configuration item	Value	Configurable
Number of queues	8	N
Scheduling mode	WRR	Y
Enable SP scheduling mode	disable	Y
Enable RR scheduling mode	disable	Y
Whether to enable wdrr scheduling mode	disable	Y
Queue weight	QP0[1],QP1[2],QP2[4],QP3[8] QP4[16],QP5[32],QP6[64] QP7[127]	Y
Mapping relationship between COS and qosprofile	COS0~ [qp0] COS1~ [qp1] COS2~ [qp2] COS3~ [qp3] COS4~ [qp4] COS5~ [qp5] COS6~ [qp6] COS7~ [qp7]	N

Mapping relationship between DSCP and qosprofile	DSCP0~DSCP7[qp0] DSCP8~DSCP15[qp1] DSCP16~DSCP23[qp2] DSCP24~DSCP31[qp3] DSCP32~DSCP39[qp4] DSCP40~DSCP47[qp5] DSCP48~DSCP55[qp6] DSCP56~DSCP63[qp7]	Y
Does the interface enable DSCP based QoS	disable	Y
Does the interface enable cos based QoS	enable	N
Interface user priority (COS value)	0	Y

1.41.2 Configure scheduling mode

The default scheduling mode of the switch is WRR. SP, RR and wdrr scheduling modes can be configured through commands。

Command	Description	CLI mode
qos sched {rr | sp | wrr | wdrr}	Configure QoS scheduling mode	Interface configuration mode

1.41.3 Configure queue weights

Command	Description	CLI mode
qos qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7} weight<1-127>	Configure the weight of each priority queue	Interface configuration mode
no qos qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7} weight	The weight of the recovery queue is configured as the default	Interface configuration mode

Queue weight refers to the number of packets forwarded by the priority queue during a polling forwarding. Therefore, when configuring the queue weight, it should be noted

that the weight of the low priority queue should not exceed the weight of the high priority queue。

1.41.4 Configure the mapping relationship between DSCP and qosprofile

Command	Description	CLI mode
qos dsc-map-qp <0-63> qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7}	Configure the mapping relationship between DSCP and qosprofile.	Interface configuration mode
no qos qosprofile {qp0|qp1|qp2|qp3| qp4|qp5|qp6|qp7} weight	Restore the mapping relationship between DSCP and qosprofile to the default configuration.	Interface configuration mode

1.41.5 Configure port QoS based on DSCP

QoS function can only be configured on physical port, not trunk or layer 3 interface。

Command	Description	CLI mode
qos dscp-based	Enable the QoS function of port based on DSCP.	Interface configuration mode
no qos dscp-based	Turn off the DSCP based QoS function of the port.	Interface configuration mode

1.41.6 Configure port user priority (COS value)

Command	Description	CLI mode
qos user-priority <0-7>	Configure the user priority of the port (COS value)	Interface configuration mode
no qos user-priority	The user priority (COS	Interface

	value) of the recovery port is the default configuration.	configuration mode

1.42 QoS configuration example

Configure the GE1 / 3 user priority (COS value) to 3, and the cos based QoS function starts by default：

Switch#configure terminal

Switch#(config)#interface ge1/3

Switch#(config-ge1/3)#qos user-priority 3

Switch#(config-ge1/3)#end

Configure interface GE1 / 3 to start the QoS function based on DSCP, and DSCP value 3 is mapped to priority queue 2：

Switch#configure terminal

Switch#(config)#interface ge1/3

Switch#(config-ge1/3)#qos dscp-map-qp 3 qosprofile qp2

Switch#(config-ge1/3)#qos dscp-based

Switch#(config-ge1/3)#end

1.43 Policy QoS configuration example

Configure ACL to capture the data flow of source Mac1, mac2 and mac3 respectively

(ACL rules can be modified as required. Here is just a simple example)

access-list 700 permit host 0000.0000.1111 vid any ip any any

access-list 701 permit host 0000.0000.2222 vid any ip any any

access-list 702 permit host 0000.0000.3333 vid any ip any any

Configure QoS classes to match the data streams of source Mac1, mac2 and mac3 respectively

(the matching rule cos or DSCP can be modified as required. Here is just a simple example)

qos class 10 match acl 700

qos class 11 match acl 701

qos class 12 match acl 702

Configure QoS policy and re label the 802.1p priority of data streams with sources of Mac1, mac2 and mac3 respectively

(the strategy can be modified according to the requirements. Here is just a simple example)

```
qos policy 10 class 10 remark cos 7
qos policy 10 class 11 remark cos 5
qos policy 10 class 12 remark cos 3
Issue QoS policy to port
interface ge1/2
 qos apply-policy 10
```

Configure MSTP

This chapter describes MSTP and its configuration, mainly including the following contents：

- MSTP introduction
- MSTP configuration
- MSTP configuration example

1.44 MSTP introduction

The switch supports IEEE802 1d,IEEE802. 1w，IEEE802. 1s standard STP protocol。

1.44.1 summary

MSTP uses RSTP to converge quickly, so that multiple VLANs are aggregated into a spanning tree instance, and each instance has a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data flow, can load balance, and reduce spanning tree instances required to support a large number of VLANs.

1.44.2 Multi spanning tree domain

For instances participating in multi spanning tree (MST) calculation, the same MST configuration information of the switch must be configured consistently. Connected switch sets with the same MST configuration constitute the MST domain.

MST configuration determines the domain to which each switch belongs. Configuration includes domain name, revision number, MST instance and VLAN assignment mapping; This information will generate a unique digest in the MST configuration. The summaries in the same domain are the same and must be the same. You can view these information through the show spanning tree MST config command.

A domain can have one or more members with the same MST configuration; Each member must have the ability to handle RSTP BPDU. There is no limit to the number of MST domains in a network, but each domain supports up to 16 instances. You can only assign one VLAN to one spanning tree instance at a time

1.44.3 IST, CIST, and CST

Internal spanning tree (IST), a spanning tree running in the MST domain.

In each MST domain, MSTP maintains multiple generated instances. Instance 0 is a special instance of a domain, which is called ist. All other MST instances are numbers 1 through 15.

This ist is just a spanning tree instance that receives and sends BPDU; All other spanning tree instance information is compressed in MSTI BPDU. Because MSTI BPDU carries the information of all instances, it needs to be processed by a switch that supports

multiple spanning tree instances. The number of BPDUs means simplification.

All MST instances in the same domain share the same protocol timer, but each MST instance has its own topology parameters, such as a root switch ID, root path cost, etc. By default, all VLANs are assigned to ist.

The common and internal spanning tree (CIST) is the collection of all ist in each MST domain and the common spanning tree (connecting the MST domain and a single spanning tree).

The spanning tree computed within a domain looks like a subtree of the CST that contains all switch domains. CIST is formed by the results of spanning tree calculation run between switches supporting 802.1w and 802.1d protocols. CIST in MST domain is the same as CST outside the domain

Common spanning tree (CST), a spanning tree running between MST domains。

1.44.4 Intra domain operation

Ist connects all MSTP switches in a domain. When ist converges, the root of ist becomes ist master, which is the switch with the lowest bridge ID and path overhead to CST root in the domain. If there is only one domain in the network, the ist master is also the CST root. If the CST root is outside the domain, an MSTP switch at the boundary of the domain is selected as the ist master.

When an MSTP switch is initialized, it sends BPDU to request it to act as CST root and ist master, and the path cost to CST root and ist master is set to 0. The switch also initializes all MST instances and requests to be their root. If the MST root information received by the switch takes precedence over the information stored in the current port (low bridge ID, low path cost, etc.), it gives up its requirement to become an ist master.

During initialization, a domain may have many subdomains, each with its own ist master. When the switch receives a higher priority ist message, it leaves its old sub domain and joins a new sub domain that may contain the real ist master. Therefore, all subdomains shrink, except those containing the real ist master.

In order to operate correctly, all switches in MST domain must recognize the same ist master. Therefore, switches in any two domains synchronize the role of the port of one of their MST instances, only if they converge to a public ist master.

1.44.5 Inter domain operation

If there are multiple domains or early 802.1d switches in the network, MSTP establishes and maintains CST, which includes MST domains in all networks and all early STP switches. MST instances join ist at the domain boundary to become CST

Ist connects all switches in MSTP domain and looks like a subtree of CST (surrounding all switch domains). The root of the subtree becomes ist master. MST domain looks like a virtual switch, adjacent to STP switch and MST domain.

Only CST instances send and receive BPDU, and MST instances add their spanning tree information to BPDU, interact with neighbor switches and calculate the final spanning tree topology. Because of this, the spanning tree parameters related to BPDU transmission (such as hello time, forward time, Max age and Max hops) are configured only in CST instances, but do not affect all MST instances. Parameters related to spanning tree topology (such as switch priority, port VLAN cost, port VLAN priority) can be configured in CST instances and MST instances.

MSTP switches use version 3 RSTP BPDU or 802.1d BPDU to communicate with 802.1d switches. MSTP switch uses MSTP BPDU to communicate with MSTP switch。

1.44.6 Skip count

In the BPDU that configures the calculation spanning tree topology, ist and MST instances do not use message age and maximum age information. Instead, use the path cost to the root and the hop count mechanism equivalent to IP TTL.

You can configure the maximum number of hops in that domain and apply it to ist and all MST instances in that domain. The implementation of hop count calculation is the same as that of message age (determined after triggering a reconfiguration). The instance root switch always sends a BPDU (or-m-record) with cost of 0 and hop count of the maximum value. When a switch receives a BPDU, it subtracts the remaining hops by 1 and propagates the remaining hops in the BPDU it generates. When the count reaches 0, the switch discards the BPDU and updates the port information.

In a domain, the message age and maximum age information in the RSTP BPDU part remain the same, and the same value is propagated at the specified port of the domain at the boundary。

1.44.7 Boundary port

The boundary port is a spanning tree domain that connects the MST domain to a separate RSTP running spanning tree domain, or a separate 801.1d spanning tree domain, or other MST domains with different configurations. A border port is also connected to a LAN. The designated switch of the LAN is either a separate spanning tree switch or a switch with different MST domain configurations.

In the boundary port, the role of MST port is not important, and their state is forced to be the same as that of ist port (when ist port is forwarding, MST port at the boundary is forwarding). An ist port at the boundary can have any role other than the backup port.

In a shared boundary connection, the MST port waits for the forward delay time to expire in the blocking state before switching to the learning state. MST port waits for another forward delay time to expire before switching to forwarding.

If the boundary port is a point-to-point connection and is the ist root port, the MST port will switch to the forwarding state as soon as the ist port changes to the forwarding state.

If a boundary port transitions to the forwarding state in the instance, it is forwarding in all instances, and a topology change is triggered. If a boundary port with ist root or specified port role receives a topology change notification, the ist instance and all MST instances on the active port of MSTP switch trigger a topology change.

1.44.8 Interoperability between MSTP and 802.1d STP

A switch running MSTP supports a built-in protocol migration mechanism, which enables it to be used in coordination with 802.1d. If the switch receives an 802.1d configured BPDU from a port, it sends an 802.1d BPDU at that port. When the boundary port of a domain receives an 802.1d BPDU, an MSTP BPDU or an RSTP BPDU of a different domain, the MSTP switch can detect it.

However, if the switch no longer receives 802.1d BPDU, it will not automatically return to MSTP mode because it cannot determine whether the other party's switch has been deleted from the connection unless the other party's switch is a designated switch. Similarly, when the switch connected to the switch has joined the domain, the switch may continue to assign a boundary port role to a port. Restart the migration processing of the protocol (force negotiation with the neighbor switch).

If all the switches of the connected party are RSTP switches, they can handle MSTP BPDU and RSTP BPDU. Therefore, MSTP switches either send a version 0 configuration and TCN BPDU or a version 3 MSTP BPDU at the boundary port. For a boundary port connected to the LAN, its designated switch is either a separate spanning tree switch or a switch with different MST configuration。

1.44.9 Port role

MSTP adopts the fast convergence algorithm of RSTP. The following is a brief introduction to MSTP port roles and fast convergence in combination with RSTP.

RSTP provides fast convergence for specifying port roles and determining active topology. RSTP is based on IEEE802 On the 1D STP, select the high priority switch as the root switch. When RSTP specifies a port role to a port:

Root port - provides optimal path cost when the switch forwards packets to the root switch.

Designed port - connect to the designated switch. When forwarding packets from LAN to root switch, it produces the lowest path cost. The port through which the specified switch connects to the LAN is called the specified port.

Alternate port - provides an alternative path from the current root port to the root switch.

Backup port - acts as a backup of the path from the specified port to the spanning tree leaf. A backup port exists only when two ports are connected together in a point-to-point loop or when two or more of a switch are connected to a shared LAN segment.

Disable port - there is no port role in the spanning tree operation.

Master port - located at the domain root or the shortest path to the total root. It is the port connecting the domain to the total root.

The root port or specified port role is included in the active topology. The replacement port or backup port role is not included in the active topology.

In the whole network with a stable topology and fixed port role, RSTP ensures that each root port and specified port are immediately migrated to the forwarding state when all replacement ports and backup ports are always in the discarding state. Port status controls forwarding and learning processing.

Fast convergence

RSTP provides fast recovery in the following cases: switch failure, port failure or LAN failure. It provides fast recovery for edge ports, new root ports and connections to a point-to-point connection:

Edge Ports - if you configure a port as an edge port, the edge port will immediately migrate to the forwarding state. You can open it as a boundary port only when this port is connected to a separate terminal or on a device that does not need to calculate the spanning tree.

Root Ports - if RSTP selects a new root port. It blocks an old root port and immediately migrates the new root port to the forwarding state.

Point to point links - if you connect a port to other ports through a point-to-point

connection and the local port becomes a designated port, it and other ports negotiate a fast migration through a proposal agreement handshake to determine a fast convergence loop free topology

Topology change

This section describes the differences between RSTP and 802.1d in dealing with spaning tree topology changes.

Detection - unlike 802.1d, any migration between blocking and forwarding states will cause topology changes. Only migration from blocking to forwarding state will cause RSTP topology changes (topology changes are considered only to increase connectivity). Changing the state of an edge port will not cause topology changes. When an RSTP switch detects a topology modification, it floods and learns information to all non edge ports except the port receiving TC information.

Notification - unlike 802.1d, which uses TCN BPDU, RSTP does not use it. However, for interoperability with 802.1d, the RSTP switch processes and generates TCP BPDU.

Acknowledgement - when an RSTP switch receives a TCN message from an 802.1d switch at the specified port, it responds to a BPDU with 802.1d and sets the TCA flag bit. However, if the TC while timer (the same as the topology change timer of 802.1d) is active, connect to the 802.1d switch at the root port and receive a configuration BPDU with TCA, the TC while timer will restart (reset). This behavior is only required to support 802.1d switches. RSTP BPDU never has TCA flag bit.

Propagation - when an RSTP switch receives a TC message from other switches through a specified port or root port, it propagates to all non edge ports, specified ports and root ports (except the receiving port). All such ports of the switch start the TC while timer and flood the information they have learned.

Protocol migration - in order to be backward compatible with 802.1d switches, RSTP selectively sends 802.1d configuration BPDU and TCN BPDU based on each port.

When a has been initialized, the migrate delay timer starts (specify the minimum value during the period when RSTP BPDU is sent), and RSTP BPDU is sent. When this timer is active, the switch processes all BPDUs received from the port and ignores the protocol type.

After the migration delay timer of the port has been aborted, if the switch receives an 802.1d BPDU, it assumes that it is connected to an 802.1d switch and starts using the 802.1d protocol BPDU. However, if the RSTP switch is using 802.1d BPDU on a port and receives an RSTP BPDU after the timer aborts, the port will restart the timer and start using the RSTP BPDU

1.44.10 802.1D Introduction to spanning tree

The spanning tree protocol is based on the following points:

1) A unique group address (01-80-c2-00-00-00) identifies all switches on a particular LAN. This group address can be recognized by all switches;

2) Each switch has a unique identifier;

3) The port of each switch has a unique port identifier. To manage the configuration of spanning tree, we also need to coordinate a relative priority for each switch; Coordinate a relative priority for each port of each switch; The cost of coordinating a path for each port.

The switch with the highest priority is called the root switch. Each switch port has a root path cost, which is the sum of the path costs of each network segment from the switch to the root switch. The port with the lowest root path cost in a switch is called the root port. If multiple ports have the same root path cost, the port with the highest priority is the root port.

In each LAN, there is a switch called a designated switch, which belongs to the switch with the least root path cost in the LAN. The port connecting the LAN and the designated switch is the designated port of the LAN. If more than two ports in the specified switch are connected to this LAN, the port with the highest priority is selected as the specified port.

Elements of decisions necessary to form a spanning tree:

1) Determine root switch

a. At first, all switches thought they were root switches;

b. The switch sends the configuration BPDU to the LAN broadcast connected to it, and its root_ ID and Bridge_ The value of ID is the same;

c. When the switch receives the configuration BPDU from another switch, if it finds root in the received configuration BPDU_ The value of the ID field is greater than the root in the switch_ If the value of the ID parameter, the frame will be discarded, otherwise the root of the switch will be updated_ ID, root path cost root_ path_ Cost and other parameters, the switch will continue to broadcast and send the configuration BPDU with the new value.

2) Determine root port

The port with the lowest root path cost in a switch is called the root port.

If multiple ports have the same lowest root path cost, the port with the highest priority is the root port. If two or more ports have the same lowest root path cost and highest priority, the port with the lowest port number is the default root port.

3) Designated switch for LAN

a. At the beginning, all switches consider themselves the designated switches of the LAN.

b. When the switch receives BPDU from other switches (in the same LAN) with lower root path cost, the switch will no longer claim to be the designated switch. If two or more switches in a LAN have the same root path cost, the switch with the highest priority is selected as the specified switch.

c. If the designated switch receives a configuration BPDU sent by other switches on the LAN competing with the designated switch at a certain time, the designated switch will send a response configuration BPDU to redefine the designated switch.

4) Determine the specified port

The port connected to the LAN in the specified switch of the LAN is the specified port. If the specified switch has two or more ports connected to the LAN, the port with the lowest identification is the specified port.

Except for the root port and the specified port, all other ports will be set to blocking state. In this way, after determining the root switch, the root port of the switch, and the designated switch and designated port of each LAN, the topology of a spanning tree is also determined。

1.45 MSTP configuration

1.45.1 Default configuration

Command parameters	Default value
spanning-tree mst enable(start mstp)	off
Spanning-tree mst priority(Switch CIST priority)	32768
spanning-tree mst hello-time(Switch cist hello-time)	2 seconds
spanning-tree mst forward-time(Switch cist forward-time)	15 seconds
spanning-tree mst max-age(Switch cist max-age)	20 seconds
spanning-tree mst max-hops(Switch cist max-hops)	20 seconds
instance 1 priority (Priority instance)	32768
spanning-tree mst instance 1 priority(Port instance priority)	128
spanning-tree mst instance 1 path-cost(Port instance path-cost)	20000000
spanning-tree mst priority （Port cist priority）	128
spanning-tree mst path-cost (Port cist path-cost）	20000000

1.45.2 General configuration

Start MSTP

MSTP is off by default when the system is started.

The configuration process of starting MSTP is:

Switch#configure terminal

Switch(config)#spanning-tree mst enable

The command to turn off MSTP is:

Switch#configure terminal

Switch(config)#no spanning-tree mst

Configure Max age

Configure Max age is the configuration of all instances. Max age is the number of seconds that the switch waits to receive spanning tree configuration information before triggering a reconfiguration.

The default configuration is 20 seconds, and the configuration range is 6 to 40 seconds.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst max-age <seconds>

Configure Max hops

Max hops is the number of hops specified in a domain before the BPDU is discarded.

The default value is 20 and the configuration range is 1 to 40.

Configuration process：

Switch#configure terminal

Switch(config)#spanning-tree mst max-hops <hop-count>

Configure forward time

Configure forward time for all instances. Forward time is the number of seconds the port waits from discarding to learning and from learning to forwarding.

The default configuration is 15 seconds, and the configuration range is 4 to 30 seconds. According to the generated number protocol, the forward time must meet the following conditions: 2 * (forward time – 1) > = max age.

Configuration process：

Switch#configure terminal

Switch(config)#spanning-tree mst forward-time <seconds>

Configure Hello time

Configuring Hello time is the configuration of all instances. Hello time is the interval between the generation of configuration information by the root switch.

The default configuration time is 2 seconds, and the configuration range is 1 to 10 seconds. According to the generated number protocol, hello time must meet the following conditions: 2 * (Hello time + 1) = max age.

Configuration process:

Switch#configure terminal

Switch(config)# spanning-tree mst hello-time <seconds>

Configure the priority of CIST Bridge

Default configuration 32768, configuration range < 0-61440 >; CIST priority can only be a multiple of 4096.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst priority <priority>

Configuration compatible with Cisco

The network switch adopts the MSTP protocol based on 802.1s, and the length of each MSTI message is 16 bytes; The length of each MSTI message of BPDU of Cisco switch is 26 bytes. In order to interoperate with Cisco switches, switch compatible with Cisco shall be started when configuring switches of the network.

When starting the Cisco compatible configuration, when judging whether it is the same domain, as long as the domain name and revision number are the same, it is considered to be the same domain.

The default system does not start this function.

Turn on Cisco compatible:

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability enable

Turn off Cisco compatibility:

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability disable

Reset protocol check task

In order to be compatible with 802.1d STP protocol, the system can automatically detect the protocol of the other system. The protocol running on this port is determined according to the protocol running on the other side.

In some cases, reset the protocol. For example, after negotiation, the system runs STP protocol on one port, and after a period of time, the other party's equipment running STP protocol has been replaced by a host. At this time, I need to configure this port as fast port, but the port has run STP protocol, and the task of protocol negotiation has stopped;

At this time, you need to reset the task of protocol negotiation and let it renegotiate the protocol between it and the host.

Reset the protocol reconnaissance task of the whole equipment:

Switch#clear spanning-tree detected protocols

Reset the protocol reconnaissance task of a port：

Switch#clear spanning-tree detected protocols interface <if-name>

1.45.3 Domain configuration

If two or more devices are in the same domain, they must have the same VLAN instance mapping relationship, the same modified version number and the same domain name.

A domain has one or more members with the same MST configuration, and each member can handle RSTP BPDUs capabilities. There is no limit to the number of members in a network, but each domain can support up to 16 instances.

The configuration of instances is described in "instance configuration". Only domain name configuration and revision number configuration are introduced here。

Configure domain name：

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#region <region-name>

Configuration revision number：

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)# revision <revision-num>

1.45.4 Instance configuration

The system supports 16 instances, and the range of instance ID number is 0-15. A VLAN can only be assigned to one spanning tree instance at a time.

By default, there is only one instance 0, and all VLANs belong to this instance.

The process of configuring an instance:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#instance <instance-id> vlan <vlan-id>

Configure the priority of MSTI Bridge

Default configuration 32768, configuration range < 0-61440 >; MSTI priority can only

be a multiple of 4096.

Configuration process：

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#instance <instance-id> priority <priority>

1.45.5 port configuration

The following describes the port configuration information related to MSTP. Only the simple configuration part is introduced here. Port fast and root guard will be introduced separately later.

The process of configuring a port to join an instance：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id>

Configure the priority of the CIST port

The default configuration is 128, the configuration range is < 0-240 >, and the priority value of CIST port can only be a multiple of 16.

Configuration process：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst priority <priority>

Configure the priority of MSTI port

The default configuration is 128. The configuration range is < 0-240 >. The priority value of MSTI port can only be a multiple of 16.

Configuration process：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id> priority <priority>

Configure path cost of CIST port

The default configuration is 20000000, and the configuration range is 1-200000000. The following is the bandwidth and path cost mapping table：

bandwidth (bps)	Path cost
100,000(100K)	200000000
1,000,000(1M)	20000000
10,000,000(10M)	2000000
100,000,000(100M)	200000
1,000,000,000(1G)	20000
10,000,000,000(10G)	2000
100,000,000,000(100G)	200
1,000,000,000,000(1T)	20
>1000000000000	2

Configuration processSwitch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst path <path-cost>

Configure path cost of MSTI por

The default configuration is 20000000, and the configuration range is 1-200000000. The bandwidth and path costs are the same as those in the table above.

Configuration process

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id> path-cost <path-cost>

Configure the version number of the sending protocol package

The default configuration is to send MSTP protocol packets. The configuration range is 0-3, and the mapping relationship is 0-stp, 2-rstp, 3-mstp

Configuration process：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)# spanning-tree mst force-version <version-id>

Configure connection type

If a port is connected to other ports through point-to-point mode, and the local port becomes a designated port, RSTP negotiates a rapid migration through the proposal agreement process, and the connected port becomes the root port to determine an acyclic topology.

The following is a brief introduction to the negotiation process of the proposal agreement.

When the switch receives a proposal message on one of its ports and that port is selected as the new root port, RSTP forces all other ports to synchronize the new root port information.

If all other ports are synchronized with the superior root information received from the root port, the switch is synchronized.

When RSTP forces it to synchronize new root information, if a specified port is in the forwarding state and is not configured as an edge port, it will migrate to the blocking state. Generally, when RSTP forces a port to synchronize new root messages and the port cannot meet the above conditions, the port state is set to blocking.

When the agreement is sent to the corresponding port of the switch, ensure that all information is sent to the corresponding port of the switch. When switches are connected to a point-to-point connection in agreement with their port roles, RSTP immediately migrates the port status to forwarding.

If it is a shared connection, the state of the port must be determined through the calculation process of 802.1d.

By default, the port connection type is point-to-point.

The connection type of the configuration port is point-to-point connection:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst link-type point-to-point

The connection type of the configuration port is shared connection：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config-ge1/2)#spanning-tree mst link-type shared

1.45.6 PORTFAST Related configuration

1) Port Fast

Port fast immediately transfers an access or trunk port from the blocking state to the forwarding state, bypassing the listening and learning states. You can use port fast to connect a separate workstation and server, which allows these devices to connect to the network immediately without waiting for the spaning tree to converge.

Configure a port as fast port：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast

2) BPDU Filtering

BPDU filtering can be opened globally based on switches or on each port, but their characteristics are different.

In the global layer, you can use the spaning tree MST portfast BPDU filter command to start the BPDU filtering function of the port in the default state of portfast BPDU filter.

In the port layer, you can use spaning tree MST portfast BPDU filter enable to open BPDU filter on any port.

This function prevents the port fast port from receiving or sending BPDUs.

Configure BPDU filtering

In global configuration mode:

Switch#configure terminal

Switch(config)# spanning-tree mst portfast bpdu-filter

In interface configuration mode：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast bpdu-filter enable

3) BPDU Guard

BPDU protection features can be turned on globally in the switch or based on each port, but their characteristics are different.

In the global layer, you can use spaning tree MST portfast BPDU guard to open the BPDU guard function of the port in the portfast BPDU guard default state.

In the port layer, you can open BPDU guard at any port.

When the port configured with BPDU gurad receives BPDU, the spaning tree will shut down this port. In a valid configuration, the port fast enabled port does not receive BPDU. Receiving a BPDU on a port fast enabled indicates an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard enters an error disabled state.

Error disabled means that when the port that starts the BPDU gurad receives the BPDU, if the system configures the error disable mechanism, the error disable timer will be started. Error disable will restart the port after the timeout configured by the system.

In global configuration mode：

Switch#configure terminal

Switch(config)# spanning-tree mst portfast bpdu-guard

In interface configuration mode：

Switch#configure terminal

Switch(config)#interface <if-name>

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

error-disable configuration

Start the error disable mechanism

Switch#configure terminal

Switch(config)#spanning-tree mst errdisable-timeout enable

Configure error disable timeoutSwitch#configure terminal

Switch(config)#spanning-tree mst errdisable-timeout interval <seconds>

1.45.7 Root Guard Related configuration

The layer 2 network of an SP can contain many switches connected to switches that are not their own. In such a topology, the spanning tree can reconfigure itself and select a customer switch as the root switch. You can avoid this by configuring the port of the root guard in the SP switch connected to the switch in the customer network. If the spanning tree calculation causes the port in the customer network to be selected as root port, the root guard configures the port to the root inconsistent (blocked) state to prevent the customer switch from becoming the root switch or the path to the root.

If a switch outside an SP network becomes a root switch, the port is blocked (root inconsistent STAT) and a new root switch is selected in the spanning tree. The customer's switch will not become the root switch and there is no path to the root.

If the switch operates in MST mode, the root guard forces the port to become the specified port. If a boundary port is blocked in ist instance because of root guard, this port is blocked in all MST instances. A boundary port is a port connected to a LAN. The specified switch is either an 802.1d switch or a switch configured in a different MST domain.

When a port is opened, the root guard is applied to all VLANs to which the port belongs. VLANs can be aggregated and mapped to an MST instance.

Configuration process

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst guard root

1.46 MSTP Configuration example

(1) Configuration

The three switches are connected into a ring. It is necessary to open the spanning tree protocol of each switch to avoid the occurrence of the ring. Perform configuration on each switch separately.

Configuration of switch 1：

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable

Configuration of switch 2：

Switch>en

Switch#configure terminal

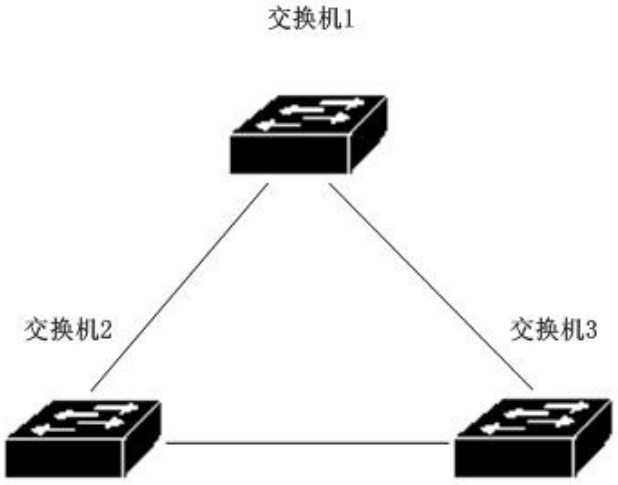
Switch(config)#spanning mst enable

Configuration of switch 3：

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable



(2) Troubleshooting：

Check which switch is selected as the root bridge:

Execute show spanning tree MST and observe that the value of cistroot is the smallest MAC address among the three exchanges, that is, the root election result is correct.

Switch#show spanning-tree mst

To view the port status of the switch in the spanning tree:

Execute the command show spanning tree MST interface GE1 / 1 and observe the state value of port GE1 / 1 in instance 0Switch#show spanning-tree mst interface ge1/1

EAPS configuration

This chapter describes EAPs and its configuration, mainly including the following contents：

- EAPS introduction
- EAPS Basic concepts
- EAPS Protocol introduction
- EAPS configuration
- Restrictions
- Configuration example

1.47 EAPS introduction

EAPs is the abbreviation of Ethernet automatic protection switching. EAPs uses standard Ethernet and VLAN technology to provide loop topology and loop recovery mechanism. In case of failure in the ring, EAPs has the ability to resume data communication within 1 second. The number of nodes running in EAPs is not limited, and the recovery time of EAPs is not limited. EAPs does not rely on other devices, that is, there can be devices in the EAPs ring that do not support EAPs protocol。

1.48 EAPS Basic concepts

Here are some basic concepts involved in EAPs:

1. EAPs domain: in a network, an EAPs domain runs in a separate ring. It is a series of node devices that form a separate loop. An EAPs domain includes a master node and one or more transit nodes.

2. A master node is a switch running EAPs or an EAPs node device. An EAPs domain has only one master node.

3. Transit node, a switch running EAPs or an EAPs node device, is a node other than the master node in an EAPs domain.

4. Primary port: the port connecting EAPs node devices in an EAPs domain. A node device has and only one primary port in an EAPs domain connected to this ring.

5. Secondary port: a port connecting EAPs node devices in an EAPs domain. A node device has only one secondary port in an EAPs domain connected to this ring.

6. Control VLAN, control VLAN, VLAN responsible for EAPs domain protocol packet transmission. There is only one control VLAN in an EAPs domain.

7. Protected VLAN, protected VLAN, VLAN that transmits business data in EAPs domain. There must be one protected VLAN or more than one protected VLAN in an EAPs domain

1.49 EAPS Protocol introduction

An EAPs domain runs on an EAPs ring. An EAPs domain contains a master node and one or more transit nodes; Each EAPs node contains one same control VLAN and multiple protected VLANs; Each EAPs node contains a primary port and a secondary port

in an EAPs domain. These two ports belong to the control VLAN and all protected VLANs of this ring. Connect all nodes in the EAPs domain through the primary port and secondary port of each EAPs node device to form an EAPs ring.

Under normal circumstances, when all primary ports and secondary ports in the EAPs domain are linked up, block the secondary port of the master node (set the port state of the secondary port to blocking) and eliminate the loop of business data in the EAPs domain. When the EAPs domain fails, immediately open the secondary port of the master node (set the state of the secondary port to forwarding), allow it to forward business data and restore the normal forwarding of business data.

The transit node has no difference in the processing of primary port and secondary port

The following describes two kinds of fault checking and loop recovery of EAPs：

1.49.1 Link-Down Give an alarm

When the transit node finds that its primary port or secondary port has link down, it will immediately send a link-down protocol package from the control VLAN to the master node through another link up port.

When the master node receives the link-down protocol package:

The master node immediately enters the failed state from the complete state, opens the secondary port (set the state of the secondary port to forwarding), refreshes its layer 2 and 3 forwarding, sends a ring-down-flush-fdb to notify EAPs domain of other transits, refreshes its forwarding table, and re learns the layer 2 and 3 forwarding.

When the master node finds that the local primary port has link down, its operation is the same as that of receiving the link-down protocol package.

When the master node finds that the local secondary port has a link down, the master node immediately enters the failed state from the complete state, refreshes its layer 2 and layer 3 forwarding, sends the ring-down-flush-fdb protocol package, and notifies EAPs domain of other transits to refresh its forwarding table and re learn the layer 2 and layer 3 forwarding。

1.49.2 Loop check

The master node will regularly send the health protocol package from the primary port. If the ring is complete, the master node can receive the health protocol package at its secondary port. At this time, the master node will restart its fail period timer, and the state of the master node is complete.

If the health protocol package is not received before the expiration of the fail period, the master node will leave the complete state, enter the failed state, open the secondary port (set the state of the secondary port to forwarding), refresh its layer 2 and layer 3 forwarding, send ring-dsown-flush-fdb to notify EAPs domain of other transits, refresh its forwarding table, and relearn the layer 2 and layer 3 forwarding。

1.49.3 Ring recovery

The master node will send the health protocol package from its primary port no matter whether the ring is complete or failed or otherwise. When the master node is in the failed state, once the health protocol packet is received from its secondary port, the ring will return to the complete state. At this time, the master node will set the state of the secondary port to blocking, refresh its layer 2 and 3 forwarding, and send a ring-up-flush-fdb package to notify other devices to refresh their layer 2 and 3 forwarding and relearn the layer 2 and 3 forwarding.

When the port of the transit node returns from link down to link up and the master node finds that the ring is restored, the secondary port of the master node may still be in the forwarding state. In this case, a temporary ring will be caused. Therefore, when one port of the transit node is in the link up state and the other port of the link down becomes link up, the transit node will enter a "pre forwarding state". In this state, the port of the subsequent link up will also be in the pre forwarding state, which cannot forward business data and interrupt the possible data loop. When the master node recovers and sends the ring-up-flush-fdb, the transit node will switch the node state to the link-up state after receiving the protocol packet, set the port in the pre forwarding state to the forwarding state, and resume the normal forwarding of business data.

If the transit node cannot receive the ring-up-flush-fdb protocol packet, it will set the port in pre forwarding status to forwarding status after double the fail time。

1.49.4 EAPs compatible with extreme

The products of extreme company are the first manufacturers to support EAPs, and the EAPs protocol supported by the switch follows the standard of rfc3619; There are some differences between the EAPs protocol package of extreme device and the protocol package definition of rfc3619. The EAPs protocol supported by the switch is fully compatible with the extreme device, and the compatibility switch is on by default。

1.49.5 More EAPS Domain

The switch can support multiple EAPs domains, a total of 16。

1.50 EAPS configuration

The basic configuration of EAPs protocol includes the following basic elements: control VLAN, node mode, primary port, secondary port, protected VLAN, hello time and fail time. Hello time and fail time are configured by default. Hello time is 1 second and fail timer is 3 seconds。

1.51 Restrictions

1. The primary port must belong to the control VLAN of an EAPs domain and the trunk mode member of all protected VLANs.

2. EAPs protocol cannot run simultaneously with MSTP protocol. If MSTP is started or MSTP instance is configured, EAPs protocol cannot be started.

3. When a VLAN starts the vllp protocol, it cannot be configured as the control VLAN or protected VLAN of EAPs

4. The control VLAN of EAPs can only contain primary port and secondary port, and can only be the trunk mode of VLAN

5. If a VLAN is configured as the control VLAN of EAPs domain and the domain has been started, the VLAN cannot be deleted, and its port members cannot be modified or deleted. Control VLAN cannot be configured with layer 3 interfaces.

6. Primary port and secondary port in protected VLAN can only be trunk mode. Other member ports are not limited.

7. One port can only be configured as the primary port or secondary port of one EAPs domain.

8. The same VLAN can only belong to the control VLAN or protected VLAN of one EAPs domain.

9. The control VLAN of all nodes in an EAPs domain must be the same。

1.52 EAPS Brief introduction of command

To create an EAPs domain, first ensure that the VLAN and port configurations meet the above conditions.

There are certain sequence requirements for configuring EAPs. First, create an EAPs domain. Before starting the EAPs domain, configure other parameters according to the previous requirements; Otherwise, the startup will not succeed. If you want to change Hello time to a value greater than the current fail time, first change the fail time to a larger number; Otherwise, the configuration will not succeed. There are no special requirements for other configuration sequences.

When an EAPs domain has been started, the control VLAN, mode, primary port and secondary port cannot be modified; Protected VLAN, fail timer, hello time, and extreme interoperability can be modified.

The primary port and secondary port support LACP ports (i.e. trunk groups)。

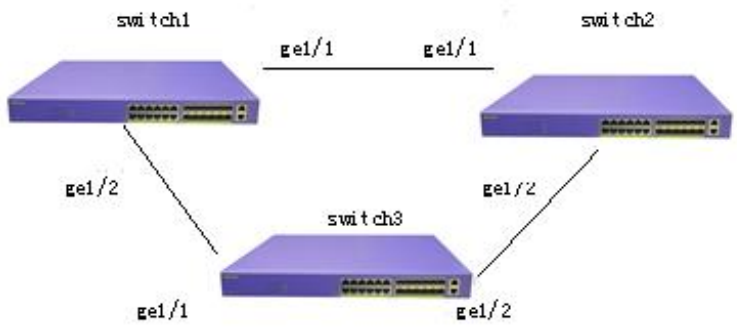
1.52.1 EAPS Configuration command

Command	Description	Mode
eaps create <ring-id>	Create an EAPs domain	Global configuration mode
eaps control-vlan <ring-id> <vlan-id>	Configure a control VLAN of EAPs domain.	Global configuration mode
eaps protected-vlan <ring-id> <vlan-id>	Add a protected VLAN of EAPs domain.	Global configuration mode
eaps mode <ring-id> <master|transit>	Configure the running node mode of an EAPs domain.	Global configuration mode
eaps primary-port <ring-id> <ifname>	Configure the primary port of an EAPs domain.	Global configuration mode
eaps secondary-port <ring-id> <ifname>	Configure a secondary port of EAPs domain.	Global configuration mode
eaps data-span <ring-id>	Configure EAPs ring data cross ring forwarding	Global configuration mode
eaps fail-time <ring-id> <secs>	Configure the timeout time of the fail period timer of an EAPs domain. The default is 3 seconds. The unit is seconds.	Global configuration mode
eaps hello-time <ring-id> <secs>	Configure the time when an EAPs domain sends health packets regularly. The default is 1 second. The unit is seconds. Hello timer must be less than fail time.	Global configuration mode
eaps extreme-interoperability <ring-id> <enable|disable>	Enable or disable compatibility with extreme devices. The default is startup compatibility.	Global configuration mode
eaps enable <ring-id>	Start an EAPs domain	Global

		configuration mode
eaps disable <ring-id>	Close an EAPs domain	Global configuration mode
show eaps	Displays the information of EAPs domain started in the system	Normal mode / privileged mode
Show eaps <ring-id>	Displays the details of an eapsdomain	Normal mode / privileged mode

1.53 Single ring configuration example

There are three switches, Switch1, switch2 and switch3. VLAN 1 will not form a loop during traffic forwarding through EAPs protocol. At the same time, it is guaranteed to enable the standby link when one link between Switch1, switch2 and switch3 is disconnected. According to the above requirements, Switch1 can be configured as master mode; Configure switch2 and switch3 to transit mode. Add a control VLAN VLAN 2 for protocol packet transmission。



Switch1 configuration:

Switch1 is configured as the master of EAPs domain ring 1. The control VLAN is VLAN 2, the protected VLAN is VLAN 1, the primary port is GE1 / 1, and the secondary port is GE1 / 2. Other configurations adopt default values。

Switch#configure terminal

#Add VLANs 2 and 3

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-3

Switch(config-vlan)#exit

#Configure GE1 / 1 as a trunk member of VLAN 1 and VLAN 2。

```
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk native vlan 3
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2
```

#Configure GE1 / 2 as a trunk member of VLAN 1 and VLAN 2。

```
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk native vlan 3
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan
 VLAN   Name         State        Member ports ([u]-Untagged, [t]-Tagged)
 ----   --------   ---------   ------------------------------------------------
 1      vlan1       active      [t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5
                                 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10
                                 [u]ge1/11 [u]ge1/12
 2      vlan2       active      [t]ge1/1 [t]ge1/2
 3      vlan3       active      [u]ge1/1 [u]ge1/2

Switch#configure terminal

# Create an EAPS Domain ring 1
Switch(config)#eaps create 1

#Configure VLAN 2 as the control VLAN
Switch(config)#eaps control-vlan 1 2

#Configure VLAN 1 as a protected VLAN
Switch(config)#eaps protected-vlan 1 1

#Configure Switch1 as the master node
Switch(config)#eaps mode 1 master
```

#Configure GE1 / 1 as primary port
Switch(config)#eaps primary-port 1 ge1/1

#Configure GE1 / 2 as secondary -port
Switch(config)#eaps secondary-port 1 ge1/2

#start-upEAPS Domain ring 1
Switch(config)#eaps enable 1

Switch2 Configuration

Switch2 is configured as the transport of EAPs domain ring 1, the control VLAN is VLAN 2, the protected VLAN is VLAN 1, the primary port is GE1 / 1, the secondary port is GE1 / 2, and other configurations adopt default values。

Switch#configure terminal

#Add VLANs 2 and 3
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-3
Switch(config-vlan)#exit

#Configure GE1 / 1 as a trunk member of VLAN 1 and VLAN 2。
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk native vlan 3
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#Configure GE1 / 2 as a trunk member of VLAN 1 and VLAN 2。
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk native vlan 3
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan

```
VLAN  Name       State      Member ports ([u]-Untagged, [t]-Tagged)
----  --------   ---------  ------------------------------------------------
1     vlan1      active     [t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5
                            [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10
2     vlan2      active     [t]ge1/1 [t]ge1/2
3     vlan3      active     [u]ge1/1 [u]ge1/2
```

Switch#configure terminal

#Create an EAPs domain ring 1

Switch(config)#eaps create

#Configure VLAN 2 as the control VLAN

Switch(config)#eaps control-vlan 1 2

#Configure VLAN 1 as a protected VLAN

Switch(config)#eaps protected-vlan 1

#Configure switch as a transit node

Switch(config)#eaps mode 1 transit

#Configure GE1 / 1 as primary port

Switch(config)#eaps primary-port 1 ge1/1

#Configure GE1 / 2 as secondary port

Switch(config)#eaps secondary-port 1 ge1/2

#Start EAPs domain ring 1

Switch(config)#eaps enable 1

Configuration of switch3

Switch3 is configured as the transport of EAPs domain ring 1, the control VLAN is VLAN 2, the protected VLAN is VLAN 1, the primary port is GE1 / 1, the secondary port is GE1 / 2, and other configurations adopt default values。

Switch#configure terminal

Add VLANs 2 and 3

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-3

Switch(config-vlan)#exit

Configure GE1 / 1 as a trunk member of VLAN 1 and VLAN 2。

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk native vlan 3

Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

Configure GE1 / 2 as a trunk member of VLAN 1 and VLAN 2。

Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk native vlan 3
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan

VLAN	Name	State	Member ports ([u]-Untagged, [t]-Tagged)
1	vlan1	active	[t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10 [u]ge1/11 [u]ge1/12
2	vlan2	active	[t]ge1/1 [t]ge1/2
3	vlan3	active	[u]ge1/1 [u]ge1/2

Switch#configure terminal
#Create an EAPs domain ring 1
Switch(config)#eaps create 1
#Configure VLAN 2 as the control VLAN
Switch(config)#eaps control-vlan 1
#Configure VLAN 1 as a protected VLAN
Switch(config)#eaps protected-vlan 1 1
#Configure switch3 as a transit node
Switch(config)#eaps mode 1 transit

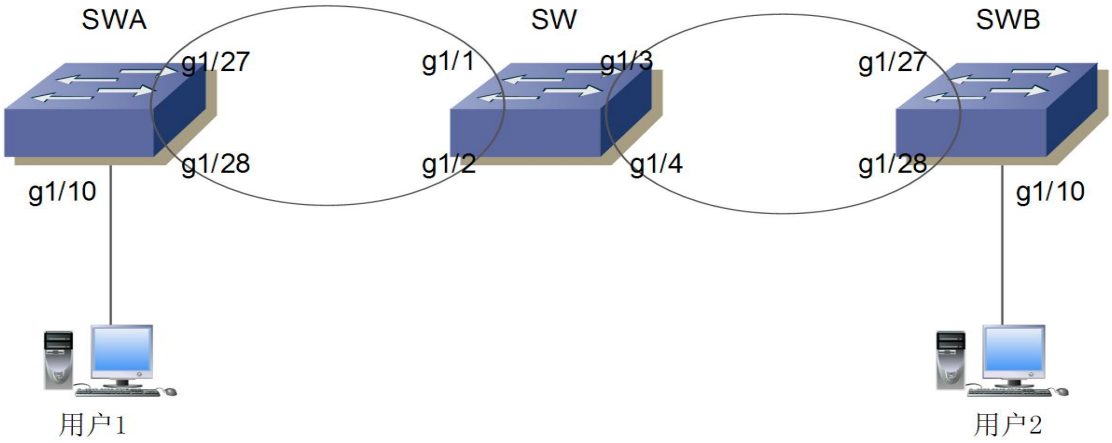
#Configure GE1 / 1 as primary portSwitch(config)#eaps primary-port 1 ge1/1

#Configure GE1 / 2 secondary -port
Switch(config)#eaps secondary-port 1 ge1/2

#start-upEAPS Domain ring 1
Switch(config)#eaps enable 1

1.54 Cross ring data forwarding configuration example

There are three switches SWA, SW and SWB, which realize vlan1 and vlan2 interworking across the ring through EAPs protocol. The topology is as follows：



SWA ring 1 controls VLAN 111 and protects VLAN 1 and 2. The configuration is as follows：

```
vlan database
 vlan 2
 vlan 111

interface ge1/10
 switchport access vlan 2
interface ge1/27
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 111
interface ge1/28
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 111

eaps create 1
eaps mode 1 Transit
eaps primary-port 1 ge1/27
eaps secondary-port 1 ge1/28
eaps control-vlan 1 111
```

```
eaps protected-vlan 1 1
eaps protected-vlan 1 2
eaps enable 1
```

SW ring 1 is connected with SWA to control VLAN 111 and protect VLAN 1 and 2. Ring 2 connects with SWB, controls VLAN 222 and protects VLAN 3333 (virtual VLAN, and the interface needs to be added). If you want to realize the cross ring forwarding of ring 1 and ring 2 data, you need to configure the command EAPs data span. The configuration is as follows：

```
vlan database
 vlan 2
 vlan 111
 vlan 222
 vlan 3333

interface ge1/1
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 111
interface ge1/2
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 111
interface ge1/3
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 222
 switchport trunk allowed vlan add 3333          ###Add virtual vlan 3333
interface ge1/4
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 222
 switchport trunk allowed vlan add 3333          ###Add virtual vlan 3333

eaps create 1
eaps mode 1 Master
```

```
eaps primary-port 1 ge1/1
eaps secondary-port 1 ge1/2
eaps control-vlan 1 111
eaps protected-vlan 1 1
eaps protected-vlan 1 2
eaps data-span 1
eaps enable 1

eaps create 2
eaps mode 2 Transit
eaps primary-port 2 ge1/3
eaps secondary-port 2 ge1/4
eaps control-vlan 2 222
eaps protected-vlan 2 3333                    ###Here is virtual protection vlan
eaps data-span 2
eaps enable 2
```

SWB ring 2 is connected with SW ring 2 to control VLAN 222 and protect VLAN 1 and 2. The configuration is as follows：

```
vlan database
 vlan 2
 vlan 222

interface ge1/10
 switchport access vlan 2

interface ge1/27
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 222

interface ge1/28
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 222

eaps create 2
```

eaps mode 2 Master
eaps primary-port 2 ge1/27
eaps secondary-port 2 ge1/28
eaps control-vlan 2 222
eaps protected-vlan 2 1
eaps protected-vlan 2 2
eaps enable 2

After vlan1 and vlan2 are configured to communicate with each other. EAPs node mode can be modified as required。

Configure ERPS

1.55 ERPS Summary

ERPs (Ethernet ring protection switching protocol) is a ring network protection protocol developed by ITU, also known as g.8032. It is a link layer protocol specially used in Ethernet ring network. When the Ethernet ring network is complete, it can prevent the broadcast storm caused by the data loop, and when a link on the Ethernet ring network is disconnected, it can quickly restore the communication between various nodes on the ring network. ERPs protocol provides a fast Ethernet ring network protection mechanism, which can quickly restore network transmission in case of ring network failure, so as to ensure high availability and high reliability of switches in the case of ring network topology。

1.56 ERPSTechnical introduction

1.56.1 ERPS Loop

The principle of ERPs ring is to minimize the ring. Each ring must be the smallest ring, which is divided into main ring and sub ring: the main ring is a closed ring; A subring is an unclosed ring or a closed ring; All need to be configured through commands.

Each ERPs ring (whether primary or secondary) has five states: (1) idle state: the state when each physical link of the ring network is connected; (2) Protection status: the status when one or more physical links in the ring network are disconnected; (3) Manual switch status: manually change the status of the ring; (4) Forced switch state: forcibly change the state of the ring; (5) Pending status: pending intermediate status。

1.56.2 ERPS node

The layer-2 switching equipment joining the ERPs ring is called a node. No more than two ports of each node can join the same ERPs ring. One port is RPL port and the other is ordinary ring port.

For the global, the roles of nodes are divided into the following two types: (1) intersecting nodes: in intersecting ERPs rings, nodes belonging to multiple rings at the same time are called intersecting nodes; (2) Non intersecting nodes: in intersecting ERPs rings, nodes belonging to only one ERPs ring are called non intersecting nodes.

The node modes specified in ERPs protocol mainly include RPL owner node, RPL neighbor node and ordinary ring node. (1) RPL owner node: there is only one RPL owner node in an ERPs ring, which is determined by the user's configuration. The RPL port is blocked to prevent loops in the ERPs ring. When the RPL owner node receives the fault message and learns that other nodes or links on the ERPs ring have faults, it will automatically release the RPL port, which will resume the reception and transmission of traffic to ensure that the traffic will not be interrupted; (2) RPL neighbor node: a node directly connected to the RPL port of the RPL owner node. Under normal circumstances, the RPL port of the RPL owner node and the RPL port of the RPL neighbor node will be blocked to prevent loop generation. When the ERPs ring fails, the RPL port of the RPL owner node and the RPL port of the RPL neighbor node will be released; (3) Ordinary ring node: in the ERPs ring, all nodes except the RPL owner node and RPL neighbor node are ordinary ring nodes. The RPL port of the ordinary ring node is no different from the ordinary ring port. The ring port of the ordinary ring node is responsible for monitoring the link status of its directly connected ERPs protocol and notifying other nodes of the change

of link status in time；

1.56.3 Links and channels

(1) RPL (ring protection link): each ERPs ring has and only has one RPL, that is, the link where the RPL port of the RPL owner node is located. When the Ethernet ring is in idle state, the RPL link is in blocking state and does not forward data messages to avoid forming a loop;

(2) Sub ring link: in the intersecting ring, it belongs to the sub ring and is controlled by the sub ring;

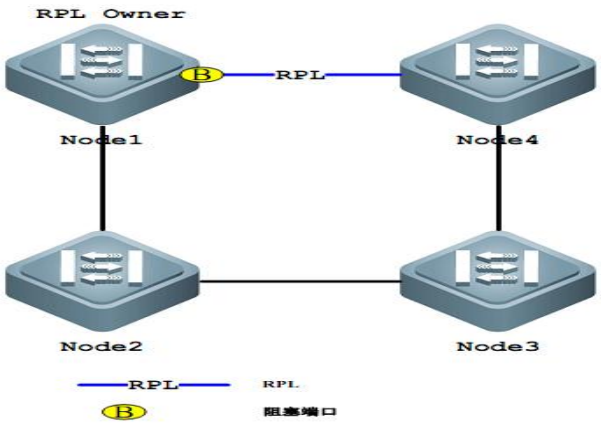
(3) Raps (ring auto protection switch) virtual channel: in the intersecting ring, the path used to transmit sub ring protocol messages between intersecting nodes, but not belonging to the sub ring, is called the raps virtual channel of the sub ring。

1.56.4 ERPS VLAN

There are two types of VLANs in ERPs: (1) raps VLAN: it is used to transmit ERPs protocol messages. The ports connected to the ERPs ring on the device belong to raps VLAN, and only the ports connected to the ERP ring can join this VLAN. Different rings must have different raps VLANs. IP address is not allowed to be configured on the interface of raps VLAN; (2) Data VLAN: as opposed to raps VLAN, data VLAN is used to transmit data messages. Data VLAN can include both ERP ring ports and non ERP ring ports。

1.57 ERPS working principle

1.57.1 Normal state

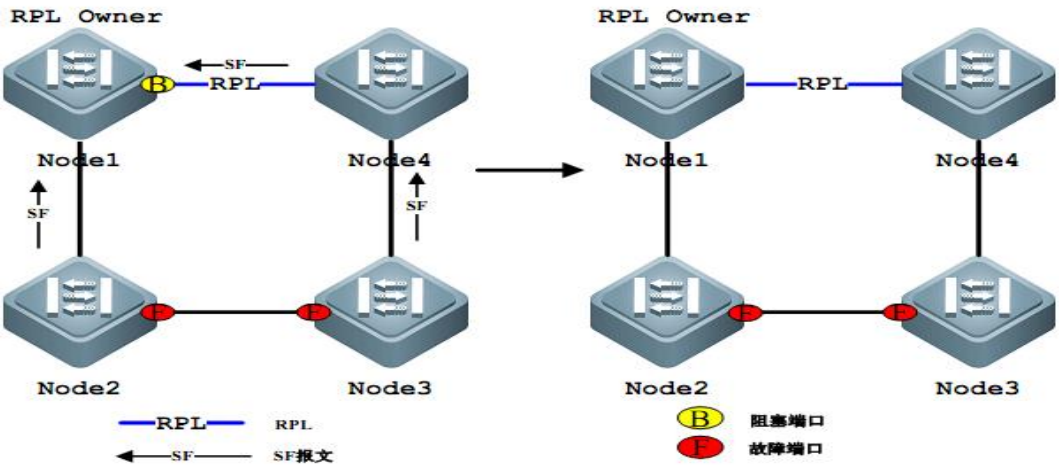


(1) All nodes are connected in the form of rings in the physical topology;

(2) The loop protection protocol ensures no looping by blocking the RPL link. As shown in the figure above, the link between node1 and node4 is an RPL link;

(3) Fault detection is carried out for each link between adjacent nodes。

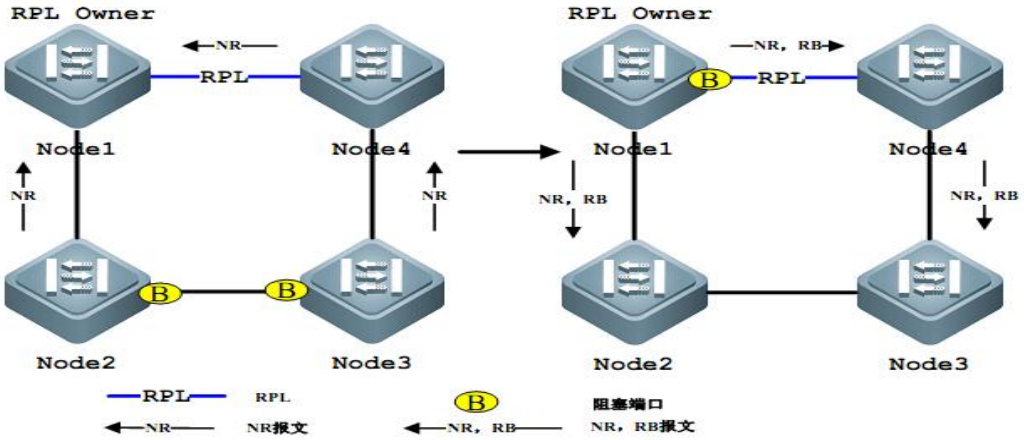
1.57.2 Link failure



(1) The node adjacent to the failed link blocks the failed link and uses raps (SF) message to report the fault to other nodes on the ring. As shown in the figure above, assuming that the link between node2 and node3 fails, node2 and node3 will block the failed link after waiting for the holdoff timer to timeout, and send raps (SF) messages to each node on the ring network respectively;

(2) The raps (SF) message triggers the RPL owning node to open the RPL port. Raps (SF) message also triggers all nodes to update their MAC table entries, and then the nodes enter the protection state

1.57.3 链路恢复



(1) When the fault recovers, the node adjacent to the fault continues to remain blocked and sends a raps (NR) message, indicating that there is no local fault;

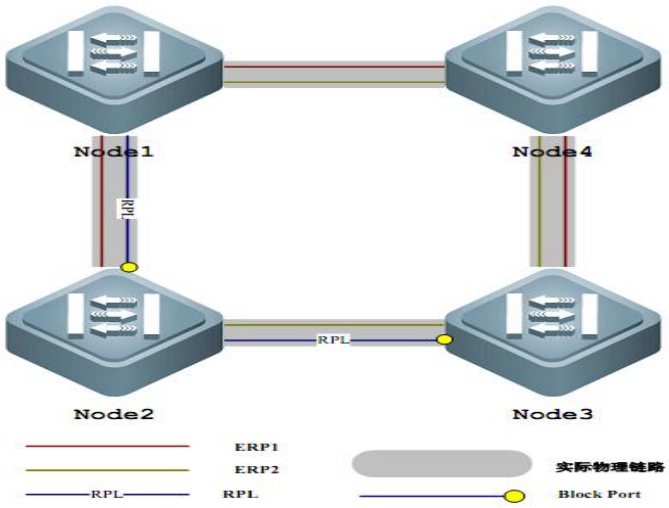
(2) After the guard timer is exhausted, the RPL owner node starts the WTR timer after receiving the first raps (NR) message;

(3) When the WTR timer is exhausted, the RPL owner node blocks the RPL and sends raps (NR, RB) messages;

(4) After receiving this message, other nodes update their MAC table entries. The node sending raps (NR) message stops sending messages periodically and opens the originally blocked port. The ring network has returned to its original normal state。

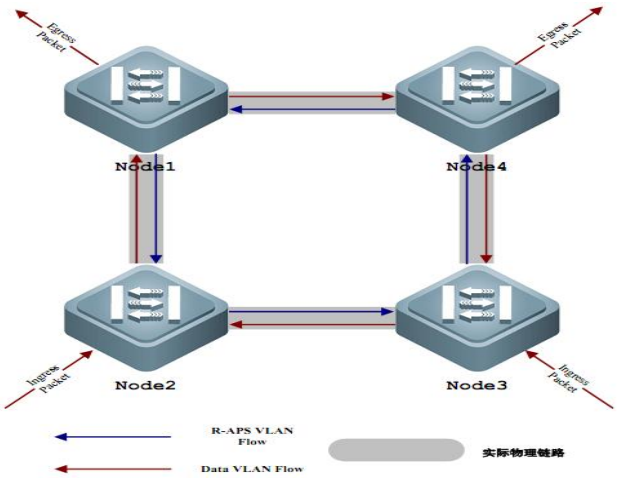
1.58 ERPS Technical features

1.58.1 ERPS load balancing



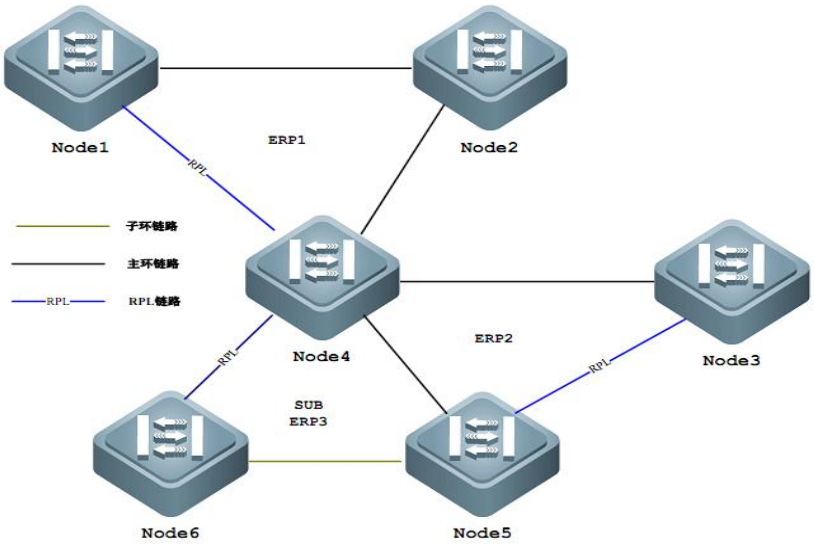
By configuring multiple instances and multiple ERPs rings on the same physical ring network, different ERPs rings send traffic of different VLANs (called protection VLANs), so as to realize different topology of data traffic of different VLANs in the ring network, so as to achieve the purpose of load sharing. As shown in the figure above, a physical ring network corresponds to two instances and two ERPs rings. The VLANs protected by the two ERPs rings are different. Node2 is the RPL owner node of erp1 and node3 is the RPL owner node of ERP2. Through configuration, different VLANs can block different links respectively, so as to realize the load sharing of a single ring。

1.58.2 Good safety



There are two types of VLANs in ERPs, one is raps VLAN and the other is data VLAN. Raps VLAN is only used to transmit the protocol message of ERPs; ERPs only processes protocol messages from raps VLAN, and will not process any protocol attack messages from data VLAN, so as to improve the security of ERPs。

1.58.3 Support multi ring intersection and tangent



As shown in the figure above, ERPs supports adding multiple rings in the form of tangency or intersection at the same node (node4), which greatly increases the flexibility of networking。

1.59 ERPS Protocol command

Command	Description	CLI mode
erps predefine configuration (ring-node | rpl-owner-node)	Enable ERPs predefined configuration	Global configuration mode
no erps predefine configuration	Disable ERPs predefined configuration	Global configuration mode
erps <1-8>	Create an ERPs instance	Global configuration

		mode
no erps <1-8>	Delete an ERPs instance	Global configuration mode
node-role (interconnection | none-interconnection)	Configure the role of the node in the ERPs ring, interconnected node or non interconnected node	ERPS mode
ring <1-32>	Create an ERPs ring	ERPS mode
no ring <1-32>	Delete an ERPs ring	ERPS mode
ring <1-32> ring-mode (major-ring | sub-ring)	Configure ERPs ring mode, main ring or sub ring	ERPS mode
ring <1-32> node-mode (rpl-owner-node | rpl-neighbor-node | ring-node)	Configure the ERPs ring node mode, including RPL owner node, RPL neighbor node or ordinary ring node	ERPS mode
ring <1-32> raps-vlan <2-4094>	Configure ERPs ring protocol VLAN	ERPS mode
no ring <1-32> raps-vlan	Delete ERPs ring protocol VLAN	ERPS mode
ring <1-32> traffic-vlan <1-4094>	Configure ERPs ring data VLAN	ERPS mode
no ring <1-32> traffic-vlan <1-4094>	Delete ERPs ring data VLAN	ERPS mode
ring <1-32> (rpl-port|rl-port) IFNAME	Configure ERPs ring port, RPL port or ordinary ring port	ERPS mode
no ring <1-32> (rpl-port|rl-port)	Delete ERPs ring port	ERPS mode
ring <1-32> revertive-behaviour (revertive|non-revertive)	Configure the recovery behavior of ERPs ring, recoverable or unrecoverable	ERPS mode
ring <1-32> hold-off-time <0-10000>	Configure the hold off time of ERPs ring	ERPS mode
no ring <1-32> hold-off-time	Restore the default hold off time of ERPs ring	ERPS mode

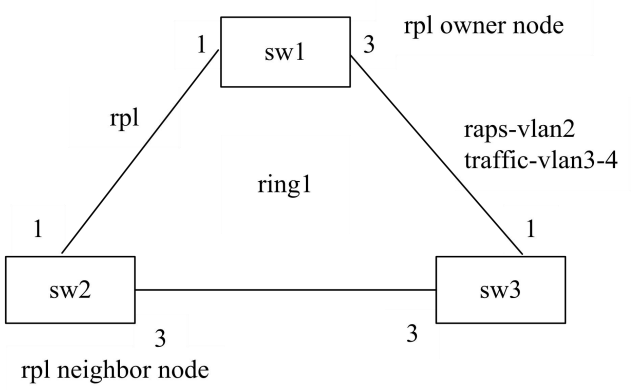
ring <1-32> guard-time <10-2000>	Configure ERPs ring guard time	ERPS mode
no ring <1-32> guard-time	Restore the default time of ERPs ring guard	ERPS mode
ring <1-32> wtr-time <1-12>	Configure ERPs ring WTR time	ERPS mode
no ring <1-32> wtr-time	Restore ERPs ring WTR default time	ERPS mode
ring <1-32> wtb-time <1-10>	Configure ERPs ring WTB time	ERPS mode
no ring <1-32> wtb-time	Restore ERPs ring WTB default time	ERPS mode
ring <1-32> raps-send-time <1-10>	Configure the sending time of ERPs ring protocol message	ERPS mode
no ring <1-32> raps-send-time	Restore the default sending time of ERPs ring protocol message	ERPS mode
ring <1-32> (enable|disable)	Open or close the ERPs ring	ERPS mode
ring <1-32> forced-switch IFNAME	Forced switching of ERPs ring port	ERPS mode
ring <1-32> clear forced-switch	Clear the forced switching of ERPs ring	ERPS mode
ring <1-32> manual-switch IFNAME	Manually switch ERPs ring port	ERPS mode
ring <1-32> clear manual-switch	Clear manual switching of ERPs ring	ERPS mode
ring <1-32> clear recovery	Manual recovery when removing the unrecoverable behavior of ERPs ring or before the expiration of WTR / WTB	ERPS mode
show erps	Displays a brief description of all ERPs instances and rings of the device	Privileged mode

show erps <1-8>	Displays the details of a single ERPs instance and ring of the device	Privileged mode

1.60 ERPS Typical application

1.60.1 Single ring example

As shown in the following figure, SW1, SW2 and SW3 nodes form an ERPs single ring ring1. Ports 1 and 3 of each node are the ERPs ring ports. The protocol VLAN of the ring is 2, the data VLAN is 3 and 4, SW1 node is the RPL owner node, SW2 node is the RPL neighbor node, and the link between SW1 and SW2 is the RPL link。



(1) Configure sw1：

Switch>enable

Switch#configure terminal

Create ERPs protocol and datavlan

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode trunk

Switch(config-ge1/1)# switchport trunk allowed vlan add 2

Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure ERPs instance 1 and ERPs single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

(2) configure sw2:
Switch>enable
Switch#configure terminal
Creating ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port to trunk, and add ERPs protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure ERPs instance 1 and ERPs single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

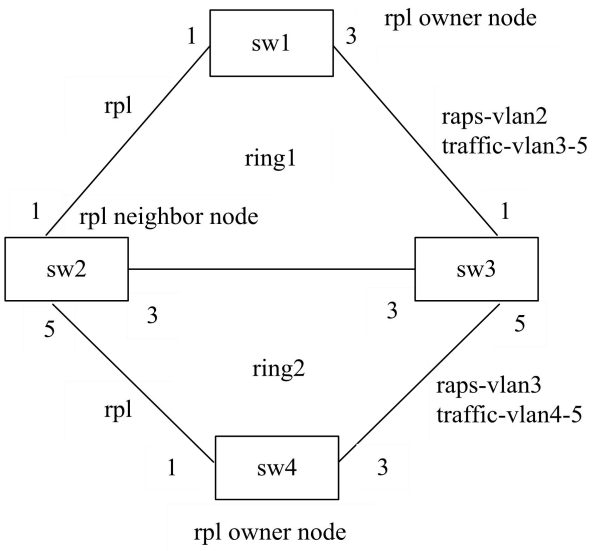
(3) configure sw3:
Switch>enable
Switch#configure terminal
Creating ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port to trunk, and add ERPs protocol and data vlan
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk

```
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure ERPs instance 1 and ERPs single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

1.60.2 Multi ring example

As shown in the following figure, SW1, SW2 and SW3 nodes form an ERPs main ring ring1. Ports 1 and 3 of SW1, SW2 and SW3 nodes are the main ring ring1 ring ports. The protocol VLAN of main ring ring1 is 2, and the data VLAN is 3, 4 and 5. SW1 node is the main ring ring1 RPL owner node, SW2 node is the main ring ring1 RPL neighbor node, and the link between SW1 and SW2 is the main ring ring1 RPL link.

SW2, SW3 and SW4 nodes form an ERPs sub ring RING2. Ports 5 of SW2 and SW3 nodes and Ports 1 and 3 of SW4 nodes are the sub ring RING2 ring ports. The protocol VLAN of sub ring RING2 is 3, the data VLAN is 4 and 5, SW4 node is the sub ring RING2 RPL owner node, and the link between SW2 and SW4 is the sub ring RING2 RPL link。



(1)configure sw1：

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-5

Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode trunk

Switch(config-ge1/1)# switchport trunk allowed vlan add 2

Switch(config-ge1/1)# switchport trunk allowed vlan add 3

Switch(config-ge1/1)# switchport trunk allowed vlan add 4

Switch(config-ge1/1)# switchport trunk allowed vlan add 5

Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3

Switch(config-ge1/3)# switchport mode trunk

Switch(config-ge1/3)# switchport trunk allowed vlan add 2

Switch(config-ge1/3)# switchport trunk allowed vlan add 3

Switch(config-ge1/3)# switchport trunk allowed vlan add 4

Switch(config-ge1/3)# switchport trunk allowed vlan add 5

Switch(config-ge1/3)#exit

Configure ERPs instance 1 and ERPs main ring 1

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode rpl-owner-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 1

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 traffic-vlan 5

Switch(config-erps-1)# ring 1 rpl-port ge1/1

Switch(config-erps-1)# ring 1 rl-port ge1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

(2)configure sw2:

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-5

Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode trunk

Switch(config-ge1/1)# switchport trunk allowed vlan add 2

Switch(config-ge1/1)# switchport trunk allowed vlan add 3

Switch(config-ge1/1)# switchport trunk allowed vlan add 4

Switch(config-ge1/1)# switchport trunk allowed vlan add 5

Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3

Switch(config-ge1/3)# switchport mode trunk

Switch(config-ge1/3)# switchport trunk allowed vlan add 2

Switch(config-ge1/3)# switchport trunk allowed vlan add 3

Switch(config-ge1/3)# switchport trunk allowed vlan add 4

Switch(config-ge1/3)# switchport trunk allowed vlan add 5

Switch(config-ge1/3)#exit
Switch(config)# interface ge1/5
Switch(config-ge1/5)# switchport mode trunk
Switch(config-ge1/5)# switchport trunk allowed vlan add 3
Switch(config-ge1/5)# switchport trunk allowed vlan add 4
Switch(config-ge1/5)# switchport trunk allowed vlan add 5
Switch(config-ge1/5)#exit
Configure ERPs instance 1, ERPs main ring 1, and ERPs sub ring 2
Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port ge1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit

(3) configursw3:
Switch>enable
Switch#configure terminal
Creating ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5

Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode trunk

Switch(config-ge1/1)# switchport trunk allowed vlan add 2

Switch(config-ge1/1)# switchport trunk allowed vlan add 3

Switch(config-ge1/1)# switchport trunk allowed vlan add 4

Switch(config-ge1/1)# switchport trunk allowed vlan add 5

Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3

Switch(config-ge1/3)# switchport mode trunk

Switch(config-ge1/3)# switchport trunk allowed vlan add 2

Switch(config-ge1/3)# switchport trunk allowed vlan add 3

Switch(config-ge1/3)# switchport trunk allowed vlan add 4

Switch(config-ge1/3)# switchport trunk allowed vlan add 5

Switch(config-ge1/3)#exit

Switch(config)# interface ge1/5

Switch(config-ge1/5)# switchport mode trunk

Switch(config-ge1/5)# switchport trunk allowed vlan add 3

Switch(config-ge1/5)# switchport trunk allowed vlan add 4

Switch(config-ge1/5)# switchport trunk allowed vlan add 5

Switch(config-ge1/5)#exit

Configure ERPs instance 1, ERPs main ring 1, and ERPs sub ring 2

Switch(config)#erps 1

Switch(config-erps-1)# node-role interconnection

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode ring-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 1

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 traffic-vlan 5

Switch(config-erps-1)# ring 1 rpl-port ge1/1

Switch(config-erps-1)# ring 1 rl-port ge1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port ge1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit

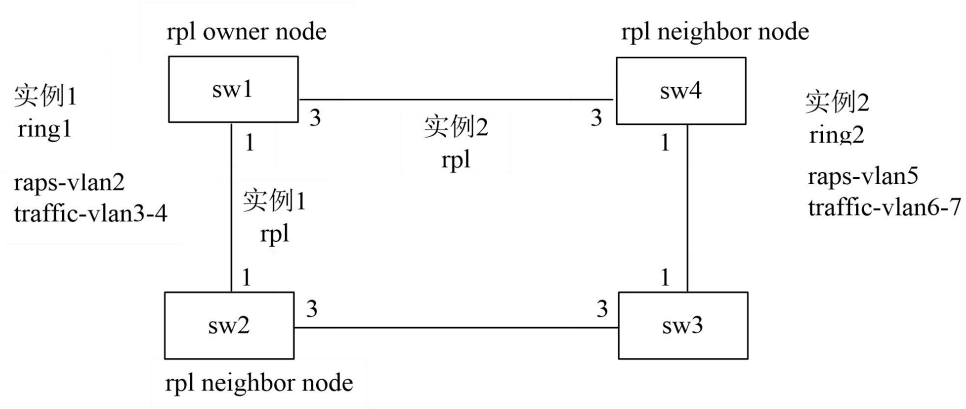
(4) configursw4：
Switch>enable
Switch#configure terminal
Creating ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 3-5
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)#exit
Configure ERPs instance 1 and ERPs sub ring 2
Switch(config)#erps 1
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode rpl-owner-node
Switch(config-erps-1)# ring 2 raps-vlan 3

Switch(config-erps-1)# ring 2 traffic-vlan 1
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port ge1/1
Switch(config-erps-1)# ring 2 rl-port ge1/3
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit

1.60.3 Multi instance load balancing example

As shown in the following figure, SW1, SW2, SW3 and SW4 nodes constitute a single ring ring1 of ERPs instance 1. Ports 1 and 3 of each node are the ERPs ring ports. The protocol VLAN of the ring is 2, the data VLAN is 3 and 4, SW1 node is the RPL owner node, SW2 node is the RPL neighbor node, and the link between SW1 and SW2 is the RPL link.

SW1, SW2, SW3 and SW4 nodes constitute a single ring RING2 of ERPs instance 2. Ports 1 and 3 of each node are the ERPs ring ports. The protocol VLAN of the ring is 5, the data VLAN is 6 and 7, SW1 node is the RPL owner node, SW4 node is the RPL neighbor node, and the link between SW1 and SW4 is the RPL link。



(1) Configuration instance 1：

Configure sw1：

Switch>enable
Switch#configure terminal
Configure instance to create ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN

Switch(config)# interface ge1/1

Switch(config-ge1/1)# switchport mode trunk

Switch(config-ge1/1)# switchport trunk allowed vlan add 2

Switch(config-ge1/1)# switchport trunk allowed vlan add 3

Switch(config-ge1/1)# switchport trunk allowed vlan add 4

Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3

Switch(config-ge1/3)# switchport mode trunk

Switch(config-ge1/3)# switchport trunk allowed vlan add 2

Switch(config-ge1/3)# switchport trunk allowed vlan add 3

Switch(config-ge1/3)# switchport trunk allowed vlan add 4

Switch(config-ge1/3)#exit

Configure ERPs instance 1 and ERPs single ring 1

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode rpl-owner-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 1

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 rpl-port ge1/1

Switch(config-erps-1)# ring 1 rl-port ge1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

Configure sw2:

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN

Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure ERPs instance 1 and ERPs single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
Configure sw3:
Switch>enable
Switch#configure terminal
Creating ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2

Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure ERPs instance 1 and ERPs single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
Configure sw4:
Switch>enable
Switch#configure terminal
Creating ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 2
Switch(config-ge1/1)# switchport trunk allowed vlan add 3
Switch(config-ge1/1)# switchport trunk allowed vlan add 4
Switch(config-ge1/1)#exit

Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 2
Switch(config-ge1/3)# switchport trunk allowed vlan add 3
Switch(config-ge1/3)# switchport trunk allowed vlan add 4
Switch(config-ge1/3)#exit
Configure ERPs instance 1 and ERPs single ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 1
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port ge1/1
Switch(config-erps-1)# ring 1 rl-port ge1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

(2) Configuration instance 2：

Configure sw1：

Switch>enable
Switch#configure terminal
Creating ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3

Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit
Configure ERPs instance 2 and ERPs single ring 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode rpl-owner-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/3
Switch(config-erps-2)# ring 2 rl-port ge1/1
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
Configure sw2:
Switch>enable
Switch#configure terminal
Creating ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6

Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit
Configure ERPs instance 2 and ERPs single ring 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode ring-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/1
Switch(config-erps-2)# ring 2 rl-port ge1/3
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
Configure sw3:
Switch>enable
Switch#configure terminal
Creating ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit
Configure ERPs instance 2 and ERPs single ring 2

Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode ring-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/1
Switch(config-erps-2)# ring 2 rl-port ge1/3
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
Configure sw4:
Switch>enable
Switch#configure terminal
Creating ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure the VLAN mode of the ring port as trunk, and add ERPs protocol and data VLAN
Switch(config)# interface ge1/1
Switch(config-ge1/1)# switchport mode trunk
Switch(config-ge1/1)# switchport trunk allowed vlan add 5
Switch(config-ge1/1)# switchport trunk allowed vlan add 6
Switch(config-ge1/1)# switchport trunk allowed vlan add 7
Switch(config-ge1/1)#exit
Switch(config)# interface ge1/3
Switch(config-ge1/3)# switchport mode trunk
Switch(config-ge1/3)# switchport trunk allowed vlan add 5
Switch(config-ge1/3)# switchport trunk allowed vlan add 6
Switch(config-ge1/3)# switchport trunk allowed vlan add 7
Switch(config-ge1/3)#exit
Configure ERPs instance 2 and ERPs single ring 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring

```
Switch(config-erps-2)# ring 2 node-mode rpl-neighbor-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 1
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port ge1/3
Switch(config-erps-2)# ring 2 rl-port ge1/1
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
```

Configure AAA

This chapter describes how to configure 802.1x and radius of the switch to prevent illegal users from accessing the network. For the use of 802.1x client and hyperboss, please refer to their respective operation manuals. This chapter mainly includes the following contents：

- 802.1x Introduction
- RADIUS Introduction
- Configure 802.1x
- Configure RADIUS

AAA is the abbreviation of authentication, authorization, and accounting. It provides a consistent framework for configuring three security functions: authentication, authorization and billing. AAA configuration is actually a kind of management of network security. Here,

network security mainly refers to access control. Which users can access the network? What services are available to users with access rights? How to account for users who are using network resources?

Authentication: verify whether the user can obtain access.

Authorization: what services can authorized users use.

Accounting: records the user's use of network resources.

The network company has launched a complete set of AAA solutions, including 802.1x clients, various switches supporting authentication and hyperboss. 802.1x client is installed on the PC where users surf the Internet. When users need to access the network, they need to use 802.1x client for authentication. Only authenticated users can use the network. It receives the authentication request from the client and transmits the user name and password to the authentication and billing system hyperboss. The switch itself does not do the actual authentication work. Hyperboss receives the authentication request from the switch, performs the actual authentication, and charges the users who have successfully authenticated.

802.1x protocol is used for communication between 802.1x client and switch, and radius protocol is used for communication between switch and hyperboss.

1.61 802.1x Introduction

802.1x protocol is a port based access control and authentication protocol. The port here refers to logical port, which can be physical port, MAC address or VLAN ID. the switches of the network implement 802.1x protocol based on MAC address.

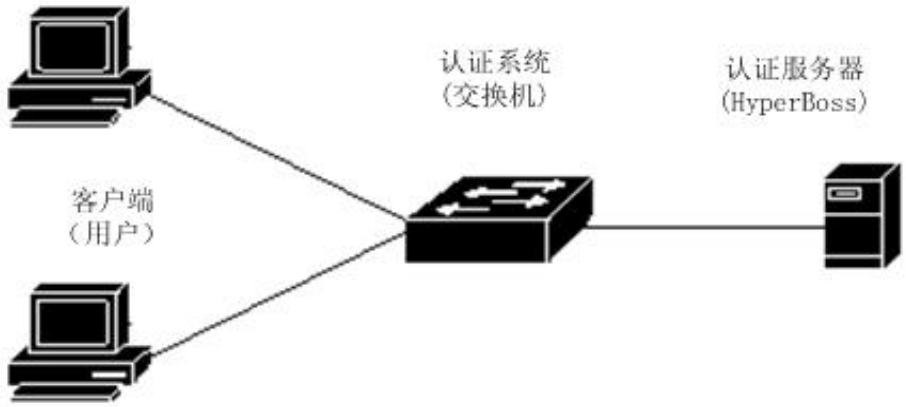
802.1x is a layer-2 protocol. The authenticated switch and the user's PC must be in the same subnet, and the protocol packet cannot cross the network segment. 802.1x authentication adopts the client server model, and there must be a server to authenticate all users. Before the user passes the authentication, only the authentication flow can pass through the port of the switch. After the authentication is successful, the data flow can pass through the port of the switch, that is, the user must pass the authentication before accessing the network.

This section mainly includes the following contents:：

- 802.1x Equipment composition
- Introduction to protocol package
- Protocol flow interaction
- 802.1x port status

1.61.1 802.1x Equipment composition

802.1x device consists of three parts: client (supplicant system), authenticator system and authentication server system. As shown in the figure below。



802.1x Equipment

The client refers to the device requesting access to the network. Generally, it is the user terminal system, such as the user's PC. an 802.1x client software must be installed on the user terminal system, which realizes the client part of 802.1x protocol. The client initiates an 802.1x authentication request and requests the authentication server to verify its user name and password. If the authentication is successful, the user can access the network.

An authentication system refers to an authenticated device, such as a switch. The authentication system controls whether the user can access the network through the state of the user's logical port (referring to the MAC address). If the user's logical port state is unauthorized, the user cannot access the network. If the user's logical port state is authorized, the user can access the network.

The authentication system is a relay between the client and the authentication server. The authentication system requests the user's identity information, forwards the user's identity information to the authentication server, and forwards the authentication result sent by the authentication server to the client. The authentication system needs to implement the 802.1x Protocol on the server side close to the user side and the radius protocol on the client side close to the authentication server side. The radius protocol client of the authentication system encapsulates the EAP information sent by the 802.1x client in radius and sends it to the authentication server, The EAP information is unpacked from the raidus protocol package sent by the authentication server and transmitted to the 802.1x client through the 802.1x server.

The authentication server refers to the device that actually authenticates the user. The authentication server receives the user's identity information from the authentication system and verifies it. If the authentication is successful, the authentication server authorizes the authentication system and allows the user to access the network. If the authentication fails, the authentication server tells the authentication system that the user authentication fails and the user cannot access the network. The authentication server communicates with the authentication system through EAP extended RADIUS protocol. The network provides an authentication and billing system hyperboss to authenticate and charge users。

1.61.2 Introduction to protocol package

The authentication data stream transmitted by 802.1x Protocol on the network is in eapol (EAP over LAN) frame format. All user identity information (including user name and password) is encapsulated in EAP (extended authentication protocol), and EAP is encapsulated in eapol frame. The user name exists in EAP in clear text, while the password exists in EAP in MD5 encryption.

Eapol frame format is shown below. PAE Ethernet type is the Ethernet protocol type number of eapol, and the value is 0x888e. Protocol version is the eapol version number with a value of 1. Packet type refers to eapol frame type. Packet body length is the length of eapol frame content. Packet body refers to the content of eapol frame。

	Octet Number
PAE Ethernet Type	1-2
Protocol Version	3
Packet Type	4
Packet Body Length	5-6
Packet Body	7-N

EAPOL frame format

The switch uses three eapol protocol frames:

Eapol start: the value of packet type is 1. The authentication initiates the frame. When the user needs to authenticate, this frame is first initiated and sent by the client to the switch.

Eapol logoff: the value of packet type is 2, exit the request frame, and send this frame to notify the switch when the user does not need to use the network.

EAP packet: the value of packet type is 0, and the authentication information frame is used to carry the authentication information.

The format of EAP package is shown in the figure below. Code refers to the type of EAP package, including request, response, success and failure. Identifier refers to the identifier used to match response and request. Length refers to the length of the EAP packet, including the header. Data refers to EAP packet data.

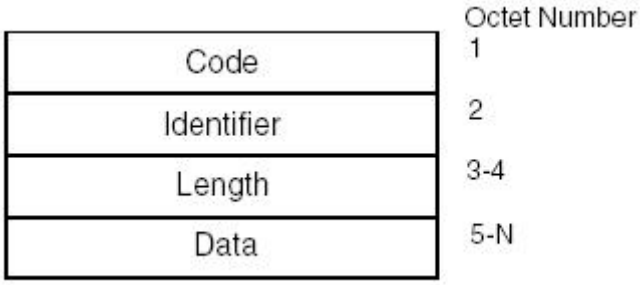
EAP packages include the following four types:

EAP request: when the code value is 1, the EAP request package is sent from the switch to the client to request the user name and / or password.

EAP response: when the code value is 2, the EAP response packet is sent from the client to the switch, and the user name and / or password are sent to the switch.

EAP success: when the code value is 3, the EAP success package is sent from the switch to the client to tell the client that the user authentication is successful.

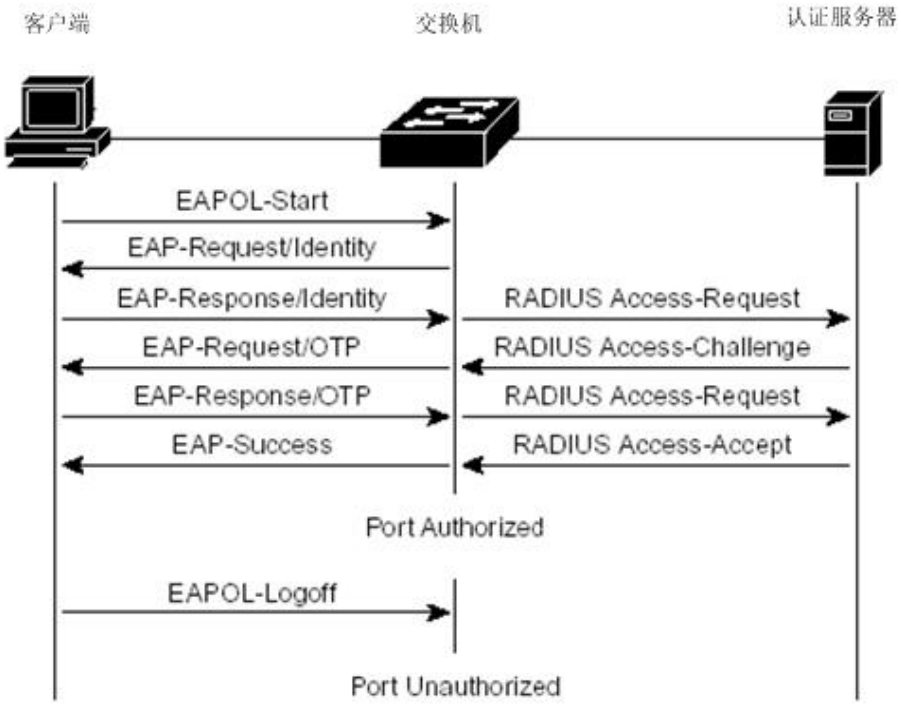
EAP failure: the code value is 4. The EAP failure packet is sent from the switch to the client and tells the client that the user authentication fails。



EAP包格式

1.61.3 Protocol flow interaction

When the switch enables 802.1x and the status of the port is auto, all access users under the port must pass authentication before accessing the network. The protocol interaction is shown in the figure below。

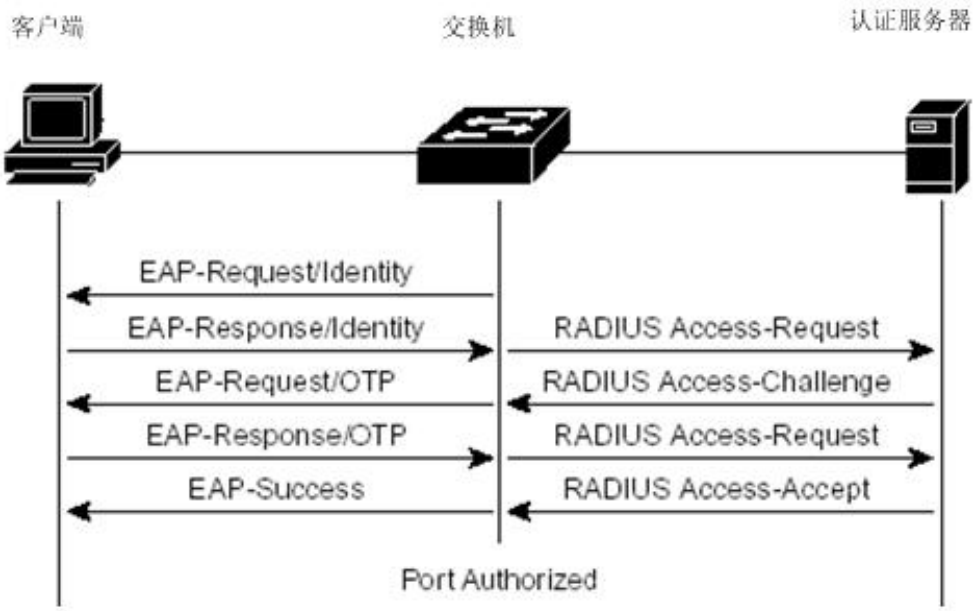


Client initiated authentication protocol interaction

When the user needs to access the network, the client first sends eapol start to the switch to request authentication. After receiving the authentication request, the switch sends EAP request to request the user's user name, and the client sends EAP response back. The switch extracts EAP information and encapsulates it in radius package and sends it to the authentication server, which requests the user's password, The switch sends EAP request to the client to request the user's password, and the client sends back EAP response. The switch encapsulates the EAP information in radius package and sends it to the authentication server, which authenticates the user according to the user name and password. If the switch is in the status of EAP success authentication, the client will be notified of the success of the switch authentication. When the client receives EAP success, it indicates that the authentication is successful, and the user can access the network.

When the user no longer needs to use the network, the client sends eapol logoff to the switch, and the switch changes the user's logical port state to unauthorized state. At this time, the user cannot access the network.

In order to prevent the abnormal offline of the client, the switch provides a re authentication mechanism. The interval of re authentication can be set on the switch. When the authentication time arrives, the switch initiates re authentication. If the authentication is successful, the user can continue to use the network. If the authentication fails, the user will not be able to use the network. The protocol interaction is shown in the figure below。



Re authenticated protocol

1.61.4 802.1xport status

The port state here refers to the physical port state of the switch. The physical port of the switch has four states: n / a state, auto state, force authorized state and force unauthorized state. When the switch does not open 802.1x, all ports are in N / a state. When the switch port is to be set to auto state, force authorized state or force unauthorized state, 802.1x of the switch must be enabled first.

When the port of the switch is in the N / a state, all users under the port can access the network without authentication. When the switch receives 802.1x protocol packets from the port, these protocol packets are discarded.

When the port of the switch is in the force authorized state, all users under the port can access the network without authentication. When the switch receives eapol start packets from this port, the switch sends back EAP success packets. When the switch receives other 802.1x protocol packets from this port, these protocol packets are discarded.

When the port of the switch is in the force unauthorized state, all users under the port can never access the network, and the authentication request can never pass. When the switch receives 802.1x protocol packets from the port, these protocol packets are discarded.

When the port of the switch is in auto state, all users under the port must pass authentication before accessing the network. 802.1x protocol interaction is shown in the figure. If the user needs to authenticate, the port should generally be set to auto state.

When the switch port is set to auto state, the anti ARP Spoofing function is enabled at the same time; The anti ARP Spoofing function can control that only the data packets whose source MAC and source IP of the IP packet comply with the information provided by the client during authentication, and the data packets whose sender IP and sender MAC of the ARP packet comply with the information provided by the client during authentication can be forwarded by this port, otherwise they will be discarded. To configure this function, the client must be a statically configured IP address. If the IP address is dynamically obtained through DHCP protocol, you can enable DHCP snooping protocol to realize this function; If you need a more detailed introduction, please refer to IP MAC binding configuration。

1.62 RADIUS Introduction

When the user authenticates, the radius protocol supporting EAP extension is used for interaction between the switch and the authentication server. Radius protocol adopts client / server model. The switch needs to implement radius client and the authentication server needs to implement radius server.

In order to ensure the security of the interaction between the switch and the authentication server and prevent the interaction between illegal switches or illegal authentication servers, the switch and the authentication server should authenticate each other. The switch and authentication server need the same key. When the switch or authentication server sends RADIUS protocol packets, all protocol packets shall generate message summaries using HMAC algorithm according to the key. When the switch and authentication server receive RADIUS protocol packets, the message summaries of all protocol packets shall be verified with the key. If the verification passes, It is considered to be a legal RADIUS protocol packet, otherwise it is an illegal RADIUS protocol packet and will be discarded。

This section mainly includes the following contents：

- 协议包简介
- 协议流交互
- 用户验证方法

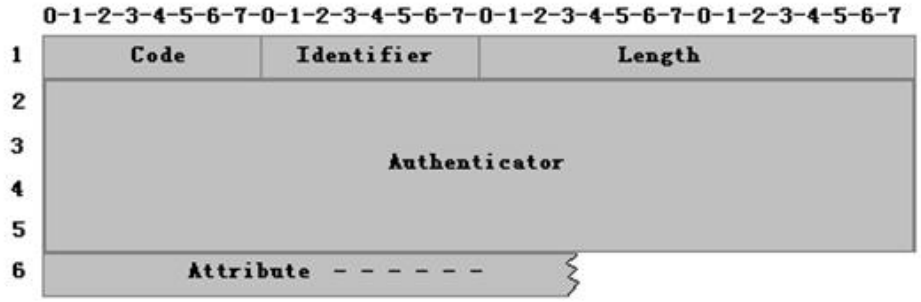
1.62.1 Introduction to protocol package

Radius is a protocol based on UDP. Radius can encapsulate authentication

information and billing information. The early radius authentication port is 1645, and the current port is 1812. The early radius billing port is 1646, and the current port is 1813.

Because radius is hosted on UDP, radius should have a timeout retransmission mechanism. At the same time, in order to improve the reliability of communication between the authentication system and radius server, two radius server schemes are generally adopted, that is, the standby server mechanism is adopted.

The format of radius message is shown in the figure below. Code refers to the radius protocol message type. Identifier indicator identifier, used to match request and response. Length refers to the length of the whole message (including the message header). Authenticator is a 16 byte string. It is a random number for request packets and a message digest generated by MD5 for response packets. Attribute refers to the attribute in the radius protocol package。



RADIUSMessage format

The network uses the following RADIUS protocol packages:

Access request: the code value is 1, which is the authentication request package sent from the authentication system to the authentication server. The user name and password are encapsulated in this package.

Access accept: the code value is 2. The response package sent from the authentication server to the authentication system indicates that the user authentication is successful.

Access reject: the code value is 3. The response package sent from the authentication server to the authentication system indicates that the user authentication fails.

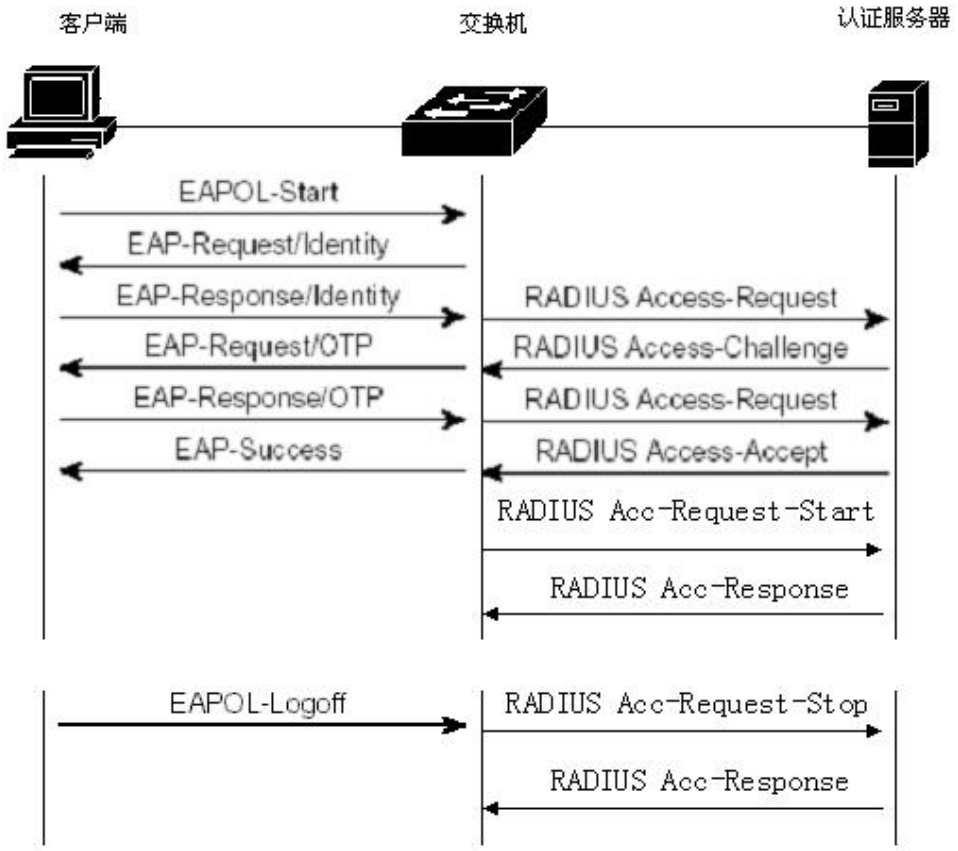
Access challenge: code value 11, the response package sent from the authentication server to the authentication system, indicating that the authentication server needs further information of the user, such as password, etc.

Accounting request: the code value is 4. The billing request package sent from the authentication system to the authentication server includes the start billing package and the end billing package. The billing information is encapsulated in this package.

Accounting response: the code value is 5. The billing response package sent from the authentication server to the authentication system indicates that the billing information has been received。

1.62.2 Protocol flow interaction

When the user initiates authentication, the authentication system and the authentication server interact through radius protocol. The protocol flow interaction in which the authentication system does not send radius billing packets is shown in the figure below. Generally, after the user authentication is successful or when the user goes offline, the authentication system needs to send radius charging package to the authentication server. The protocol flow interaction is shown in the figure below。



When the user authenticates, the switch encapsulates the user name in the access request message and sends it to the authentication server. The server responds to the access challenge request for the user's password. The switch requests the password of the client user. The client encapsulates the password in EAP. After the switch obtains this EAP, it encapsulates it in access request and sends it to the authentication server. The authentication server authenticates the user, If the authentication is successful, send back

access accept to the switch. After receiving this message, the switch notifies the client that the authentication is successful. At the same time, it sends accounting request to notify the authentication server to start charging, and the authentication server sends back accounting response.

When the user does not want to use the network, notify the switch user to go offline, and the switch sends an accounting request to notify the authentication server to end the billing. The billing information is encapsulated in this package, and the authentication server sends back the accounting response。

1.62.3 User authentication method

Radius has three user authentication methods, as follows：

- PAP（Password Authentication Protocol）。 The user passes the user name and his password to the switch in clear text. The switch passes the user name and password to the radius server through the radius protocol package. The radius server looks up the database. If there are the same user name and password, it indicates that the authentication is passed, otherwise it indicates that the authentication is not passed。
- CHAP（Challenge Handshake Authentication Protocol）。 When the user requests to access the Internet, the switch generates a 16 byte random code to the user. The user encrypts the random code, password and other domains to generate a response, and transmits the user name and response to the switch. The switch transmits the user name, response and the original 16 byte random code to the radius server. Radius looks up the database at the switch end according to the user name, obtains the same password as the encryption used by the user end, and then encrypts it according to the transmitted 16 byte random code, and compares the result with the transmitted response. If it is the same, it indicates that the authentication is passed, and if it is different, it indicates that the authentication is failed。
- EAP（Extensible Authentication Protocol）。

With this authentication method, the switch does not really participate in the authentication, but only plays the role of forwarding between the user and the radius server. When the user requests to access the Internet, the switch requests the user's user name and forwards the user name to the radius server. The radius server generates a 16 byte random code to the user and stores the random code. The user encrypts the random code, password and other domains to generate a response, transmits the user name and

response to the switch, and the switch forwards it to the radius server. Radius looks up the database at the switch end according to the user name, obtains the same password as that used by the user end for encryption, then encrypts it according to the stored 16 byte random code, and compares the result with the transmitted response. If it is the same, it indicates that the authentication is passed, if it is different, it indicates that the authentication is failed.

The authentication and billing solution of the network adopts EAP user

1.63 Configure 802.1x

This section describes the configuration of 802.1x in detail, mainly including the following contents：

- 802.1x Default configuration
- Turn 802.1x on and off
- Configure 802.1x port status
- Configure re authentication mechanism
- Configure the maximum number of port access hosts
- Configure interval and number of retransmissions
- Configure port as transport port
- Configure 802.1x client version number
- Configure whether to check the client version number
- Configure authentication method
- Configure whether to check the timing package of the client
- 802.1x display information

1.63.1 802.1xDefault configuration

The default configuration of switch 802.1x is as follows:：

- 802.1x is closed。
- The status of all ports is N/A。
- The recertification mechanism is turned off, and the interval between recertification is 3600 seconds。
- The maximum number of access hosts for all ports is 100。
- The timeout interval for resending EAP request is 30 seconds。
- The number of times to resend EAP request after timeout is 3。

- The waiting time for user authentication failure is 60 seconds。
- The time interval of timeout retransmission at the server is 10 seconds

The switch provides a command in the global config mode to return all configurations to the default state. The commands are as follows：

Switch(config)#dot1x default

1.63.2 Turn 802.1x on and off

The first step in configuring 802.1x is to start 802.1x. In global config mode, enter the following command to start 802.1x:

Switch(config)#dot1x

When 802.1x is turned off, all ports return to the N / a state. In global config mode, enter the following command to turn off 802.1x:

Switch(config)#no dot1x

1.63.3 Configure 802.1x port status

Be sure to start 802.1x before setting the 802.1x port status. If all users under the port must pass authentication before accessing the network, the port must be set to auto state.

The following command sets port GE1 / 1 to auto state in the interface configuration mode and enables the anti ARP Spoofing function:

Switch(config-ge1/1)dot1x control auto

If the anti ARP Spoofing configuration fails, it may be caused by the following reasons:

1. System CFP resources are exhausted.
2. The ACL filtering function is configured for the current interface.
3. The DHCP snooping function is enabled on the current interface.
4. The configured interface is a three-layer interface or trunk interface.

The following command sets port GE1 / 1 to force authorized status in interface configuration mode:

Switch(config-ge1/1)dot1x control force-authorized

The following command sets port GE1 / 1 to force unauthorized state in interface configuration mode:

Switch(config-ge1/1)dot1x control force-unauthorized

The following command sets port GE1 / 1 to N / a status in interface configuration

mode:

Switch(config-ge1/1)no dot1x control

Note: if a port is bound with a MAC address, it cannot be set to auto, force authorized or force unauthorized status。

1.63.4 Configure re authentication mechanism

In order to prevent the switch and authentication server from being unaware of the abnormal offline of the client, the switch provides a re authentication mechanism, and the switch initiates authentication every re authentication interval.

The following command starts the re authentication mechanism in global config mode:

Switch(config)#dot1x reauthenticate

The following command turns off the re authentication mechanism in global config mode:

Switch(config)#no dot1x reauthenticate

The following command sets the interval of re authentication in global config mode:

Switch(config)#dot1x timeout re-authperiod <interval>

Note: the interval of re authentication should not be set too short, otherwise the network bandwidth and CPU resource consumption of the switch are too large。

1.63.5 配置端口接入主机最大个数

交换机的每个端口都可控制接入的最大主机个数，此功能可以限制用户使用多台主机非法接入到网络中。端口接入主机最大个数缺省是100个，最大可以设置成100个。如果端口的接入主机最大个数设置为0，那么该端口拒绝任何用户接入。

下面的命令在接口配置模式下设置端口ge1/1接入主机最大个数：

Switch(config-ge1/1)dot1x support-host <number>

1.63.6 Configure interval and number of retransmissions

802.1x protocol standard specifies some interval times and retransmission times of protocol interaction and protocol state machine. The switch uses standard interval times

and retransmission times. It is recommended that users do not change these interval times and retransmission times when using

TX period refers to the interval time of the switch retransmitting EAP request protocol packet; Max req indicates the number of times the switch retransmits EAP request; The interval used to indicate the time when the user waits for re authentication; Server timeout indicates the interval between the switch retransmitting radius packets to the authentication server; Sup timeout indicates the interval between the switch and the client to resend EAP request packets.

The following command configures these intervals and the number of retransmissions in global config mode：

Switch(config)#dot1x timeout tx-period <interval>

Switch(config)#dot1x max-req <number>

Switch(config)#dot1x timeout quiet-period <interval>

Switch(config)#dot1x timeout server-timeout <interval>

Switch(config)#dot1x timeout supp-timeout <interval>

1.63.7 Configure port as transport port

When the switch does not turn on 802.1x authentication, but other switches in the subnet turn on 802.1x authentication, the port connecting the client and the authentication switch of the switch can be configured as the transmission port, and the eapol authentication packet can be forwarded between the client and the 802.1x authentication switch. So as to realize the 802.1x authentication of other switches to clients.

The following command sets port GE1 / 1 as the transmission port in the interface configuration mode:

Switch(config-ge1/1)dot1x transmit-port

The following command sets port GE1 / 1 as a non transmission port in the interface configuration mode

Switch(config-ge1/1)no dot1x transmit-port

1.63.8 Configure 802.1x client version number

Configure the version number of 802.1x client. Only the client whose version is not lower than the configured version number can be authenticated, otherwise the authentication fails. The default client version number of the switch is 2.0.

The following command configures the client version number in global config mode：

Switch(config)# dot1x client-version <string>

1.63.9 Configure whether to check the client version number

Configure whether to check the version number of 802.1x client. If it is configured to check, the switch must first check the version number of client during authentication. The default is configured to check.

The following command is configured to turn on the check of the client version number in the global config mode：

Switch(config)# dot1x check-version open

1.63.10 Configure authentication method

Configure the authentication mode of the switch for 802.1x packets. The authentication mode initiated by the client is divided into general authentication and extended authentication. The switch can be configured to authenticate in which mode first. If the authentication method initiated by the client is inconsistent with the authentication method configured by the switch, the client will convert to another authentication method to initiate authentication after a certain number of authentication failures.

The following command configures the authentication mode of the switch to the extended authentication mode in the global config mode：

Switch(config)# dot1x extended

1.63.11 Configure whether to check the timing package of the client

After the client configures the 802.1x timing, it will check whether all packets have passed the 802.1x authentication. After the client configures the timing, it will check whether all packets have passed the 802.1x authentication.

The following command is configured for the switch to check the timing packet of the client in the global config mode：

Switch(config)# dot1x check-client

1.63.12 display 802.1x information

The following command displays 802.1x information in normal mode / privileged mode. When the command is show dot1x, it displays all 802.1x configuration information, including the configuration information of all ports; When the command is show dot1x interface, the information of all access users under the port is displayed：

Switch#show dot1x

Switch#show dot1x interface

1.64 Configure RADIUS

This section describes the radius configuration in detail, mainly including the following contents：

- Radius default configuration
- Configure the IP address of the authentication server
- Configure shared key
- Start and close billing
- Configure radius port and attribute information
- Configure radius roaming function
- Display radius information

1.64.1 RADIUS Default configuration

The default configuration of switch radius is as follows:：

- The IP addresses of the primary authentication server and the backup authentication server are not configured, that is, the IP address is 0.0.0.0。
- The shared key is not configured, that is, the shared key string is empty。
- Billing is enabled by default。
- Radius authentication UDP port is 1812 and billing UDP port is 1813。
- The value of radius attribute nasport is 0xc353, the value of nasporttype is 0x0f, and the value of nasportserver is 0x02。

1.64.2 Configure the IP address of the authentication server

In order to enable radius communication between the switch and the authentication server, the IP address of the authentication server needs to be configured on the switch. In practical application, one authentication server or two authentication servers can be used, one as the main authentication server and one as the backup authentication server. If the switch is configured with the IP addresses of two authentication servers, the switch can switch to communicate with the backup authentication server after the communication between the switch and the main authentication server is interrupted.

The following command configures the IP address of the primary authentication server in global config mode：

Switch(config)#radius-server host <ip-address>

The following command configures the IP address of the backup authentication server in the global config mode：

Switch(config)#radius-server option-host <ip-address>

1.64.3 Configure shared key

Mutual authentication is required between the switch and the authentication server, and the same shared key needs to be set on the switch and the authentication server.

Note that the shared key on the switch must be the same as that of the authentication server.

The following command configures the shared key of the switch in global config mode：

Switch(config)#radius-server key <string>

1.64.4 Start and close billing

If the switch turns off charging, the switch will not send radius charging package to the authentication server after successful authentication or when the user goes offline. Generally, in practical application, billing is turned on.

The following command starts billing in global config mode：

Switch(config)#radius-server accounting

The following command turns off billing in global config mode：

Switch(config)#no radius-server accounting

1.64.5 configure radius port and attribute information

It is recommended that users do not modify the radius port and attribute information configuration.

The following command modifies the radius authenticated UDP port in the global config mode:

Switch(config)#radius-server udp-port <port-number>

The following commands modify radius attribute information in global config mode：

Switch(config)#radius-server attribute nas-portnum <number>

Switch(config)#radius-server attribute nas-porttype <number>

Switch(config)#radius-server attribute service-type <number>

1.64.6 Configure radius roaming function

When the client is bound with Mac, IP or VLAN, when the client is moved to other

places, the bound client cannot carry out 802.1x authentication due to the change of MAC address, IP address or VLAN. When the radius roaming function is turned on, the Mac, IP or VLAN binding of the client will be ignored, so as to continue to realize 802.1x authentication.

The following commands configure radius roaming function in global config mode:

Switch(config)#radius-server roam

The following command turns off the radius roaming function in global config mode：

Switch(config)#no radius-server roam

1.64.7 Display radius information

The following command displays radius configuration information in normal mode / privileged mode：

Switch#show radius-server

1.65 Configuration example

Open the 802.1x protocol, configure the port GE1 / 1 as auto, configure the master authentication server as 198.168.80.111, and configure the shared key of the switch as ABCDEF。

Switch#

Switch# dot1x

Switch#config t

Switch(config)#radius-server host 198.168.80.111

Switch(config)#radius-server key abcdef

Switch(config)# interface ge1/1

Switch(config-ge1/1)# dot1x control auto

1.66 TACACS+ Introduction

TACACS + authentication and authorization provides more rigorous user authority management, which can not only verify the legitimacy of users, but also authorize commands. After the TACACS + authentication is enabled, the user needs to verify the user name and password through the TACACS + server when accessing the switch. Only when the user name and password are correct and consistent can they pass the authentication. Users can access the switch after authentication.

TACACS + also divides users' permissions into two levels: ordinary users and privileged users. Ordinary users can only stay in the normal mode of CLI command line interface, and privileged users can access all modes of CLI command line interface. Based on the permission level, the command execution permission is also set. When a user enters a command (except enable, end and exit), he must verify his permission on the TACACS + server. If the verification fails, he will not execute it.

TACACS + authentication and authorization function is only applicable to telnet and SSH terminals, and does not control console terminals. When accessing the switch through telnet or SSH terminal, the user name and password need to be verified. The CLI can be accessed only after the user name and password are verified. During SSH access, only privileged users can pass through. TACACS + authentication is also applied to web login, but only verifies password privileges and permissions without command authorization.

By default, the switch does not turn on the TACACS + function. At this time, Telnet, SSH or web login all use the multi-user management function. After the TACACS + function is turned on, the multi-user management function can continue to be configured, but it is not actually used.

The commands related to TACACS + authentication authorization are shown in the table below：

Command	Description	CLI mode
tacacsplus enable	Turn on the TACACS + function	Global configuration mode
tacacsplus disable	Turn off the TACACS + function	Global configuration mode
tacacsplus host <server-ip>	Configure the primary server address and	Global configuration mode

	support IPv4 and IPv6. It is recommended to use ACS of Cisco	
tacacsplus option-host <server-ip>	Configure the address of the standby server and support IPv4 and IPv6. It is recommended to use ACS of Cisco	Global configuration mode
tacacsplus key WORD	Configure the shared key, which is used to encrypt the transmission data and must be consistent with the configuration on the server	Global configuration mode
tacacsplus auth-type (PAP|CHAP)	Select the authentication method. The supported methods include PAP and chap. PAP is the default mode, and the field encapsulates the secret. Chap encapsulates the MD5 check code of the secret.	Global configuration mode
show tacacsplus	View TACACS + configuration information	Global configuration mode
no tacacsplus host	Clear primary server address	Global configuration mode
no tacacsplus key	Clear shared key	Global configuration mode

GMRP configuration

This chapter mainly includes the following contents：

- GMRP Introduction
- Configure GMRP
- Display GMRP

1.67 GMRP Introduction

At present, GMRP (GARP Multicast Registration Protocol) is a multicast registration protocol based on GARP, which is used to maintain the multicast registration information in the switch. All switches supporting GMRP can receive the multicast registration information from other switches, dynamically update the local multicast registration information, and spread the local multicast registration information to other switches. This information exchange mechanism ensures the consistency of multicast information maintained by all equipment supporting GMRP in the same switching network.

When a host wants to join a multicast group, it will send a GMRP join message. The switch adds the port receiving the GMRP join message to the multicast group, and broadcasts the GMRP join message in the VLAN where the receiving port is located. The multicast source in the VLAN can know the existence of multicast members. When the multicast source sends the multicast message to the multicast group, the switch only forwards the multicast message to the port connected to the multicast group member, so as to realize the two-layer multicast in the VLAN。

1.68 Configure GMRP

GThe main configurations of MRP include:
Open GMRP
View GMRP
In the configuration task, the global GMRP must be enabled before the port GMRP can be enabled。

1.68.1 Turn on GMRP settings

Command	Description	CLI mode

set gmrp enable | disable	Enable / de enable global VLAN GMRP	Global configuration mode
set gmrp enable vlan <vlan-id>	Enable global specific VLAN GMRP	Global configuration mode
set gmrp registration{fixed | forbidden | normal} <if-name>	Configure interface registration multicast mode	Global configuration mode
set gmrp timer {join | leave | nleaveall} <time-value>	Configure the time of various timers	Global configuration mode
set port gmrp enable <if-name>	Enable port GMRP function	Global configuration mode
set port gmrp disable <if-name>	Disable GMRP function of port	Global configuration mode

1.68.2 View GMRP information

After completing the above configuration, execute the show command in privileged mode to display the operation of GMRP after configuration, and verify the effect of configuration by viewing the display information。

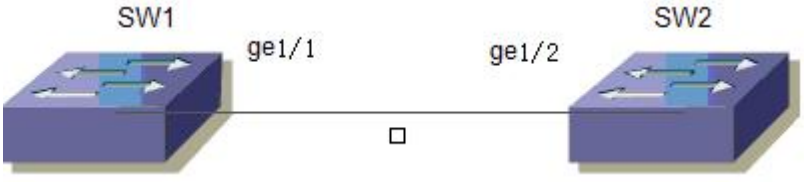
Command	Description	CLI mode
show gmrp configuration	View GMRP configuration information	Privileged mode
show gmrp machine	View GMRP state machine information	Privileged mode
show gmrp statistics vlanid	View GMRP statistics for specific vlanids	Privileged mode
show gmrp timer <ifname>	View the timer information of specific port	Privileged mode

1.69 GMRPTypical configuration example

1. Networking requirements

In order to realize the dynamic registration and update of multicast information between switches, GMRP needs to be started on the switch

2. Networking diagram



GMR example networking diagram

3. Configuration steps

Configure SW1

Start global GMRP

Switch(config)# set gmrp enable

Start GMRP on Gigabit Ethernet port GE1 / 1

Switch(config)# set port gmrp enable ge1/1

Switch(config)#

Configure SW2

Start global GMRP

Switch(config)# set gmrp enable

Start port GMRP on Gigabit Ethernet port GE1 / 2Switch(config)# set port gmrp enable ge1/2

Switch(config)#

Configure IGMP SNOOPING

In man / Internet, when unicast is used to send the same data packets to multiple rather than all recipients in the network, due to the need to copy packets to each receiving endpoint, the number of packets to be sent will increase linearly with the increase of the number of recipients, which will increase the overall burden of hosts, switching and routing equipment and network bandwidth resources, Efficiency is greatly affected. With the increasing demand of multi-point video conference, video on demand and group communication applications, multicast has increasingly become a widely used

transmission mode in multi-point communication in order to improve resource utilization.

The switch realizes IGMP snooping function to serve multicast applications. IGMP snooping monitors IGMP packets on the network to realize dynamic learning of IP multicast MAC address.

This chapter describes the concept and configuration of IGMP snooping, mainly including the following contents：

- IGMP SNOOPING introduction
- IGMP SNOOPING configuration
- IGMP SNOOPING configuration example

1.70 IGMP SNOOPING introduction

In traditional networks, multicast packets are treated as broadcast packets in a subnet, which is easy to cause large network traffic and network congestion. When IGMP snooping is implemented on the switch, IGMP snooping can dynamically learn the IP multicast MAC address, maintain the output port list of IP multicast MAC address, and make the multicast data flow only sent to the output port, which can reduce the network traffic.

This section mainly includes the following contents:：

- IGMP SNOOPING Processing process
- Layer 2 Dynamic Multicast
- Join a group
- Left a group

1.70.1 IGMP SNOOPING Processing process

IGMP snooping is a layer-2 network protocol that monitors IGMP protocol packets passing through the switch, maintains a multicast group according to the receiving port, VLAN ID and multicast address of these IGMP protocol packets, and then forwards these IGMP protocol packets. Only the ports that join the multicast group can receive the multicast data stream; This reduces the network traffic and saves the network bandwidth。

Multicast group includes multicast group address, member port, VLAN ID and age time.

The formation of IGMP snooping multicast group is a learning process. When a port of the switch receives an IGMP report packet, IGMP snooping will generate a new

multicast group, and the port receiving the IGMP report packet will be added to the multicast group. When the switch receives an IGMP query packet, if the multicast group already exists in the switch, the port receiving the IGMP query will also join the multicast group, otherwise it will only forward the IGMP query packet. IGMP snooping also supports the leave mechanism of IGMP V2; If IGMP snooping is configured with fast leave as enable, its receiving port can leave the multicast group immediately when it receives the leave packet of IGMP V2; If the fast leave timeout is configured, the multicast group will leave the multicast group after the time expires.

IGMP snooping has two update mechanisms. One is the leave mechanism introduced above. In most cases, IGMP snooping deletes expired multicast groups through age time. When the multicast group joins IGMP snooping, the joining time is recorded. When the multicast group remains in the switch for more than a configured age time, the exchange opportunity deletes the multicast group.

When a port receives a leave protocol packet, the port will be deleted from its multicast group immediately, which may affect the continuity of network data flow; Because a hub or network device without IGMP snooping function may be connected under this port, many devices receiving multicast data streams are connected under this device. When a device sends a leave, it may affect other devices and cannot receive multicast data streams. The fast leave timeout mechanism can prevent this from happening. Configure a departure waiting time through fast leave timeout. After receiving the leave packet, the port waits for a long time for fast leave timeout and then deletes it from the multicast group it belongs to, which may ensure the continuity of network multicast flow。

1.70.2 Layer 2 Dynamic Multicast

The multicast MAC address entries in the layer 2 hardware multicast forwarding table can be obtained through IGMP snooping dynamic learning. The IP multicast MAC address is dynamically learned through IGMP snooping.

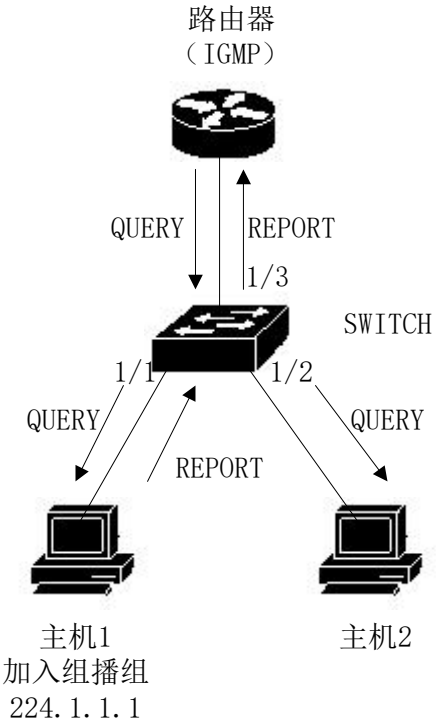
When the switch turns off IGMP snooping, the layer-2 hardware multicast forwarding table is in the unregistered forwarding mode, and the multicast MAC address cannot be dynamically learned. There are no entries in the layer-2 hardware multicast forwarding table, and all layer-2 multicast data streams are treated as broadcast.

When the network has a multicast environment, in order to effectively control the multicast traffic of the network, the switch can turn on IGMP snooping. At this time, the

layer-2 hardware multicast forwarding table is in the registered forwarding mode. The switch can learn the multicast MAC address by listening to the IGMP protocol packet on the network. Only the layer-2 multicast flow matching the entries in the layer-2 hardware multicast forwarding table can be forwarded。

1.70.3 Join a group

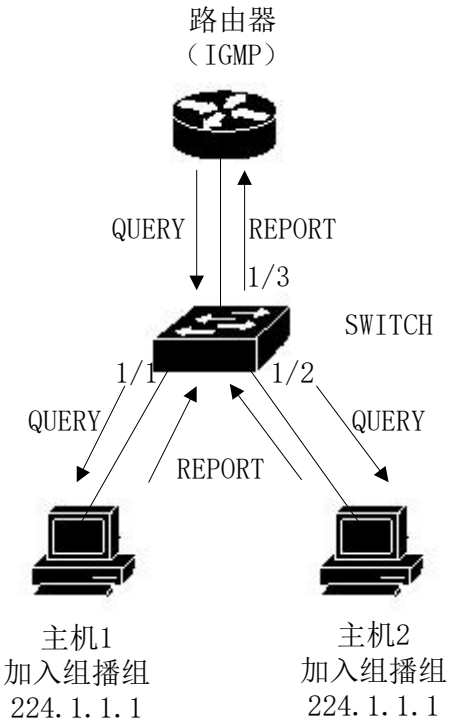
When a host wants to join a multicast group, the host will send an IGMP report packet, which specifies the multicast group that the host wants to join. When the switch receives an IGMP query packet, the switch will forward the packet to all other ports of the same VLAN. When the host under the port wants to join the multicast group receives the IGMP query packet, it will return an IGMP report packet. When the switch receives an IGMP report packet, it will establish a layer-2 multicast entry. The port receiving the IGMP query packet and the port of the IGMP report packet will be added to the layer-2 multicast entry and become its output port。



As shown in the figure above, all devices are in a subnet, assuming that the VLAN of the subnet is 2. The router runs igmpv2 protocol and sends IGMP query packets regularly. Host 1 wants to join multicast group 224.1.1.1. After receiving IGMP query packet from port 1 / 3, the switch will record this port and forward the packet to Ports 1 / 1 and 1 / 2. Host 1 sends back an IGMP report packet after receiving an IGMP query packet. Host 2 does not send an IGMP report packet because it does not want to join the multicast group.

After receiving the IGMP report packet from port 1 / 1, the switch will forward the packet from query port 1 / 3 and create a layer-2 multicast entry (assuming that the entry does not exist). The layer-2 multicast entry includes the following items:：

Layer 2 multicast address	VLAN ID	Output port list
01:00:5e:01:01:01	2	1/1，1/3



As shown in the above figure, the conditions are the same as those in Figure 1. Host 1 has joined multicast group 224.1.1.1, and now host 2 wants to join multicast group 224.1.1.1. When host 2 receives IGMP query packet, it sends back an IGMP report packet. After receiving IGMP report from port 1 / 2, the switch will forward the packet from query port 1 / 3, and add packet port 1 / 2 to the layer-2 multicast entry. The layer-2 multicast entry becomes：

Layer 2 multicast address	VLAN ID	Output port list
01:00:5e:01:01:01	2	1/1，1/2，1/3

1.70.4 Left a group

In order to form a stable multicast environment, devices running IGMP (such as routers) will send an IGMP query packet to all hosts at regular intervals. Hosts that have joined the multicast group or want to join the multicast group will send back an IGMP report after receiving the IGMP query

If the host wants to leave a multicast group, there are two ways: active leaving and passive leaving. Active leave means that the host sends an IGMP leave packet to the router. Passive leave means that the host does not send back IGMP report after receiving the IGMP query sent by the router.

Corresponding to the way the host leaves the multicast group, there are also two ways to leave the layer-2 multicast entry at the port on the switch: timeout leaving and receiving IGMP leave packet leaving.

When the switch does not receive the IGMP report packet of a multicast group from a port for more than a certain time, the port shall be cleared from the corresponding layer 2 multicast entry. If the layer 2 multicast entry has no port, the layer 2 multicast entry shall be deleted.

When the fast leave configuration of the switch is enabled, if a port receives an IGMP leave packet of a multicast group, the port is cleared from the corresponding layer 2 multicast entry. If the layer 2 multicast entry has no port, the layer 2 multicast entry is deleted.

Fast leave is generally used when one port is connected to another host; If there are more than one host under a port, the fast leave timeout waiting time can be configured to ensure the continuity and reliability of multicast streams in the network。

1.70.5 IGMP Interrogator

In a network with three-layer multicast devices, the three-layer multicast devices act as IGMP queries. Layer 2 multicast equipment only needs to listen to IGMP messages, and can establish and maintain forwarding table entries to realize layer 2 multicast. In a network without layer 3 multicast devices, layer 3 multicast devices cannot act as IGMP queries. In order to enable the layer-2 multicast device to monitor IGMP messages, the IGMP query function must be configured on the layer-2 device. The layer-2 multicast device not only acts as an IGMP query, but also monitors IGMP messages, so as to establish and maintain forwarding table entries and realize layer-2 multicast。

working principle

The IGMP query function is that the layer-2 device plays the role of IGMP routing

query, regularly sends IGMP query messages, listens and maintains the IGMP report messages answered by users, and establishes the forwarding table entry of layer-2 multicast. The relevant parameters of the query message sent by IGMP query can be adjusted by the user through configuration.

Start query

The user can configure to enable the query function on the specified VLAN.

Specifies the IGMP version that the query runs

Specifies the IGMP version used by the query message sent by the query, which can be configured as V1 or V2 or V3 version

Configure the source IP of the query

Configure the source IP address carried by the query message sent by the query device,

Configure the query interval of the querier

Configure the time interval of the query message sent by the global query

1.70.6 Igmp snooping Multicast filtering

The equipment running IGMP snooping can control the multicast service range and load, and can effectively prevent illegal multicast flows. By configuring multicast filtering rules globally and applying rules on the interface, you can allow or restrict the participation of specific groups。

1.71 IGMP SNOOPING configuration

1.71.1 IGMP SNOOPING default configuration

IGMP snooping is off by default, and the layer 2 hardware multicast forwarding table is in unregistered forwarding mod

Fast leave is off by default.

The fast leave timeout time is 300 seconds.

The age time of the multicast group report port defaults to 400 seconds.

The age time of multicast group query port is 300 seconds by default。

1.71.2 Open and close IGMP SNOOPING

Open IGMP snooping protocol, which can be opened globally or separately; IGMP snooping of a VLAN can be turned on or off only when IGMP snooping is turned on globally。

Open global IGMP SNOOPING

Switch#configure terminal

Switch(config)#ip igmp snooping

Open IGMP snooping for a VLAN

Switch#configure terminal

Switch(config)#ip igmp snooping vlan <vlan-id>

Close GMP SNOOPING

Switch#configure terminal

Switch(config)#no ip igmp snooping

Close VLAN GMP SNOOPING

Switch#configure terminal

Switch(config)#no ip igmp snooping vlan <vlan-id>

1.71.3 Configure lifetime

Configure multicast group lifetime

Switch#configure terminal

Switch(config)#ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>

Interval is in milliseconds。

Configure query group lifetime

Switch#configure terminal

Switch(config)#ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>

Interval is in milliseconds。

1.71.4 Configure fast-leave

Start fast leave of a VLAN

Switch#configure terminal

Switch(config)#ip igmp snooping fast-leave vlan <vlan-id>

Close fast-leave

Switch#configure terminal

Switch(config)#no ip igmp snooping fast-leave vlan <vlan-id>

Configure fast leave wait time

Switch#configure terminal

Switch(config)# ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>

Restore the default fast leave wait time

Switch#configure terminal

Switch(config)#no ip igmp snooping fast-leave-timeout vlan <vlan-id>

1.71.5 Configure MROUTER

Configure static query port

Switch#configure terminal

Switch#interface ge1/6

Switch(config-ge1/6)#ip igmp snooping mrouter vlan [vlan-id]

1.71.6 Configure IGMP snooping query port function

Configure static query port

Switch#configure terminal

Switch(config)#interface ge1/6

Switch(config-ge1/6)#ip igmp snooping mrouter vlan [vlan-id]

1.71.7 Configure IGMP snooping query function

Start IGMP snooping query function of vlan1

Switch#configure terminal

Switch(config)#ip igmp sno

Switch(config)#ip igmp snooping querier vlan 1

1.71.8 Configure IGMP snooping multicast filtering

Configure port GE1 / 1 to filter the multicast address to 235.0.0.1

Switch#configure terminal

Switch(config)#ip igmp snooping filter-rule 1 deny 235.0.0.1

Switch(config)#interface ge1/1

Switch(config-ge1/1)#ip igmp snooping filter-group 1

1.71.9 display information

Display IGMP snooping configuration information

Switch#show ip igmp snooping

Displays the configuration information of a VLAN

Switch#show ip igmp snooping vlan <vlan-id>

Display aging information of report multicast group

Switch#show ip igmp snooping age-table group-membership

Display aging information of query

Switch#show ip igmp snooping age-table query-membership

Display forwarding information of multicast group

Switch#show ip igmp snooping forwarding-table

Display mrouter information

Switch#show ip igmp snooping mrouter

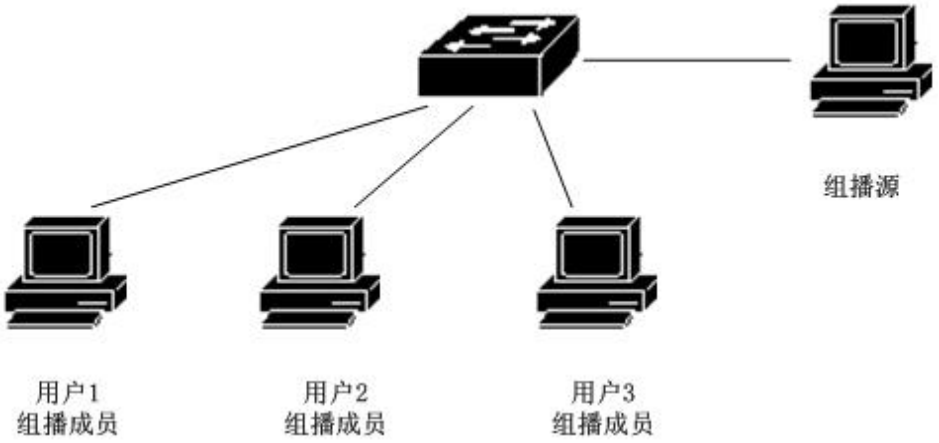
Displays the current configuration of the system, including the configuration of IGMP snooping

Switch#show running-config

1.72 IGMP SNOOPING Configuration example

1.72.1 Configuration

Enable IGMP snooping on the switch, and users 1, 2 and 3 can join a specific multicast group。



Switch#config t

Switch(config)#ip igmp snooping

Switch(config)#vlan database

Switch(config-vlan)#vlan 200

Switch(config-vlan)#exit

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 200

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

```
Switch(config-ge1/2)#switchport access vlan 200
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 200
Switch(config)#ip igmp snooping vlan 200
Switch(config)#ip igmp snooping group-membership-timeout 60000 vlan 200
```

MVR Configuration

This chapter mainly includes the following contents：

- MVR introduction
- Configure MVR

1.73 MVR introduction

Multicast VLAN registration (MVR) is applied to multicast streaming applications in service provider networks, such as TV on demand. MVR allows subscribers on the port to subscribe to or cancel the multicast flow in the multicast VLAN, and allows the data flow in one multicast VLAN to be shared by other VLANs. MVR has two purposes: (1) through simple configuration, it can effectively and safely transfer multicast streams between VLANs; (2) Support dynamic joining and leaving of multicast groups;

The operation mode of MVR is similar to IGMP snooping. The two functions can be started at the same time. MVR only handles the joining and leaving of the configured

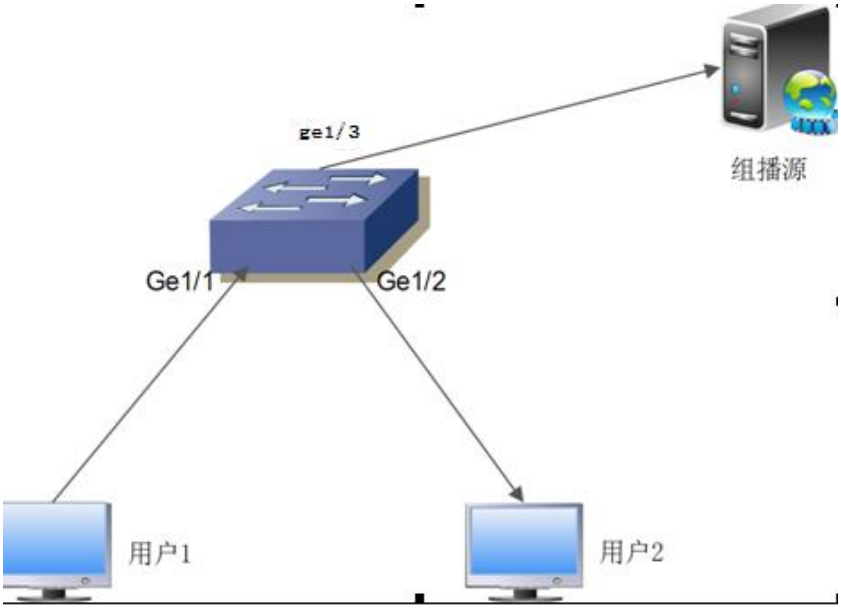
multicast group, and the joining and leaving of other groups are managed by IGMP snooping. The difference between the two is that the multicast flow in IGMP snooping can only be forwarded in one VLAN, while the multicast flow of MVR can be forwarded in different VLANs

1.74 Configure MVR

Command	Description	CLI mode
mvr (enable|disable)	Start global MVR	Global configuration mode
no mvr	Clear all MVR configurations	Global configuration mode
mvr group A.B.C.D	Configure IP multicast address	Global configuration mode
no mvr group A.B.C.D	Delete IP multicast address	Global configuration mode
mvr group A.B.C.D <1-256>	Configure IP multicast address and configure a continuous MVR group address	Global configuration mode
mvr vlan <1-4094>	Specifies the VLAN that receives multicast data	Global configuration mode
no mvr vlan	Restore the default vlan1 for receiving multicast data	Global configuration mode
mvr-interface (enable|disable)	Start interface MVR	Interface configuration mode
show mvr	Display MVR configuration information	Privileged mode

1.75 MVR Configuration example

The networking topology is shown in the figure below. User 1 and user 2 belong to VLAN 10 and VLAN 20 respectively. User 1 and user 2 watch the same program. The program range is 225.1.1.1 ~ 225.1.1.64, and the MVR VLAN is 100：



Configure VLAN, start global IGMP snooping, configure MVR VLAN, MVR program group range, and enable MVR globally：

Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)# mvr enable
Switch(config)#mvr vlan 100
Switch(config)#mvr group 225.1.1.1 64
Switch#

Configure switch user ports GE1 / 1, GE1 / 2, and uplink ports GE1 / 3：
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode hybrid
Switch(config-ge1/1)# switchport hybrid native vlan 10
Switch(config-ge1/1)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/1)#mvr enable
Switch(config-ge1/1)#

Switch#configure terminal
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode hybrid
Switch(config-ge1/2)# switchport hybrid native vlan 20
Switch(config-ge1/2)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/2)#mvr enable
Switch(config-ge1/2)#

Switch#configure terminal
Switch(config)#interface ge1/3
Switch(config-ge1/3)# switchport access vlan 100
Switch(config-ge1/3)#

Configure DHCP SNOOPING

In the dynamic access network environment, the host obtains the IP address and network parameters through the DHCP server. DHCP snooping is a snooping protocol for ARP attacks. By listening to DHCP messages, dynamically bind the IP address and client MAC address assigned by DHCP server to the client, so as to filter ARP attack messages on the switch.

The switch supports DHCP snooping function, which can effectively defend against ARP attacks. DHCP snooping listens to DHCP messages on the network and binds port ARP information.

Four physical ports linked to DHCP server can be configured to prevent unknown server from interfering with the network to a certain extent.

This chapter describes the concept and configuration of DHCP snooping, mainly including the following contents：

- DHCP SNOOPING introduction
- DHCP SNOOPING configuration
- DHCP SNOOPING configuration example

1.76 DHCP SNOOPING introduction

ARP protocol has caused loopholes in network security due to its simple trust mechanism. When the ARP attack message carrying false MAC information reaches the host, it will directly overwrite the local ARP cache table without restriction, resulting in normal data flow to the attacker. Therefore, the ARP information binding of the port is realized on the network layer-2 switch, which can effectively filter the ARP attack message and make the attack message unable to reach the attacked host. If an unpredictable DHCP server enters the network, it will lead to confusion in IP address allocation. The DHCP snooping protocol provides the physical port of the binding link server. The unspecified physical port cannot forward the DHCP protocol packet sent by the DHCP server, which can reduce the chance of this unknown server entering the network.

This section mainly includes the following contents:：

- DHCP SNOOPING Processing process
- DHCP SNOOPING Binding table

- DHCP SNOOPINGBind the physical port of the server

1.76.1 DHCP SNOOPINGProcessing process

DHCP snooping protocol only listens to dhcprequest, dhcpack and dhcprelease messages, does not receive other types of DHCP messages, and binds the mapping relationship between IP and MAC according to these messages.

The global DHCP snooping switch is responsible for opening the switch to receive DHCP messages, that is, IP messages with UDP ports of 67 and 68。

1.76.2 DHCP SNOOPING Binding table

DHCP snooping binding table entries are indexed by MAC addresses, including entry type, IP address, MAC address, interface information, delay timer and lease timer. There are two types: req and ACK. The entry of req indicates that the dhcprequest message has been received, but the dhcpack message has not been received. At this time, start the delay timer, and the default time interval is 10 seconds. If the dhcpack message is not received within 10 seconds, the binding table entry of this req type will be deleted; An ACK type entry indicates that the dhcpack message is received. The recorded IP address is the IP address assigned by the server. At this time, start the lease timer. The time interval is the lease value provided by the DHCP server contained in the dhcpack message. When the contract is renewed, the timer is restarted. When the lease expires, the binding table entry is deleted. The interface information records the interface where the client is located, that is, the interface corresponding to the binding relationship between IP address and MAC address.

When receiving the dhcprequest message, create a binding table entry with the entry type of req, record the IP address, MAC address, interface information, and start a 10 second delay timer.

When the dhcprequest message is received and there is already a binding table entry of req type, update the entry and restart the delay timer.

When the dhcprequest message is received and the binding table entry of ACK type already exists, the interface information is recorded.

When the dhcpack message is received, if there are req type binding table entries, record the IP address assigned by the server in the dhcpack message, close the delay timer and start the lease timer.

When the dhcpack message is received and there is no req type binding table entry, the message is discarded.

When the dhcpack message is received, the binding table entry of ACK type already exists. If the interface has been changed, delete the binding table entry of the original interface and update the entry.

If the interface does not change and the IP address assigned by the server changes, delete the binding table entry of the original interface and update the entry.

If the interface has not changed and the IP address has not changed, it indicates that it is a renewal process. Just restart the lease timer.

If the delay timer times out, the binding table entry of req type is deleted。

If the lease timer times out, the binding table entry of ACK type is deleted。

1.76.3 DHCP SNOOPING Specify the physical port of the linked server

DHCP snooping specifies the physical port of the linked server. DHCP messages can be received only on the specified port. If there are multiple DHCP servers in the network, the offer provided by the server from the unspecified port will be filtered and the client cannot be assigned an IP address. The specified port is conducive to the unified allocation of IP addresses in the network, so as to avoid that the address pool of unknown servers is not in the IP planning, and some clients cannot connect to the network normally. To a certain extent, it reduces the probability of abnormal network communication caused by private access to the server。

1.77 DHCP SNOOPING Configuration

1.77.1 DHCP SNOOPING Default configuration

DHCP SNOOPING The default is off。

DHCP SNOOPING The default time interval of the entry delay timer of type req in the binding table is 10 seconds。

1.77.2 Global on and off DHCP SNOOPING

DHCP snooping of an interface can be turned on or off only after DHCP snooping is turned on globally. DHCP snooping of all interfaces can be turned off only after DHCP snooping of all interfaces is turned off globally.

Open global DHCP snooping

Switch#configure terminal

Switch(config)#ip dhcp snooping [IF_LIST]

The parameter is the physical port list of the linked DHCP server to be bound. A total of four ports can be specified. The port list is separated by ",", such as GE1 / 1, GE1 / 4 and GE1 / 5

Turn off global DHCP snoopingSwitch#configure terminal

Switch(config)#no ip dhcp snooping

1.77.3 Interface on and off DHCP SNOOPING

Open a port DHCP SNOOPING

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#dhcp snooping

Close a port DHCP SNOOPING

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no dhcp snooping

1.77.4I nterface on and off DHCP SNOOPING OPTION82

Open a port DHCP SNOOPING **OPTION82**

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#dhcp snooping **option82**

Open a port DHCP SNOOPING **OPTION82**

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no dhcp snooping **option82**

Configure the circuit ID of DHCP snooping option82 of a port

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)# dhcp snooping option82 circuit-id vlan111

Delete the circuit ID of DHCP snooping option82 of a port

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)# no dhcp snooping option82 circuit-id

1.77.5 display information

Display DHCP snooping configuration information

Switch#show dhcp snooping

Display DHCP snooping binding table information

Switch#show dhcp snooping binding-table

Displays the current system configuration, including DHCP snooping configuration。

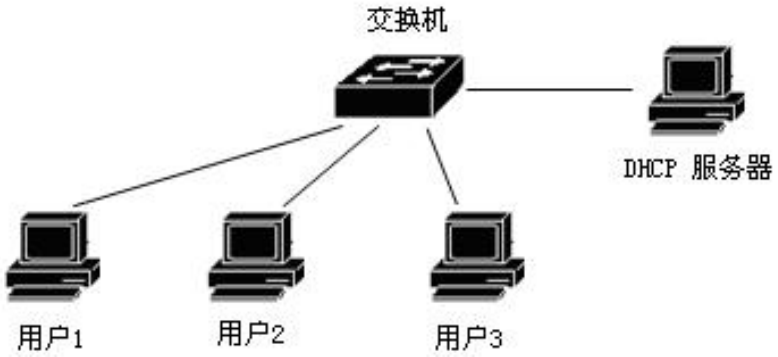
Switch#show running-config

1.78 DHCP SNOOPING Configuration example

1.78.1 Configuration

Enable the DHCP snooping function on the layer-2 switch. Users 1, 2 and 3

dynamically obtain the IP address and network parameters through the DHCP server. The interface of user 1, user 2 and user 3 starts the DHCP snooping option82 function, the circuit ID is AAA, and the ARP information is dynamically bound on the interface。



Switch#configure terminal
Switch(config)#ip dhcp snooping ge1/5
Switch(config)#interface ge1/1
Switch(config-ge1/1)#dhcp snooping
Switch(config-ge1/1)#dhcp snooping option82
Switch(config-ge1/1)#dhcp snooping option82 circuit-id aaa
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#dhcp snooping
Switch(config-ge1/2)#dhcp snooping option82
Switch(config-ge1/2)#dhcp snooping option82 circuit-id aaa
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#dhcp snooping
Switch(config-ge1/3)#dhcp snooping option82
Switch(config-ge1/3)#dhcp snooping option82 circuit-id aaa
Switch(config-ge1/3)#end
View DHCP snooping information
Switch#show dhcp snooping
DHCP Snooping is enabled globally
DHCP Server interface: ge1/5
Enable interface: ge1/1 ge1/2 ge1/3
Option 82 interface: ge1/1(Circuit ID: aaa) ge1/2(Circuit ID: aaa) ge1/3(Circuit

ID: aaa)

Switch#
Switch#show dhcp snooping binding-table

IP	MAC	FLAG	PORT	LEASE
192.168.1.100	00:11:5b:34:42:ad	ACK	ge1/1	23:59:58
192.168.1.101	00:11:64:52:13:5d	ACK	ge1/2	23:50:01
192.168.1.102	00:11:80:4d:a2:46	ACK	ge1/3	20:34:45

1.79DHCP SNOOPING Configuration troubleshooting

If DHCP snooping configuration fails, it may be caused by the following reasons:

1. Run out of CFP resources.
2. If an interface is configured with ACL filtering function, the global opening of DHCP snooping fails
3. If an interface is configured with IP and MAC binding, the global opening of DHCP snooping fails
4. The ACL filtering function is configured for the current interface.
5. The 802.1x anti ARP Spoofing function is enabled on the current interface.
6. The configured interface is a three-layer interface or trunk interface。

DHCP CLIENT Configuration

1.80 DHCP CLIENT introduction

DHCP (Dynamic Host Configuration Protocol) is based on the client / server working mode. The function of DHCP client is that the three-layer interface address of the switch can obtain the address and gateway through the DHCP server.

This section mainly includes the following contents:：

- DHCP CLIENT Configuration

1.81 DHCP CLIENT Configuration

Open the DHCP client function of interface vlan1
switch(config)#
Switch(config)#interface vlan1
Switch(config-vlan1)#dhcp client enable

Re acquire the IP address of interface vlan1
switch(config)#
Switch(config)#interface vlan1
Switch(config-vlan1)#dhcp client renew

Release the IP address of interface vlan1
switch(config)#
Switch(config)#interface vlan1
Switch(config-vlan1)#dhcp client release

Configure DHCP RELAY

This chapter mainly includes the following contents：

- DHCP RELAY introduction
- DHCP RELAY configuration
- DHCP RELAY configuration example

1.82 DHCP RELAY introduction

DHCP (Dynamic Host Configuration Protocol) is an enhanced version of BOOTP. It dynamically configures the network environment for hosts on the network, which is divided into server and client. The server centrally manages the IP network data, processes the requests of the client, and dynamically configures the TCP / IP environment of the client. When DHCP works, at least one server is on the network. It can listen to the DHCP requests of hosts on the network and negotiate TCP / IP parameters. There are two modes of its allocation: automatic and dynamic. In automatic mode, once the client obtains the IP address, it will permanently use the address. In dynamic mode, the IP address obtained by the client has a lease. Once the lease expires, the IP needs to be released; You can also renew the contract in advance or rent other IP. Dynamic allocation can effectively solve the problem of insufficient actual IP.

Working process of DHCP:

If the client logs into the network for the first time and has no IP data, it will broadcast a discover message with source address 0.0.0 and destination address 255.255.255.255. If the server does not respond, four discover requests will be issued according to a certain interval.

When the server receives discover, it selects an idle IP to respond to the offer message from the client.

If there are multiple servers on the network, the client will receive multiple offer messages. Generally, select the offer that arrives first and broadcast the request message to tell all servers which server has received the IP address provided by.

If the client finds that the IP has been used through ARP, it sends a decline message to the server to reject the offer; And restart the discover process.

After receiving the request message, the server will send an ACK message to the client to confirm the effectiveness of the lease.

If the client has applied for a DHCP lease, it is generally unnecessary to use the discover process. Before the lease expires, send a request for renewal to the server using the leased IP. The server will try to let the client use the original IP. If there is no problem, the server will respond to the ACK message for confirmation. If the IP has been used by other clients, the server responds to the NACK message and rejects the renewal request.

The client can use the release message to actively terminate the lease.

The workstation sends a request when starting up; The request will be sent again at half of the lease. If there is no confirmation, the IP can still be used; A request will also be sent when the lease is 3 / 4. If there is no confirmation at this time, this IP can no longer be used.

The discover message is published in broadcast mode. It can only be in the same network segment, and the router will not spread the broadcast message. When the server and the client are not in the same network segment, and the client has not obtained the IP environment setting and does not know the location of the router, the discover message cannot reach the server. In order to solve this problem, the function of DHCP relay can be used to let the router transfer DHCP protocol messages, so that DHCP can operate across network segments。

1.83 DHCP RELAY Configuration

The DHCP relay function is related to the interface, which realizes the protocol message forwarding of DHCP across network segments, and carries out relevant configuration in the interface mode.

DHCP relay configuration includes：

- Start the DHCP relay function of the interface

1.83.1 Start the DHCP relay function of the interfac

Mode: interface configuration mode

Command: DHCP relay < ip-address-1> [ip-address-2] Open DHCP relay protocol on the interface

Command: no DHCP relay Close the DHCP relay protocol on the interface

Default: do not open DHCP relay protocol。

1.83.2 display information

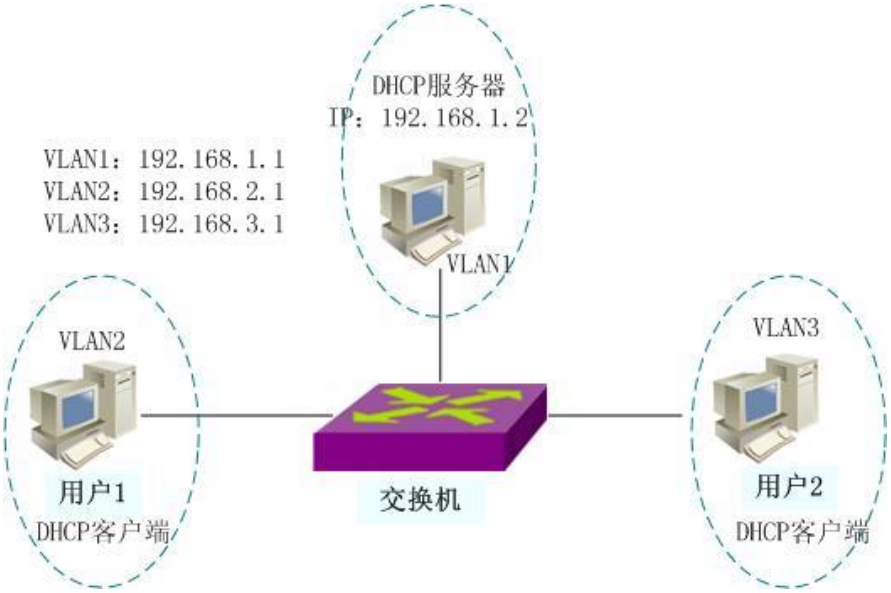
Display DHCP relay configuration information

Switch#show dhcp relay

1.84 DHCP RELAY configuration example

(1) Configuration

The DHCP relay switch 1 needs to forward the DHCP relay request and reply to the DHCP relay switch 2. Enable user 1 and user 2 to obtain legal IP addresses through DHCP servers in different network segments, so as to access the network。



Switch>en

Switch# configure terminal

Switch(config)# vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Switch(config-vlan)#exit

Switch(config)#ip interface vlan 2

Switch(config)#ip interface vlan 3

Switch(config)#int ge1/2

Switch(config-ge1/2)#sw access vlan 2

```
Switch(config-ge1/2)#int ge1/3
Switch(config-ge1/3)#sw access vlan 3
Switch(config-ge1/3)# interface vlan2
Switch(config-vlan2)#ip address 192.168.2.1/24
Switch(config-vlan2)#dhcp relay 192.168.1.2
Switch(config-vlan2)#interface vlan3
Switch(config-vlan3)#ip address 192.168.3.1/24
Switch(config-vlan3)#dhcp relay 192.168.1.2
```

(2) Verification

```
show running-config          Display configuration command
show dhcp relay      Display DHCP relay configuration information
```

Configure DHCP SERVER

This chapter mainly includes the following contents：

- DHCP SERVER introduction
- DHCP SERVER configuration
- DHCP SERVER configuration example

1.85 DHCP SERVER introduction

DHCP (Dynamic Host Configuration Protocol) is an enhanced version of BOOTP. It dynamically configures the network environment for hosts on the network, which is divided into server and client. The server centrally manages the IP network data, processes the requests of the client, and dynamically configures the TCP / IP environment of the client. When DHCP works, at least one server is on the network. It can listen to the DHCP requests of hosts on the network and negotiate TCP / IP parameters. There are two modes of its allocation: automatic and dynamic. In automatic mode, once the client obtains the IP address, it will permanently use the address. In dynamic mode, the IP address obtained by the client has a lease. Once the lease expires, the IP needs to be released; You can also renew the contract in advance or rent other IP. Dynamic allocation can effectively solve the problem of insufficient actual IP.

Working process of DHCP:

If the client logs into the network for the first time and has no IP data, it will broadcast a discover message with source address 0.0.0 and destination address 255.255.255.255. If the server does not respond, four discover requests will be issued according to a certain interval.

When the server receives discover, it selects an idle IP to respond to the offer message from the client.

If there are multiple servers on the network, the client will receive multiple offer messages. Generally, select the offer that arrives first and broadcast the request message to tell all servers which server has received the IP address provided by.

If the client finds that the IP has been used through ARP, it sends a decline message to the server to reject the offer; And restart the discover process.

After receiving the request message, the server will send an ACK message to the client to confirm the effectiveness of the lease.

If the client has applied for a DHCP lease, it is generally unnecessary to use the discover process. Before the lease expires, send a request for renewal to the server using the leased IP. The server will try to let the client use the original IP. If there is no problem, the server will respond to the ACK message for confirmation. If the IP has been used by other clients, the server responds to the NACK message and rejects the renewal request.

The client can use the release message to actively terminate the lease.

The workstation sends a request when starting up; The request will be sent again at half of the lease. If there is no confirmation, the IP can still be used; A request will also be sent when the lease is 3 / 4. If there is no confirmation at this time, this IP can no longer be used.

The DHCP server protocol module receives discover, request, decline and release messages, which are used to allocate IP addresses to clients in the network and maintain their own address pool information and allocated client information。

1.86 DHCP SERVER configuration

DHCP server function needs to be configured in global mode, interface mode and address pool mode, including startup command, address pool configuration, global setting, mode switch and other commands.

DHCP server configuration includes：

- Start global DHCP server function
- Start interface to receive DHCP server message
- Configure address pool
- Configure address pool range
- Configure address pool subnet mask
- Configure address pool lease
- Configure address pool default gateway
- Configure address pool DNS server
- Configure address pool to exclude addresses manually

1.86.1 Start global DHCP server function

Mode: global configuration mode

Command: IP DHCP server Start global DHCP server protocol

Command: no IP DHCP server Turn off the global DHCP server protocol

Default: do not open DHCP server protocol; Use this command to start the DHCP server protocol。

1.86.2 Start interface to receive DHCP server message

Mode: interface configuration mode

Command: DHCP server listen The interface starts to receive DHCP server protocol message

Command: no DHCP server listen interface closes and does not receive DHCP server protocol messages

Default: the interface is not started and cannot receive DHCP server protocol messages。

1.86.3 Configure address pool

Mode: global configuration mode

Command: DHCP server pool < pool name > Create an address pool and enter address pool mode

Command: no DHCP server pool < pool name > Delete the specified address pool

Parameter: < pool name > address pool name, used to distinguish different address pools. Maximum 16 characters.

Default: no address pool is configured. Configure the address pool, only create the address pool name, enter the address pool configuration mode, and do not configure the actual address。

1.86.4 Configure address pool range

Mode: address pool configuration mode

Command: range < low address > < high address > Configure address pool range

Command: no range Delete address pool range

Parameter: < low address > starting address of address pool range, dotted decimal format< High address > the end address of the address pool range, in dotted decimal format.

Default: the address pool range is not configured. When a range is configured in the address pool, each dynamically assignable address entry in the range in the address pool is created。

1.86.5 Configure address pool subnet mask

Mode: address pool configuration mode

Command: subnet mask < address > Configure address pool subnet mask

Parameter: < address > mask address, dotted decimal format, variable length mask.

Default: 255.255.255.0. The default is 24 bit mask。

1.86.6 Configure address pool lease

Mode: address pool configuration mode

Command: leave [< days > < hours > < minutes > |infinite] Configure address pool lease

Parameter: < days > is the number of days, ranging from 0 to 999< Hours > is the number of hours, ranging from 0 to 23< Minutes > is the number of minutes, ranging from 0 to 59; Are integer numbers. Infinite is an infinite lease.

Default: the lease is 8 days。

1.86.7 Configure address pool default gateway

Mode: address pool configuration mode

Command: default router < IP address > Configure address pool default gateway

Default route command Delete address pool default gateway

Parameter: < IP address > default gateway IP address, dotted decimal format, which should be within the same network segment as the address pool.

Default: no default gateway is configured。

1.86.8 Configure address pool DNS server

Mode: address pool configuration mode

Command: DNS server < IP address1 > [IP address2] Configure address pool DNS server

Command: no DNS server Delete address pool DNS server

Parameters: < IP address1 > and < IP address2 > are the IP addresses of DNS servers in decimal format. At most two DNS servers or one can be configured. If two sets are configured, they should be entered in one command instead of twice. If it is entered twice, the DNS server IP address entered later will overwrite the DNS server address configured previously, regardless of whether one or two are configured previously.

Default: do not configure DNS server。

1.86.9 Configure address pool to exclude addresses manually

Mode: address pool configuration mod

Command: exclude address < IP address > Configure address pool to exclude addresses manually

Command: exclude address < low address > < high address > configure manual exclusion of address range

Command: no exclude address < IP address > Restore a manually excluded address

Command: exclude address < low address > < high address > configure manual exclusion address range recovery

Command: no exclude address all Recover all manually excluded addresses in the address pool

Parameters: < IP address > manually excluded IP address, dotted decimal format. One command can exclude one available address in the address pool at a time< Low address > and < high address > are the starting and ending IP addresses of the manually excluded address range, in decimal format. One command can exclude multiple consecutive available addresses in the address pool range at one time. If there are addresses in the range that are manually excluded, just skip without any prompt. Manual exclusion, that is, the address entry within the address pool will not be dynamically allocated.

Default: manual exclusion address is not configured。

1.86.10 Configure option82

Mode: address pool configuration mode

Command: option82 circuit ID < circuit ID > Configure the circuit ID of option82

Parameter: < circuit ID > string, the maximum length is 64。

1.86.11 Clear assigned address table entries

Exec configuration mod

Command: clear DHCP server address {[IP address] | [all]}

Delete an assigned address or all address table entries。

1.86.12 Clear conflicting address table entries detected

Exec configuration mod

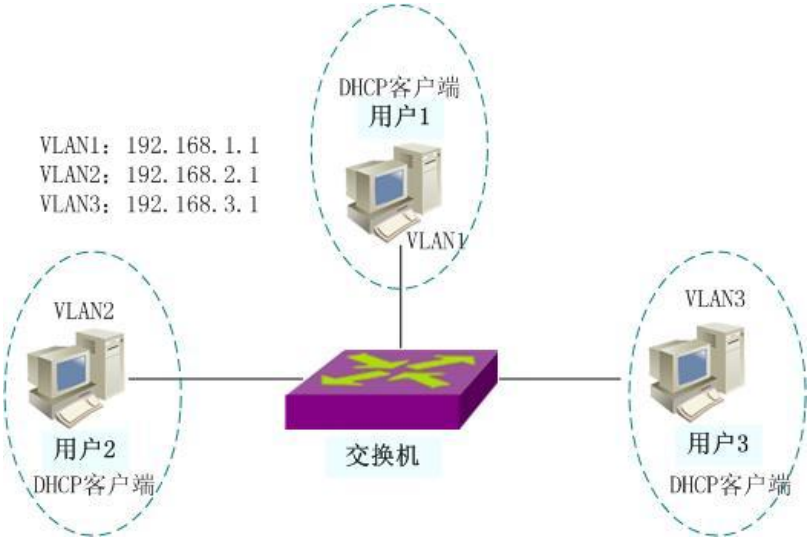
Command: clear DHCP server address conflict {[IP address] | [all]

Delete the addresses automatically excluded due to conflict detection, delete all conflict addresses, and delete a single address automatically excluded due to conflict。

1.87 DHCP SERVER Configuration example

(1) Configuration

The corresponding address pool is configured for the clients of vlan1, vlan2 and vlan3 subnets, so that the switch as DHCP server can assign the IP address of the corresponding network segment to the clients in these three subnets。




```
Switch>en
Switch# configure terminal
Switch(config)#ip dhcp server
Switch(config)# vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#exit
Switch(config)#ip interface vlan 2
Switch(config)#ip interface vlan 3
Switch(config)#int ge1/2
Switch(config-ge1/2)#sw access vlan 2
Switch(config-ge1/2)#int ge1/3
Switch(config-ge1/3)#sw access vlan 3
Switch(config-ge1/3)#interface vlan2
Switch(config-vlan2)#ip address 192.168.2.1/24
Switch(config-vlan2)#dhcp server listen
Switch(config-vlan2)#interface vlan3
```

```
Switch(config-vlan3)#ip address 192.168.3.1/24
Switch(config-vlan3)#dhcp server listen
Switch(config-vlan3)#interface vlan1
Switch(config-vlan1)#dhcp server listen
Switch(config)#dhcp server pool a
Switch(config-dhcp)#range 192.168.2.1 192.168.2.20
Switch(config-dhcp)#lease 2 0 0
Switch(config-dhcp)#default-router 192.168.2.1
Switch(config-dhcp)#dns-server 1.1.1.1 2.2.2.2
Switch(config-dhcp)#exclude-address 192.168.2.10
Switch(config-dhcp)#exit
Switch(config)# dhcp server pool b
Switch(config-dhcp)#range 192.168.3.2 192.168.3.20
Switch(config-dhcp)#default-router 192.168.3.1
Switch(config-dhcp)#exit
Switch(config)# dhcp server pool c
Switch(config-dhcp)#range 192.168.1.2 192.168.1.20
Switch(config-dhcp)#default-router 192.168.1.1
Switch(config-dhcp)#exit
```

(2) verification

show running-config Display configuration command

show dhcp server Display global configuration information

show dhcp server pool [pool-name] Display the address pool configuration information, which can display the information of a single address pool。

show dhcp server address Displays the information of the assigned address table entry。

In the actual network, the access security of the network is a problem that the administrator is very concerned about. The switch supports ACL filtering and provides network access security. By configuring ACL rules, the switch filters the input data stream according to these rules to achieve network access security.

This chapter describes how to configure ACL, mainly including the following contents：

- ACLIntroduction to resource library
- Introduction to ACL filtering
- ACL repository configuration
- ACL filtering configuration
- ACL configuration example

1.88 ACLIntroduction to resource library

ACL (access list control) repository is a collection of multiple groups of access rules. ACL repository has no function of controlling data forwarding, but a collection of rules with conflict sorting. After the ACL resource library is referenced by applications, these applications control the forwarding of data according to the rules provided by ACL resources. ACL can be applied to port access filtering, service access filtering, QoS and so on.

ACL resource library includes standard IP rule group (group number 1 ~ 991300 ~ 1999), extended IP rule group (group number 100 ~ 1992000 ~ 2699), IP MAC group < group number 700 ~ 799 >, ARP group (group number 1100 ~ 1199); The priority of conflict rules is automatically sorted within each group of rules. When a user configures an ACL rule, the system will insert the rule into the corresponding position according to the sorting rule.

In application, when a data packet passes through a port, the switch compares the fields in each rule with all the corresponding fields in the data packet; When multiple rules are completely matched at the same time, the first fully matched rule takes effect; This matching rule determines whether the packet is forwarded or discarded. The so-called exact match is that the value of the field in the rule is exactly equal to the value of the corresponding field in the packet. Only when an ACL rule is exactly matched, the rule will

perform the corresponding deny or permit operation.

In the switch, the rules in the same group are sorted automatically. The automatic sorting of rules is relatively complex. In the sorting process, the rules with a large range are in the back and the rules with a small range are in the front. The size of the range is determined by the constraints of the rule; The fewer the constraints of the rule, the larger the scope of rule matching, and the more the constraints of the rule, the smaller the scope of rule matching. The constraints of the rule are mainly reflected in the address's wildcard and the number of some non address fields. Wildcard is a bit string. The IP address is four bytes and the MAC address is six bytes. Bits' 1 'means no matching is required, and bits' 0' means matching is required. Non address fields refer to protocol type, IP protocol type and protocol port. These fields also hide a wildcard. Their length is the byte length of the corresponding field, so the same field length is unified, and only the number of fields needs to be calculated. The more bits wildcard is' 0 ', the more constraints there are.

The following takes port access filtering as an example to illustrate the necessity of rule sorting and the advantages of automatic sorting. If the user needs to reject the address forwarding of the network segment with the source address of 10.10.10.0/16 and allow the address forwarding of the network segment with the source address of 192.168.1.0/24, the following two rules can be configured:

Access list 1 permit 192.168.1.0 0.0.255 - rule 1

Access list 1 deny 10.10.10.0 0.0.255.255 - Rule 2

Hereinafter referred to as rule 1 and rule 2.

These two rules are in conflict; Because the address of rule 1 is included in the address of rule 2, and one is deny and the other is permit; According to the filtering principle of ACL, different sequences have different results. If you want to achieve the above requirements, the order of the above two rules must be: Rule 1 is in the front and rule 2 is in the back. The switch automatically realizes the above sorting function. No matter what order the user configures the above rules, the last order is rule 1 ahead of rule 2. When a packet with a source address of 192.168.1.1 is forwarded, first compare the first rule, and then compare the second rule. Both rules match, and the previous one takes effect (forwarding); If the forwarding address is 10.1, only the first address is discarded.

If sorting is not performed, the user may configure rule 2 first and then rule 1; Rule 1 is in the back and rule 2 is in the front

Access list 1 deny 10.10.10.0 0.0.255.255 - Rule

Access list 1 permit 192.168.1.0 0.0.255 - rule 1

Because the previous rule 2 contains the following rule 1, it may lead to the following situation: the packets that exactly match rule 1 also exactly match rule 2, and rule 2 will take effect every time; And can not meet the needs of the application.

In the switch, '0.0.255.255' is the wild card bits, bits' 1 'means no matching is required, and bits' 0' means matching is required. It can be seen that the wildcard bits of rule 2 is' 0.0.255.255 ', which needs to match two bytes (16 bits); The wildcard bits in rule 1 is' 0.0.255 ', and three bytes (24 bits) need to be matched; So rule '2' comes after rule '2'. In the extended IP, the sorting needs to consider more rule fields, such as IP protocol type, communication port and so on. Their sorting rules are the same, that is, the more configuration restrictions, the smaller the 'scope' of the rule, and vice versa. The sorting of rules is implemented in the background, and user commands can only be displayed in the order configured by the user.

The filter fields supported by ACL include source IP, destination IP, IP protocol type (such as TCP, UDP, OSPF), source port (such as 161) and destination port. Users can configure different rules for access control according to different needs.

In a switch, a set of rules can be applied by multiple applications; For example, a set of rules is referenced by port access filtering and service access filtering at the same time, or by port access filtering of two ports at the same time

1.89 ACLFilter introduction

ACL filtering is carried out at the input port of the switch. The data flow input to this port is matched by rules to realize port filtering. ACL filtering is processed at the line speed of the switch, which will not affect the forwarding efficiency of data flow.

When a port of the switch is not configured with ACL filtering, all data streams entered through the port will not match the rules and can be forwarded through the port. When ACL filtering is configured for a port of the switch, all input data streams passing through the port will be matched with rules. If the action of the matching rule is permit, the data stream is allowed to be forwarded; if deny, the data stream is not allowed to be forwarded and discarded.

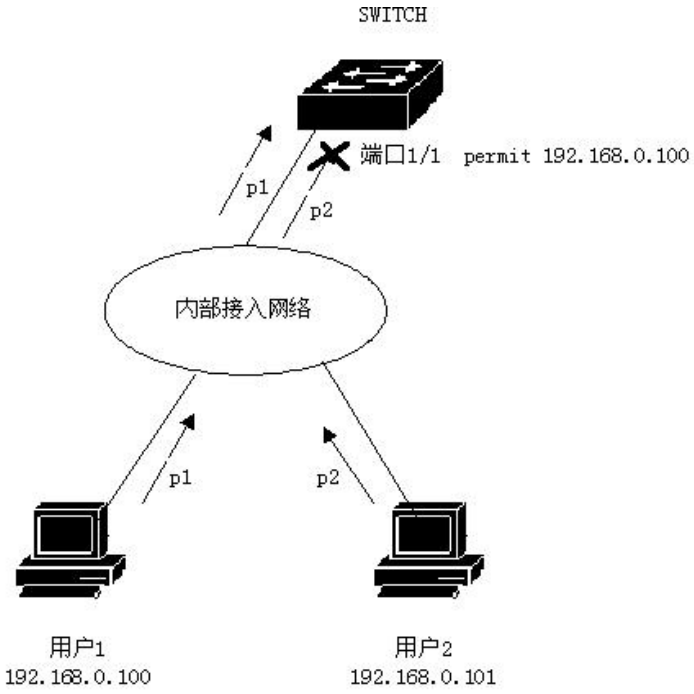
When configuring the ACL filtering of a port, a port can select multiple ACL rule groups. After selection, the group rules are imported into the CFP of the port. If there is no rule to reject or allow all IP protocol packets in the group rules, a rule to reject all IP protocols will be added when writing to the CFP. When the rules of ACL repository change, the rules written into CFP will also change automatically.

For example, there is only one rule in a group of rules: access list 1 permit 192.168.1.0 0.0.255. By default, a rule rejecting all IP protocol packets will be hidden. In fact, two rules will be imported into the CFP of the port. When data flows through the filter, only data streams with source addresses from 192.168.1.0 to 192.168.1.255 can be

forwarded through this port, and all other data streams are filtered out.

For example, there are two rules in a set of rules: access list 1 deny 192.168.1.0 0.0.255 and access list 1 permit any. At this time, there is a rule that allows all IP protocol packets. At this time, there are no hidden rules. In fact, two rules will be imported into the CFP of the port. When the data flows through the filter, only the data stream with the source address from 192.168.1.0 to 192.168.1.255 is filtered, and all other data streams can be forwarded.

The following figure is an example of ACL filtering. Select an ACL rule group 1 for port 1 / 1 of the switch. There is only one rule access list 1 permission 10.10.10.100 in this group. Under port 1 / 1 of the switch, two users want to access the network from this port. The IP address of user 1 is 10.10.10.100 and that of user 2 is 10.10.10.101. Only user 1 can access the network through port 1 / 1 of the switch, while user 2 cannot access the network through port 1 / 1 of the switch. The data stream P1 sent by user 1 can be forwarded through port 1 / 1 of the switch, while the data stream P2 sent by user 2 is discarded at port 1 / 1 of the switch。



When using the same ACL filter rule group, you can use the same ACL filter rule group.

Whether a group of rules or multiple groups of rules are referenced by a port, they will be sorted automatically, even if the sorting between the two groups of rules is crossed.

When a user references a group of rules, if the group of rules changes, the port that references the group of rules will automatically respond to the user's configuration; There

is no need to reconfigure the reference of this port。

1.90 ACL Repository configuration

The switch does not have any rules by default.

The resource library in the switch supports four types of ACL rules: standard IP rules, extended IP rules, IP MAC group and ARP group. Here are four types of rules to introduce ACL configuration

Standard IP rules: standard IP rules control the forwarding of data packets through the source IP address.

Command form: access list < groupid > {deny | permit} < source >

Parameter Description:

Groupid: access control list group number. Standard IP ACL supports groups from 1 to 99 or 1300 to 1999.

Deny / permit: if it matches exactly, reject or allow the packet to be forwarded.

Source: the source IP has three input methods:

1) A.b.c.d wildcard can control the IP address from a network segment;

2) Any is equivalent to a.b.c.d 255.255.255.255

3) Host a.b.c.d is equivalent to a.b.c.d 0.0.0

Wildcard: decide which bits need to be matched, '0' means to be matched, '1' means not to be matched.

Extended IP rule: the extended IP rule is an extension of the standard IP rule. The forwarding of data packets can be controlled through the source IP, destination IP, IP protocol type and service port.

Command form: access list < groupid > {deny | permit} < protocol > < source > [EQ < srcport >] < destination > [destport] < TCP flag >

Parameter Description:

Groupid: access control list group number. Extended IP ACL supports groups from 100 to 199 or 2000 to 2699.

Deny / permit: if it matches exactly, reject or allow the packet to be forwarded.

Protocol: the protocol type above the IP layer, such as TCP, UDP, etc. you can also enter the corresponding number 6 (TCP). If you do not need to control these protocols, you can enter IP or 0.

Source: the source IP has three input methods:

1) A.b.c.d wildcard can control the IP address from a network segment;

2) Any is equivalent to a.b.c.d 255.255.255.255

3) Host a.b.c.d is equivalent to a.b.c.d 0.0.0

Srcport: when the protocol is TCP or UDP, you can control the source port of the data packet. The input method can be some familiar port service names, such as WWW or numbers, such as 80.

Destination: destination IP has three input methods:

1) A.b.c.d wildcard can control the IP address from a network segment;

2) Any is equivalent to a.b.c.d 255.255.255.255

3) Host a.b.c.d is equivalent to a.b.c.d 0.0.0

Destport: when the protocol is TCP or UDP, you can control the destination port of the data packet. The input method is the same as that of srcport.

TCP flag: when the protocol is TCP. TCP field matching of data packets can be controlled. The optional parameters are ACK, fin, PSH, RST, syn and urg.

IP MAC rules: the IP MAC group can control the source destination MAC address and source destination IP address of IP packets.

Command form: access list < groupid > {deny | permit} < SRC MAC > IP < SRC IP > < DST IP >

Parameter Description:

Groupid: access control list group number. Extended IP ACL supports groups from 700 to 799.

Deny / permit: if it matches exactly, reject or allow the packet to be forwarded.

SRC MAC: source MAC address.

There are three input methods for MAC address:

1)HHHH. HHHH. Hhhh wildcard can control the MAC address from one segment;

2) Any is equivalent to HH HHHH. HHHH FFFF. FFFF. FFFF.

3) Host a.b.c.d is equivalent to HH HHHH. HHHH 0000.0000.0000

SRC IP: source IP address.

DST IP: destination IP address.

There are three input methods for IP address:

1) A.b.c.d wildcard can control the IP address from a network segment;

2) Any is equivalent to a.b.c.d 255.255.255.255

3) Host a.b.c.d is equivalent to a.b.c.d 0.0.0

ARP rules: ARP group can control the operation type of ARP packet, sender Mac and sender IP.

Command form: access list < groupid > {deny | permit} ARP {ARP type} < sender MAC > < sender IP >

Parameter Description:

Groupid: access control list group number. The extended IP ACL supports groups from 1100 to 1199.

Deny / permit: if it matches exactly, reject or allow the packet to be forwarded.

ARP type: refers to any | reply | request. Any is the type that does not control ARP packets, reply is the response packet that controls ARP, and request is the request packet that controls ARP packets.

Sender MAC: the MAC address of the sender of the ARP packet.

There are three input methods for MAC address:

1)HHHH. HHHH. Hhhh wildcard can control the MAC address from one segment;

2) Any is equivalent to HH HHHH. HHHH FFFF. FFFF. FFFF

3) Host a.b.c.d is equivalent to HH HHHH. HHHH 0000.0000.0000

Sender IP: the sender IP address of the ARP packet.

There are three input methods for IP address:

1) A.b.c.d wildcard can control the IP address from a network segment;

2) Any is equivalent to a.b.c.d 255.255.255.255

3) Host a.b.c.d is equivalent to a.b.c.d 0.0.0

List of other commands:

show access-list [groupId]

Displays a list of rules configured in the current ACL. If groupid is the current rule list; Otherwise, a list of all rules is displayed.

no access-list <groupId>

Deletes the specified rule list. Groupid all rules of the group.

1.91 Time period based ACL

Time period is used to describe a special time range. Users may have such requirements: some ACL rules need to take effect in a certain or some specific time, but they are not used for message filtering in other time periods, that is, filtering by time period. At this time, the user can first configure one or more time periods, and then reference the time period through the time period name under the corresponding rule. This rule will only take effect within the specified time period, so as to realize ACL filtering based on time period.

If the time period referenced by the rule is not configured, the system will give a prompt and allow such a rule to be created successfully, but the rule cannot take effect immediately until the user configures the referenced time period and the system time is within the specified time period.

The time period can be configured in the following two ways

(1) Configure relative time period: from a certain time to a certain time on a certain day;

(2) Configure absolute time period: in the form of from a certain time and a minute on a certain day of a certain month of a certain year to a certain time and a minute on a certain day of a certain month of a certain year.

Configure time period based ACLS：

Command	Description	CLI mode
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59>	Configure a relative time period that only contains time division for a time period	Global configuration mode
time-range WORD cycle-time days from <0-6> to <0-6>	Configure a relative time period that only contains weeks for a time period	Global configuration mode
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59> days from <0-6> to <0-6>	Configure a relative time period including time division and week for time period	Global configuration mode
time-range WORD utter-time from <2000-2100> <1-12> <1-31> <0-23> <0-59> to <2000-2100> <1-12> <1-31> <0-23> <0-59>	Configure a time period with an absolute time period including time, month, day and hour	Global configuration mode
no time-range WORD cycle-time	Delete all relative time periods of a certain time period	Global configuration mode
no time-range WORD utter-time	Delete all absolute time periods of a certain time period	Global configuration mode
no time-range WORD	Delete a certain time period (including deleting all relative time periods and absolute time periods)	Global configuration mode
no time-range	Delete all time periods	Global configuration mode
show time-range WORD cycle-time	Display all relative time periods of a certain time period	Privileged mode
show time-range WORD utter-time	Display all absolute time periods of a certain time period	Privileged mode
show time-range WORD	Display a certain time period (including all absolute time	Privileged mode

	periods and relative time periods)	
show time-range	Show all time periods	Privileged mode
time-acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range WORD	A certain ACL rule is applied for a certain period of time, which works when ACL is applied to the interface	Global configuration mode
no time-acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range (WORD|)	Cancel the application of certain ACL rule to certain time period or all time periods	Global configuration mode
show time-acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range	Displays all the time periods in which a certain ACL rule is applied	Privileged mode
show time-acl all time-range	Displays the time period in which all ACL rules are applied	Privileged mode

(1) It should be noted that:

(2) (1) Configure multiple relative time periods for a certain time period. The relationship between relative time periods is or. The system time is in any relative time period, and the time period is active;

(3) (2) Configure multiple absolute time periods for a certain time period. The relationship between absolute time periods is or. The system time is in any absolute time period, and the time period is active;

(4) (3) If relative time period and absolute time period are configured for a certain time period at the same time, the relative time period and absolute time period are related to each other. The time period is activated only when the system time is within both relative time period and absolute time period;

(5) (4) Up to 256 time periods can be defined; One time period can be configured with 256 relative time periods and absolute time periods at most; One ACL rule can be applied for up to 256 time periods; The time period comes into effect when the ACL rule associated with the time period is applied to the interface。

1.92 ACLFilter configuration

By default, all ports of the switch are not ACL filtered.

Command list:

access-group <groupId>

Mode: layer 2 interface configuration mode

Parameters:

Groupid: the ACL group number bound to the port

Function: configure ACL port filtering.

Note: if the above command configuration fails or is invalid, there may be the following reasons:

There are too many rules in ACL group, or hardware resources are exhausted or occupied by other applications.

Display ACL port filtering configuration

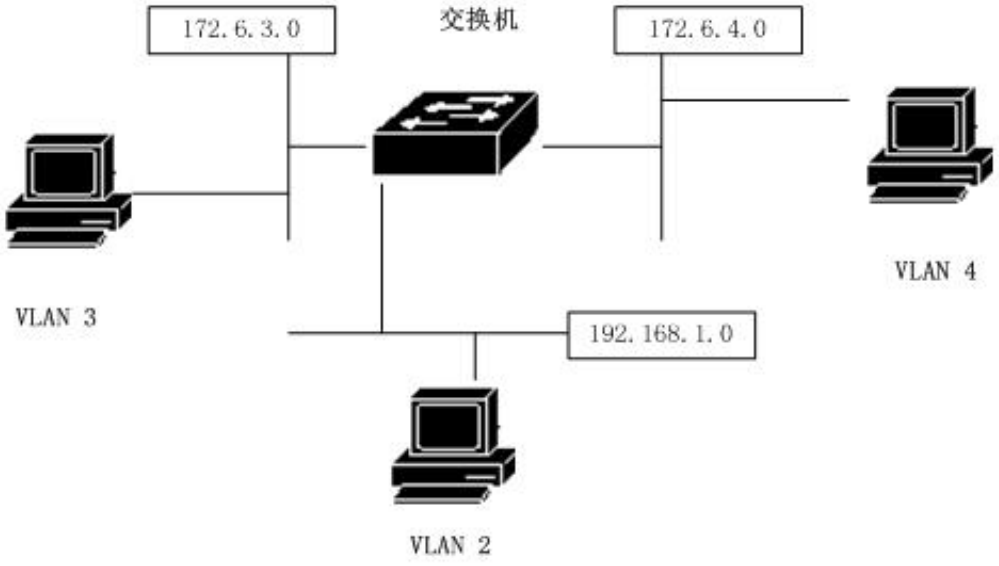
show acccess-group

Delete the configuration related to the current port and ACL port filtering

no acl- group <groupId>

1.93 ACL Configuration example

One switch connects three subnets, designs ACL, and the blocking source address is 192.168.1.0 network address. And allow the traffic of other network addresses to pass through. The 192.168.1.0 network segment is connected to the 1 / 1 port of the switch。



The configuration on the switch is as follows：

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config)#interface ge1/1
Switch(config-ge1/1)# switchport mode access
Switch(config-ge1/1)#switchport access vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip add 192.168.1.1/24
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 3
Switch(config)#interface vlan3
Switch(config-vlan2)#ip add 172.16.3.1/24
Switch(config)#access-list 10 deny 192.168.1.0 0.0.0.255
Switch(config)#access-list 10 permit any
Switch(config)#interface ge1/1
Switch(config-ge1/1)#access-group 10
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#access-group 10
```

1.94 ACLConfiguration troubleshooting

If ACL configuration fails, there may be the following reasons:

1. Before configuring the access control list, make sure that all IPS are connected, and then add the access control list. This access control list blocks the IP data flow of the network segment with the source address of 192.168.1.0 through the switch. Pay attention to the writing of subnet inverse code. Use the show access list command to list the access control list for viewing. Be sure not to write the source address and destination address upside down. Then view the access control list. Moreover, there is an implicit deny any statement at the end of the default access control list. If you want others to pass, you need to add a allow any statement, otherwise they can't pass.

2. The system is configured with static IP MAC binding.

3. DHCP snooping protocol is enabled for the current interface.

4. System CFP resource exhausted。

TCP/IPBasic configuration

For a layer-2 switch with network management function, it is necessary to provide basic network configuration for TCP / IP protocol to realize the communication function with other devices。

This chapter mainly includes the following contents：

- Configure VLAN interface
- Configure ARP
- Configure static routing
- IP routing configuration example

1.95 Configure VLAN interface

In the switch, each layer-3 interface is attached to a VLAN, so the layer-3 interface is also called VLAN interface. The creation and deletion of VLAN interface are completed manually. The switch can be divided into 4094 VLANs at most, but only 32 subnets can be established at most. The creation of subnet interface can be created according to the needs of users; The subnet interface can be manually deleted by the user, or it can be deleted with the VLAN of the subnet being deleted.

Each VLAN interface has a name. The name of the VLAN interface is the string

"VLAN" followed by the VLAN ID number. For example, the name of the layer 3 interface of VLAN 1 is "vlan1", and the name of the layer 3 interface of VLAN 4094 is "vlan4094".

Like ports, VLAN interfaces have management status and link status. At present, the switch does not provide the configuration of VLAN interface management status. As long as the VLAN interface is created, the VLAN interface management status is always up. The link state of the VLAN interface is related to the ports contained in the VLAN corresponding to the interface. As long as the link state of a port in the VLAN is running, the link state of the VLAN interface is running. If all ports in the VLAN are not running, the link state of the VLAN interface is not running.

On the VLAN interface, you can configure the IP address and indicate the network prefix of the network segment connected to this interface (which can be converted into a network mask). At present, the switch only supports one IP address configured on one VLAN interface. Before configuring IP addresses, users need to create VLANs and add related ports to VLANs. By default, the switch has vlan1 interface, and the IP address 10.10.10.1/24 is set on this interface. Users can also modify the IP address of vlan1 interface. The interfaces of VLANs other than vlan1 do not have IP addresses set by default.

The commands for configuring the IP address of VLAN interface are shown in the following table：

Command	Description	CLI mode
Ip interface vlan <2-4094>	Create a VLAN interface	Global configuration mode
No Ip interface vlan <2-4094>	Delete a VLAN interface	Global configuration mode
ip address <ip-prefix>	Set the IP address on the VLAN interface. The parameters include the IP address of the interface and the network prefix of the connected network segment. If the VLAN interface has an original IP address, delete the original IP address first, and then set the specified IP address. The format of the parameter is a.b.c.d/m。	Interface configuration mode
no ip address [ip-prefix]	Delete the IP address of the	Interface configuration

	VLAN interface. If a parameter is specified, it must be the same as the parameter given during setting, otherwise this command is invalid. The format of the parameter is a.b.c.d/m.	mode

The commands for viewing VLAN interfaces are shown in the following table：

Command	Description	CLI mode
show interface [if-name]	View the information of VLAN interface, including IP address, MAC address, management status, link status, etc. Parameter is the interface name of VLAN interface. If no parameter is specified, view the information of all ports and VLAN interfaces.	Normal mode, privileged mode
show running-config	View the current configuration of the system, and you can view the configuration of VLAN interface.	privileged mode

For example：

Configure subnet 193.1.1.0 on vlan3 interface, the subnet prefix is 24 (i.e. mask 255.255.255.0), the IP address of the interface is 193.1.1.1, and view the information of vlan3 interface. The command is as follows：

switch(config)#interface vlan3

switch(config-vlan3)#ip address 193.1.1.1/24

switch(config-vlan3)#end

switch#show interface vlan3

1.96 Configure ARP

ARP (address resolution protocol) protocol is a protocol that provides mapping from IP address to corresponding MAC address. When the source sends the Ethernet data frame to the destination in the same VLAN, the destination is determined according to the 48 bit Ethernet MAC address, and the destination determines whether to receive the data packet according to the destination MAC address of the data packet.

It is assumed that hosts a and B of two adjacent network segments communicate through the switch. Before sending data to host B, host a first sends ARP request message to the interface of the switch directly connected to host a, and sends data packet to the interface after receiving ARP response. After receiving this data packet, the switch first broadcasts an ARP request message to host B, obtains the ARP response message from host B, and then sends the data packet to host B.

There is an ARP cache on the switch, called ARP table, which stores the mapping record from IP address to MAC address in the directly connected network. Each item in the ARP table has a lifetime, which is 20 minutes by default. When the switch does not receive the ARP request or response message of the IP address during the lifetime, the ARP table item corresponding to the IP address will be deleted.

This section includes the following：

- Configure static ARP
- Configure ARP binding
- View ARP information

1.96.1 Configure static ARP

There are two different ARP table entries in the ARP table, one is static ARP and the other is dynamic ARP. Static ARP is the ARP table item configured by the user through the command. The system will not refresh and delete automatically, which needs to be completed manually by the user. Dynamic ARP is an ARP automatically learned by the system according to the received ARP request or response package. The system automatically creates and deletes, updates and maintains it in real time, without user intervention, but users can manually delete dynamic ARP table entries

The switch is not configured with static ARP table entries by default. It should be noted that when a VLAN interface is deleted or the subnet segment IP of the interface is changed, the static and dynamic ARP table entries in the original subnet segment will be deleted.

The commands for configuring static ARP are shown in the following table

Command	Description	CLI mode
arp <ip-address> <mac-address>	Configure static ARP table entries. The first parameter is the IP address, which must be within a subnet segment. The second parameter is the MAC address. The MAC address must be a unicast MAC address. The format of the MAC address is hhhh HHHH. Hhhh, such as 0010.5cb1 7825。	Global configuration mode
no arp <ip-address>	Delete the ARP table entry. Including deleting the ARP table entry of an IP	Global configuration mode

1.96.2 View ARP information

The commands for viewing ARP information are shown in the following table：

Command	Description	CLI mode
show arp	Look at the ARP table item information in the ARP table, including all ARP table items	Normal mode, privileged mode
show running-config	View the current configuration of the system, and you can view the configuration of ARP.	privileged mode

1.97 Configure static routing

Static routing is a user-defined route that enables packets to reach the destination

address through a specified path from the source address. You can configure a static route as the default route to send packets that cannot be routed to the default gateway.

Static routing is manually configured by the administrator. It is suitable for networks with simple networking structure. The administrator only needs to configure static routing to make the switch work normally. Static routing will not occupy valuable network bandwidth because there will be no route update.

The default route is also a static route. Simply put, the default route is the route used when no matching route item is found. That is, the default route is used only when there is no suitable route. In the routing table, the default route appears as a route to the network 0.0.0.0/0 (mask 0.0.0.0). If the destination of the message is not in the routing table and there is no default route in the routing table, an ICMP message indicating the destination address or network unreachable information at the source will be returned when the message is discarded. Default routing is very useful in networks. In a typical network with hundreds of switches, running dynamic routing protocol may consume a lot of bandwidth resources. Using default routing can save the time occupied by routing and the bandwidth resources occupied by packet forwarding, so as to meet the needs of a large number of users to communicate at the same time to a certain extent.

The switch can configure multiple static routes to the same destination, but only one of them is activated for actual data forwarding. The switch is not configured with static routing by default.

The commands for configuring static routing are shown in the following table：

Command	Description	CLI mode
ip route <ip-prefix> <nexthop-address>	Set the static route. The first parameter specifies the network segment IP and network prefix length, and the second parameter specifies the next hop IP address.	Global configuration mode
ip route <ip-address> <mask-address> <nexthop-address>	The function is the same as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the IP address of the next hop.	Global configuration mode

no ip route <ip-prefix> [nexthop-address]	Delete static route. The first parameter specifies the network segment IP and network prefix length, and the second parameter specifies the next hop IP address. If there are no parameters matching the specified network segment, delete the second one. If there is the second parameter, the route matching the specified network segment and the next hop will be deleted.	Global configuration mode
no ip route <ip-address> <mask-address> [nexthop-address]	The function is the same as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the IP address of the next hop. If there is no third parameter, all routes matching the specified network segment are deleted. If there is a third parameter, the route matching the specified network segment and the next hop will be deleted.	Global configuration mode

查看路由的命令如下表：

Command	Description	CLI mode
show ip route [<ip-address> | <ip-prefix>	To view the information of active routes, you can choose to view all routes, a route, a route of a network segment, and static routes。	Normal mode, privileged mode
show ip route database	View the information of all	Normal mode, privileged mode

	routes (including active and inactive routes), and you can choose to view all routes。	
show running-config	View the current configuration of the system, and you can view the configuration of static routes.	privileged mode

Example：

Set the destination network to 200.1.1.0, the subnet mask to 255.255.255.0, and the next hop to 10.1.1.2. The configuration command is:

Switch(config)#ip route 200.1.1.0 255.255.255.0 10.1.1.2

or Switch(config)#ip route 200.1.1.0/24 10.1.1.2

Delete the static route with destination IP address of 200.1.1.0, subnet mask of 255.255.255.0 and next hop of 10.1.1.2. The configuration command is：

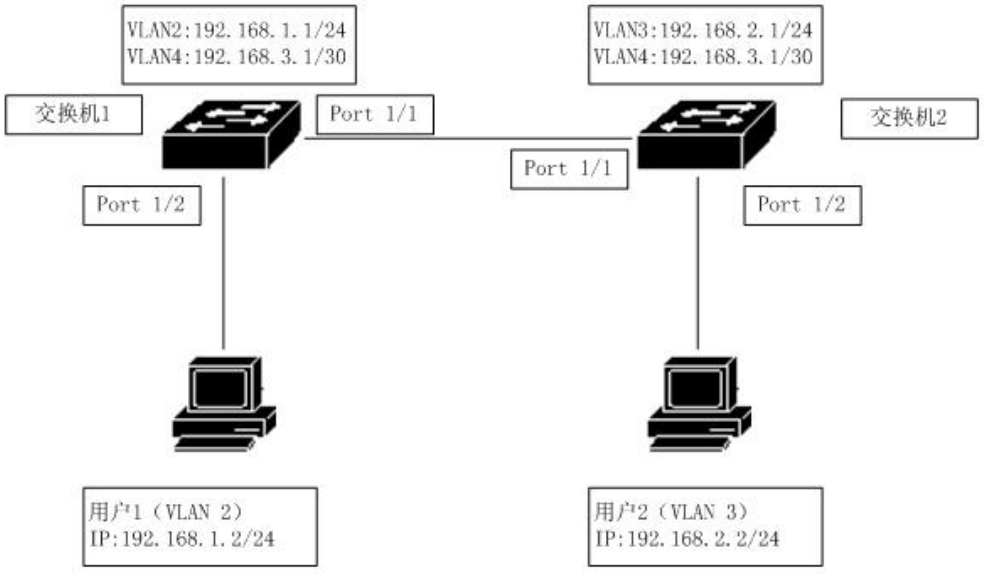
Switch(config)#no ip route 200.1.1.0/24

Or Switch(config)#no ip route 2001.1.0/24 10.1.1.2

Or Switch(config)#no ip route 200.1.1.0 255.255.255.0

Or Switch(config)#no ip route 200.1.1.0 255.255.255.0 10.1.1.2

1.98 TCP/IP Basic configuration example



In the figure, switch 1 is a layer 2 switch and switch 2 is a layer 3 switch。

1.98.1 L3 layer interface

Configure the three-layer interface corresponding to vlan2 on switch 1, and assign an IP address 192.168.1.1/24 at the same time.

The configuration is as follows：

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switch access vlan 2

Switch(config)#ip interface vlan 2

Switch(config)#interface vlan2

Switch(config-vlan2)#ip add 192.168.1.1/24

Verification: user 1 can ping the layer 3 interface IP address corresponding to vlan2 of switch 1。

1.98.2 Static routing

To access switch 1, user 2 must pass the routing function of switch 2 to access switch 1.

The configuration on switch 1 is as follows:

Switch#config t

Switch(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2

The configuration on switch 2 is as follows:

Switch#config t

Switch(config)#ip route 192.168.1.0/24 192.168.3.1

Verification: User 2 can ping general switch 1。

1.98.3 ARP

Configure the static ARP of user 1 and only allow user 1 to access from vlan2. Assume that the MAC address of user 1 is 00:00:00:00:01.

Switch 1 is configured as follows:

Switch#config t

Switch(config)#arp 192.168.1.2 0000.0000.0001

Verification: user 1 can ping the layer 3 interface IP address corresponding to vlan2 of switch 1。

Configure SNMP

The switch provides SNMP for remote management of the switch. This chapter describes how to configure SNMP, mainly including the following contents：

This chapter mainly includes the following contents：

- SNMP Introduction
- SNMP configuration
- SNMP configuration example

1.99 SNMP introduction

SNMP is a simple network management protocol. It is the most widely used network management protocol at present. It has five functions: fault management, billing management, configuration management, performance management and security management. It provides the information format of communication between network management application software and network management agent.

SNMP network management protocol has four elements: management workstation,

management agent, management information base and network management protocol. On the switch, the management agent is the server of the management workstation accessing the switch. The information of the management workstation accessing the network management agent is organized in the form of MIB to form a management information base.

SNMP has three operations: get, set and trap. The get operation enables the management station to obtain the value of the object in the agent. The set operation enables the management workstation to set the value of the object in the agent. The trap operation enables the agent to announce events to the management workstation.

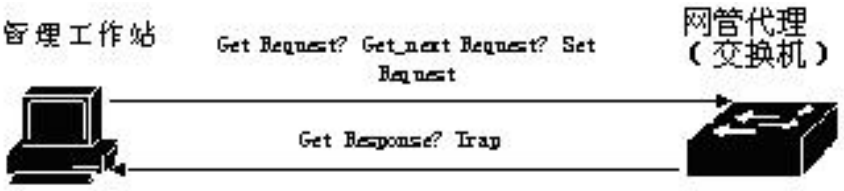
Trap messages are actively sent to the management workstation when events occur in the switch. These messages include cold start, hot start, link up and link down of ports, failure of common name authentication, state switching of STP, etc.

At present, SNMP has three versions: SNMPv1, SNMPv2 and SNMPv3. The later version is the upgraded version of the previous version, with enhanced functions and improved security. The switch supports all three SNMP versions and can analyze the three versions of SNMP protocol packets. When sending a trap message, you can use any version of SNMPv1, SNMPv2 and SNMPv3.

The switch supports RFC, bridge and private MIB objects. The switch can be fully managed through SNMP. Some MIBs supported by the switch are listed below: RFC 1213, RFC 1493, RFC 1724, RFC 1850, RFC 1907, RFC 2233, RFC 2571, RFC 2572, RFC 2573, RFC 2574, RFC 2575,

RFC 2674 and other common MIBs

The figure is an example of SNMP protocol interaction between management workstation and management agent. The management workstation can access the switch management agent by sending SNMP messages of get request, GetNext request, getbulk request and set request, obtain or set the value of the MIB object of the switch, and the switch management agent sends back the SNMP message of get response to the management workstation. When some events occur on the switch, the management agent of the switch actively sends SNMP trap messages to the management workstation。



SNMP protocol interaction between management workstation and management agent

1.100 SNMP configuration

SNMP configuration includes community configuration of switch, trap workstation and SNMP system information configuration. The switch has a read-only common body by default. The common body name is public. The switch can configure up to 8 common bodies. The switch is not configured with trap workstation by default

SNMP commands are shown in the following table：

Command	Description	CLI mode
snmp community <community-name> {ro | rw}	Configure the common name of the access network management. This is an interactive command. During configuration, the user can enter the required community name and read / write permission according to the prompt.	Global configuration mode
no snmp community <community-name>	Deletes the specified SNMP community name.	Global configuration mode
snmp trap <notify-name> host <ipaddress> version {1 | 2c | 3}	Add or modify the sending destination of SNMP trap. This is an interactive command. Notify name is unique. If you modify an existing name, you can modify the trap sending target item. Host is the destination address of sending trap; Whether version is sent in the form of SNMPv1, snmpv2c or SNMPv3. The default configuration target port of this command is 162.	Global configuration mode
no snmp trap <notify-name>	Delete the specified SNMP	Global configuration mode

	trap.	
snmp system information <contact | location | name> <information-string>	Configure system information. Configurable system information includes contact, location and name.	Global configuration mode
no snmp system information <contact | location | name >	Delete a system configuration information.	Global configuration mode
show snmp community	Displays all the current public body names and the corresponding read-write permission information.	Normal mode / privileged mode
show snmp trap	Displays all the current trap names and the target IP address and version information sent by the corresponding trap.	Normal mode / privileged mode
show snmp system information	Displays system information for SNMP settings 。	Normal mode / privileged mode

1.101 SNMP Configuration example

1.101.1 Configuration

Configure a common name named private. The operation permission is read and write.

Configure an SNMP trap named test and the sending destination IP is 10.10.10.10; The SNMP version used is 1.

The specific contents of configuring the system's contact are: E-mail: networks@acb.com 。

The specific content of configuring the location of the system is: Shenzhen.

Configure the system name. The specific content is: switch.

The configuration of the switch is as follows：

Switch#config t

Switch(config)#snmp community private rw

Switch(config)#snmp system information contact E-mail:networks@abc.com

Switch(config)#snmp system information location Shenzhen
Switch(config)#snmp system information name switch

RMON Configuration

This chapter mainly includes the following contents：

- RMON introduction
- RMON configuration
- RMON configuration example

1.102 RMON introduction

RMON (remote monitoring) is a standard monitoring specification, which is mainly used to monitor the data flow in a network segment and even the whole network. It is one of the widely used network management standards at present. RMON specification is extended from SNMP MIB, so it is also a kind of MIB and the most important enhancement to MIB II standard. RMON enables SNMP to monitor remote devices more effectively and proactively.

RMON monitoring system consists of two parts: detector (agent or monitor) and management station. The RMON agent stores network information in the RMON MIB, which is directly implanted into network devices (such as routers, switches, etc.). The management station uses SNMP to obtain RMON data information.

This device supports the four most commonly used groups in RMON:

(1) Statistics: provides statistical data of each interface. Most of the objects are counters, which record the information collected by the monitor from the interface.

(2) History: save the data sampled on the specified interface at fixed time intervals.

(3) Alarm group: sample the specified data of all interfaces at a fixed time interval and compare it with the set threshold. When the conditions are met, the corresponding events will be triggered.

(4) Event group: set events. You can choose to log or issue trap.

1.103 RMON Configuration

The RMON command includes the configuration of four groups, viewing configuration and viewing data：

Command	Description	CLI mode
rmon statistics <1-100> (owner WORD|)	Enable the statistical group configuration of the specified serial number for this port. This is an interactive command. Configuration is that the user can enter the serial number and owner according to the prompt, in which the owner is optional (the same below). Serial number is the number of statistical group configuration,取值范围是1到100。	Port configuration mode
no rmon statistics <1-100>	Cancel the statistics group configuration of the specified sequence number.	Port configuration mode
rmon history <1-100> buckets <1-100> interval <1-3600> (owner WORD|)	Configure the history group parameter of the specified serial number for the port. This is an interactive command. The configuration user can enter the serial number, number of request buckets, time interval and owner according to the prompt. Serial	Port configuration mode

	number is the number of history group configuration, and the value range is 1 to 100; The number of request buckets is the maximum number of saved data, and the value range is 1 to 100; The sampling time interval is in seconds, and the value range is 1 to 3600.	
no rmon history <1-100>	Cancel the history group configuration of the specified sequence number。	Port configuration mode
rmon alarm <1-60> WORD <1-3600> (absolute|delta) rising-threshold <1-2147483647> <1-60> falling-threshold <1-2147483647> <1-60> (owner WORD|)	Configure the alarm group parameters of the specified serial number. This is an interactive command. The configuration user can enter the serial number, monitoring object, time interval, comparison method, upper limit threshold, upper limit event serial number, lower limit threshold, lower limit time piece serial number and owner according to the prompt. Serial number is the number of alarm group configuration, and the value range is 1 to 60; The monitoring object is the oid of a MIB node. The sampling time interval is in seconds, and the value range is 1 to 3600; The comparison method can be absolute or delta, which respectively represents the absolute value (the value of each sampling) and the relative value (the increment of each sampling	Global configuration mode

	relative to the last sampling); The upper and lower thresholds range from 1 to 2147483647; Events must be configured in advance, and the number range is 1 to 60.	
no rmon alarm <1-60>	Cancel the alarm group configuration of the specified serial number.	Global configuration mode
rmon event <1-60> (log|log-trap WORD|none|trap WORD) (description WORD|) (owner WORD|)	Configure the event group parameters of the specified sequence number. This is an interactive command. The configuration user can enter serial number, event type, common body name, description and owner according to the prompt. Serial number is the number of event group configuration, and the value range is 1 to 60; The event type can be log, log trap, none and trap. When log trap or trap is selected, the common body name must also be specified (the common body name configuration in this device is ignored)。	Global configuration mode
no rmon event <1-60>	Cancel the event group configuration of the specified sequence number。	Global configuration mode
show rmon (statistics|history-control|alarm|event) config	View RMON configuration information, which is an interactive command. Configure that the user can enter the viewing object according to the prompt.	Global configuration mode
show rmon statistics-data interface IFNAME|	To view RMON statistical group data, the configuration user must enter the interface name.	Global configuration mode

show rmon history-data interface IFNAME|	To view the RMON historical group data, the configuration user must enter the interface name.	Global configuration mode

1.104 RMONConfiguration example

Enable statistical group configuration for port GE1 / 1, with serial number of 10 and owner of tereco.

Enable the historical group data collection of port GE1 / 8. The serial number is 2. The maximum number of data is 80. The sampling interval is 1 minute. There is no owner.

Configure the event with sequence number 1, record the log, and there is no owner.

Configure the event with sequence number 3, send trap, the common body name is public, and there is no owner.

Enable the alarm group with serial number 5 to monitor the number of bytes received by each port. When the number of bytes per half minute is greater than 1000, a trap alarm is issued, and when it is less than 10, a log is recorded. No owner.

The switch configuration is as follows：

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#rmon statistics 10 owner tereco

Switch(config-ge1/1)#exit

Switch(config)#interface ge1/8

Switch(config-ge1/8)#rmon history 2 buckets 80 interval 60

Switch(config-ge1/8)#exit

Switch(config)#rmon event 1 log

Switch(config)#rmon event 3 trap public

Switch(config)#rmon alarm 5 1.3.6.1.2.1.2.2.1.10 30 delta rising-threshold 1000 3 falling-threshold 10 1

Cluster configuration

The switch provides cluster management function, which can realize a group of network devices managed by a single device. This chapter mainly describes how to configure a cluster：

- Introduction to cluster management
- Configuration management device
- Configure member devices
- Cluster management display and maintenance
- Typical configuration examples of cluster management

1.105 Introduction to cluster management

1.105.1 Cluster definition

A cluster is a collection of network devices that can be managed as a single device.

The purpose of cluster management is to solve the problem of centralized management of a large number of decentralized network devices.

Advantages of cluster: save public IP address; Simplify configuration management tasks. Network managers only need to configure the public IP address on one switch in the cluster to manage and maintain other switches in the cluster.

The switch that configures the public network IP address and performs the management function is the command switch. Other managed switches are member switches. The command switch and member switches form a "cluster".

The cluster configures and manages the switches inside the cluster through the following three protocols。

- NDP（Neighbor Discovery Protocol）
- NTDP（Neighbor Topology Discovery Protocol）
- Cluster （Cluster Management Protocol）

The working process of the cluster includes topology collection and cluster establishment and maintenance. The topology collection process and cluster maintenance process are relatively independent. The topology collection process starts before the cluster is established. The working principle is as follows：

- All devices obtain the information of neighbor devices through NDP, including the software version, host name, MAC address, port name and other information of neighbor devices。
- The management device collects the device information within the hop number range specified by the user and the connection information of each device through ntdp, and determines the candidate devices of the cluster from the collected topology information。
- The management device completes the operations of adding candidate devices to the cluster and leaving the cluster according to the candidate device information collected by ntdp.
- All messages of the cluster are layer-2 Ethernet messages. For the specific format and interaction process, see the national standard YDT 1692-2007 technical requirements for Ethernet switch cluster management》

1.105.2 Cluster role

Different roles are formed according to the status and functions of each device in the cluster. Users can specify roles through configuration. All roles are as follows:

1) Command switch:

In the cluster, the only switch that can configure and manage the whole cluster is also the only switch with public IP address in the cluster。

- Command switches to create clusters；
- Command switches discover and determine candidate switches by collecting NDP (neighbor discovery protocol) and ntdp (neighbor Topology Discovery Protocol) information；
- Command the switch to control the maintenance of the cluster. You can add candidate switches to the cluster or delete member switches from the cluster；
- After the cluster is established, the command switch provides a management channel for the cluster。

1) Member switch

Managed switches in the cluster.

Member switches are candidate switches before joining the cluster.

The member switch does not have public IP;

The management of the member switch is completed through the command switch agent.

2) Candidate switch

A switch that has the ability to join a cluster but has not joined any cluster. The switch must be a candidate switch before it can become a member switch

3) Independent switch

Switches without cluster function.

Various roles can be converted according to certain rules:

- While creating a cluster on the candidate device, the user designates the current candidate device as the cluster management device. Each cluster must specify one (and only one) management device. After the management device is designated, the management device finds and determines the candidate device by collecting relevant information. Users can add candidate devices to the cluster through corresponding configuration。
- After joining the cluster, candidate devices become member devices。
- After the member devices in the cluster are deleted, they will be restored to candidate devices。
- The management device can be restored as a candidate device only when the cluster is deleted。

1.105.3 NDP introduction

NDP is used to obtain the information of directly connected neighbor devices, including connection port, device name, software version and other information. The working principle is as follows：

- The equipment running NDP periodically sends NDP messages to neighbors, which contain NDP information (including the device name, software version, connection port and other information of the current equipment) and the aging time of NDP information on the receiving equipment. At the same time, it will also receive but not forward NDP messages sent by neighbor devices。
- Devices running NDP will store and maintain the NDP neighbor information table, and create a table entry for each neighbor device in the NDP neighbor information table. If a new neighbor is found, that is, the NDP message sent by it is received for the first time, a table entry will be added to the NDP neighbor information table; If the NDP information received from the neighbor device is different from the old information, the corresponding data item in the NDP table will be updated. If it is the same, only the aging time will be updated. If the NDP information sent by the neighbor is not received after the aging time, the

corresponding neighbor table item will be deleted automatically。

1.105.4 NTDP introduction

Ntdp is used to collect the information of each device and the connection information between devices within a certain network range. Ntdp provides management devices with device information that can join the cluster and collects topology information of devices within the specified hops.

NDP provides ntdp with adjacency table information. Ntdp sends and forwards ntdp topology collection request according to adjacency information to collect NDP information of each device within a certain network range and its connection information with all neighbors. After collecting this information, the management equipment or network management can use this information as needed to complete the required functions. When the NDP on the member device finds that the neighbor has changed, it notifies the management device of the neighbor change message through the handshake message. The management device can start ntdp to collect the specified topology, so that ntdp can reflect the change of network topology in time.

The management device can conduct topology collection in the network regularly, and the user can also start topology collection once through manual configuration command. The process of collecting topology information from the management device is as follows：

- The management device sends ntdp topology collection request message from the port enabling ntdp function regularly。
- The device receiving the request message immediately sends the topology response message to the management device, copies the request message at the port with ntdp function enabled and sends it to the adjacent device; The topology response message contains the basic information of the device and the NDP information of all adjacent devices。
- After receiving the request message, the adjacent device will perform the same operation until the topology collection request message spreads to all devices within the specified hop number range。

When the topology collection request message spreads in the network, a large number of network devices receive the topology collection request and send the topology response message at the same time. In order to avoid network congestion and busy task of management equipment, the following measures can be taken to control the diffusion

speed of topology collection request message：

- After receiving the topology collection request, the device does not immediately forward the topology collection request message, but delays waiting for a certain time before starting to forward the topology collection request message at the port enabling ntdp function。
- On the same device, except for the first port, each port enabling ntdp function will delay for a certain time after the previous port sends the topology collection request message before forwarding the topology collection request message 发。

1.105.5 Cluster management and maintenance

1) Candidate devices join the cluster

Before establishing a cluster, the user should first specify the management equipment. The management equipment finds and determines the candidate equipment through NDP and ntdp protocols, and automatically adds the candidate equipment to the cluster. You can also add the candidate equipment to the cluster through manual configuration.

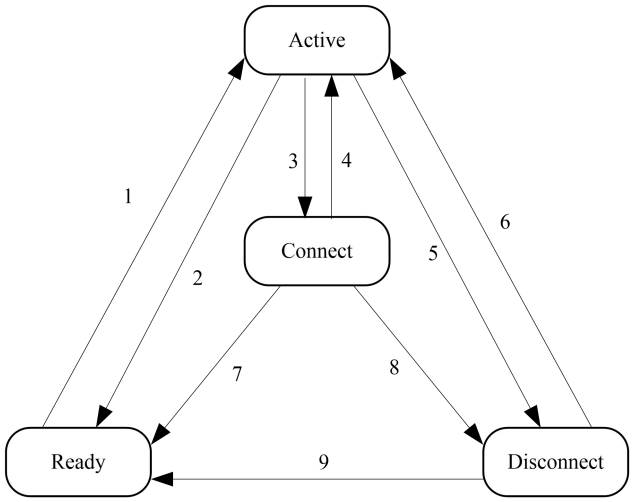
After the candidate device successfully joins the cluster, it will obtain the cluster member serial number and cluster management information assigned by the management device

Private IP address used, etc.

2) Cluster internal communication

Within the cluster, the management device and the member device communicate in real time through handshake message to maintain the communication between them

Connection status: the connection status of management devices and member devices is shown in the figure below。



1 member joining

6 interruption recovery, re registration passed

2 member deletion

7 member deletion

3 the handshake signal is not received for three consecutive times.

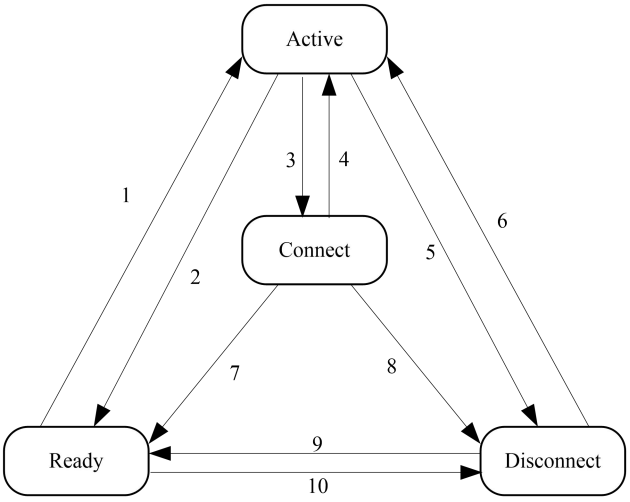
8 the state remains for more than the specified time

4 receive handshake signal

9 delete member

5 recovery request received

Command switch state transition diagram



1 join the cluster

6 interrupt recovery and re register

2 exit the cluster

7 exit the cluster

3 the handshake signal is not received for three consecutive times.

8 the state remains for more than the specified time or the join request message is received

4 receive handshake signal

9 exit the cluster

5. After receiving the join request,

10. Configuration recovery

Member switch state migration diagram

Command the switch to collect the basic information of the device, identify a device as a candidate switch, and the initial state is ready.

Deleting a member in any state will migrate the state of the member switch back to the ready state and identify it as a candidate switch。

- The cluster is established successfully. After the candidate equipment joins the cluster and becomes a member equipment, the management equipment saves the status information of the member equipment locally and identifies the member status as active. The member equipment also saves its own status information locally and identifies its own status as active。
- The management device and the member device regularly send handshake messages to each other. After receiving the handshake message from the member equipment, the management equipment does not respond and keeps the member equipment in active state; The member equipment does not respond and keeps its status active。
- If the management device does not receive the handshake message sent by the member device within three times the handshake message sending time interval after sending the handshake message to the member device, the state of the local member device will be migrated from active to connect; Similarly, if the member device does not receive the handshake message sent by the management device within three times the handshake message sending time interval after sending the handshake message to the management device, its own state will also migrate from active to connect。
- If the management device receives the handshake message or management message sent by the member device in the connect state within the effective retention time, it will migrate the state of the member device back to active, otherwise it will be migrated to disconnect, and the management device will consider the member disconnected at this time; If the member device in the connect state receives the handshake message or management message sent by the management device within the effective retention time, it will migrate its state to active, otherwise it will migrate to disconnect。

When the interrupted communication between the management device and the member device is restored, the member device in the disconnected state will rejoin the cluster. After joining successfully, the member device in the management device and the local state will return to active.

If a topology change is found, the member device also transmits the change information to the management device through the handshake message。

1.105.6 Manage vlan

Management VLAN limits the scope of cluster management. The following functions can be realized by configuring management VLAN：

- The management messages (including NDP, ntdp and handshake messages) of the cluster will be limited to the management VLAN and isolated from other messages to increase security。
- Management devices and member devices realize internal communication through management VLAN.

  When the candidate devices are connected to each other through a cascade management port, it is required that the candidate devices are connected to each other through a management port. Therefore, when the candidate devices are connected to each other through a cascade management port, the candidate devices are allowed to be connected to each other through a VLAN：
- If the port does not allow the management VLAN to pass through, the equipment connected to the port cannot join the cluster. Therefore, before clustering, determine the ports connected to the candidate equipment and the management equipment, including cascade ports, to allow the management VLAN to pass through。
- Only when the default VLAN ID of the port connected between the management device and the member / candidate device and the cascade port are the management VLAN, the message of the configuration management VLAN is allowed to pass without a tag, otherwise the message of the management VLAN must pass with a tag.

  For VLAN related knowledge, see "configuring VLAN"。

1.106 Introduction to cluster configuration

Before configuring the cluster, users need to clarify the roles and functions of various devices in the cluster. In addition, they need to configure relevant functions and make a good plan for communication with the devices in the cluster。

Configure task	
Configuration management device	Enable NDP function of system and port
	Configure NDP parameters
	Enable ntdp function of system and

	port
	Configure ntdp parameters
	Configure manual collection of ntdp information
	Enable cluster function
	Establish cluster
	Configure member interaction within the cluster
	Configure cluster member management
Configure member devices	Enable NDP function of system and port
	Enable ntdp function of system and port
	Configure manual collection of ntdp information
	Enable cluster function
Configure cluster member mutual access	

Note：

After the cluster is established, the cluster will not be dissolved after the NDP or ntdp function is turned off on the management equipment and member equipment, but the normal operation of the established cluster will be affected。

1.107 Configuration management device

1.107.1 Enable NDP function of system and po

Command	Description	CLI mode
ndp global enable	Enable the global NDP function. Global off by default.	Configuration mode
ndp enable	Enable the NDP function of the port. NDP is turned off by default for all ports	Interface configuration mode

Note：

- *The NDP function of global and port must be enabled at the same time for NDP to operate normally。*
- *The NDP feature does not support aggregation ports。*

- *In order to prevent the management device from collecting the topology information of the device that does not need to join the cluster and adding it to the cluster, it is recommended to turn off the NDP function on the port connected to the device that does not need to join the cluster。*

1.107.2 Configure NDP parameters

Command	Description	CLI mode
ndp aging-timer <aging-time>	Configure the aging time of NDP message sent by the device on the receiving device. The default is 180 seconds.	Configuration mode
ndp hello-timer <hello-time>	Configure the time interval for sending NDP messages. The default is 60 seconds.	Configuration mode

Note

Generally, the aging time of NDP message on the receiving equipment shall not be less than the sending time interval of NDP, otherwise it will cause the instability of NDP port neighbor information table。

1.107.3 Enable ntdp function of system and interfa

Command	Description	CLI mode
ntdp global enable	使能全局NTDP功能。缺省情况下全局关闭。	Configuration mode
ntdp enable	使能端口的NTDP功能。缺省所有端口关闭NDP	Interface configuration mode

NOTE：

- *Ntdp functions of global and port must be enabled at the same time for ntdp to operate normally。*
- *The ntdp feature does not support aggregate ports。*
- *In order to prevent the management device from collecting the topology information of the device that does not need to join the cluster and adding it to the cluster, it is recommended to turn off the ntdp function on the port connected to the device that does not need to join the cluster。*

1.107.4 Configure ntdp parameter

Command	Description	CLI mode
ntdp hop <hop-value>	Configure the scope of topology collection. By default, in the collected topology, the maximum number of hops between the farthest device and the topology collection device is 3.	Configuration mode
ntdp timer <interval-time>	Configure the time interval for timed topology collection. The default is 1 minute.	Configuration mode
ntdp timer hop-delay <time>	Configure the waiting time of the collected device before forwarding the topology collection request message at the first port. The default is 200 milliseconds.	Configuration mode
ntdp timer port-delay <time>	Configure the port delay time for the current device to forward topology collection requests. The default is 20 milliseconds.	Configuration mode

1.107.5 Configure manual collection of ntdp informatio

After the cluster is established, the management equipment will collect topology information periodically. In addition, users can manually collect ntdp information through configuration at any time (no matter whether the cluster is established or not), and initiate a collection process of ntdp information, so as to more effectively manage and monitor the equipment in real time。

Command	Description	CLI mode
ntdp explore	Collect topology information manually once.	Normal mode, privileged mode

1.107.6 Enable cluster function

Command	Description	CLI mode
cluster enable	Enables the cluster function. The default cluster function is off.	Configuration mode

1.107.7 Establish cluster

管理 VLAN 限制了集群管理的范围，通过配置管理 VLAN，可实现如下功能：

- 集群的管理报文（包括 NDP、NTDP 报文以及握手报文）都将限制在管理 VLAN 内，与其它报文隔离，增加了安全性。
- 管理设备和成员设备通过管理 VLAN 实现内部通讯。

Command	Description	CLI mode
cluster management-vlan <vlan-id>	指定管理VLAN。缺省管理VLAN为VLAN1。	Configuration mode

NOTE：

If the current device is in the cluster, it is not allowed to modify the management VLAN.

Not in the cluster:

1） Check whether the VLAN exists. If there is no direct failure, continue to the next step

2）Recheck all interfaces. If the VLAN where the interface is located and the management VLAN are not the same VLAN, turn on the global switches of NDP and ntdp, turn off and clear them accordingly, and then turn them on again.

3） Find the layer-3 interface of the VLAN to be configured. If it is not found, create a layer-3 interface corresponding to the VLAN. If the creation fails, the management VLAN is configured successfully. You can NDP and ntdp, but you cannot join the cluster.

4） Set the MAC of the current layer 3 interface to dev_ ID. if the VLAN is set successfully and the new layer 3 interface fails, the MAC of vlan1 is used as the dev_ id

If the management VLAN has been configured, but the user directly deletes the VLAN in the VLAN database, the management VLAN will be automatically set to vlan1, and the global switches of NDP, ntdp and cluster that have been turned on will be turned off, and the corresponding closing and emptying operation will be performed.

Before establishing a cluster, the user must first set the private IP address range used by the member devices in the cluster. When the candidate devices join, the management device dynamically allocates a private IP address that can be used in the cluster range and sends it to the candidate devices for communication within the cluster, so as to realize the management and

maintenance of the management device to the member devices。

Command	Description	CLI mode
cluster ip-pool <IP/MASK>	onfigure the private IP address range used by the member devices in the cluster on the device to be set as the management device。	Configuration mode

NOTE:

- *The IP address and cluster address pool of VLAN interface of management equipment and member equipment cannot be configured in the same network segment, otherwise the cluster will not work normally。*
- *Only when the device is not in the cluster can it be configured。*
- *Use the management VLAN to find out whether there is a corresponding layer-3 interface. If there is no layer-3 interface, it will directly return failure. (the device cannot be used as a cluster command switch) if there is a three-layer interface, configure the base address of ip-pool to the three-layer interface. If the configuration fails, the ip-pool configuration also fails。*

By default, the device is not a management device, and the cluster is established：

Command	Description	CLI mode
cluster build <name>	Create a cluster manually, configure the current device as a management device, and assign a cluster name at the same time.	Configuration mode
cluster auto-build <name>	Automatically establish clusters. The automatic cluster function automatically adds all candidate devices found within the specified hop number range to the created cluster.	Configuration mode
cluster delete <name>	Delete the cluster.	Configuration mode
cluster stop auto-add member	In the case of automatic cluster establishment configuration, stop automatically joining the	Configuration mode

	member switch. This operation can only stop adding new devices. Devices that have joined the cluster will remain in the cluster.	

note：

- *The user can only specify the management VLAN before establishing the cluster. After the device has joined the cluster, the user cannot modify the management VLAN. If the management VLAN needs to be changed after the cluster is established, delete the cluster on the management device, reassign the management VLAN, and finally re-establish the cluster。*
- *For security reasons, it is recommended not to configure the management VLAN as the default VLAN ID of the port connected between the management device and the member device and the cascade port。*
- *Only when the default VLAN ID of the port connected to the management device and the member device and all cascaded ports are management VLANs, can the message of management VLANs be allowed to pass without labels. Otherwise, the management device, the port connected to the member device and all cascaded ports must be configured to allow the message of management VLANs to pass with labels. See "VLAN" for specific configuration。*
- *The private IP address range of the member devices in the cluster can be configured only when the cluster has not been established, and can only be configured on the management device. If the cluster has been established, the system cannot modify the IP address range。*

1.107.8 Configure member interaction within the cluster

In the cluster, the management device communicates with the member devices in real time through handshake messages to maintain the connection status between them. The time interval for sending handshake messages and the effective retention time of the devices can be configured on the management device. This configuration will take effect for all member devices in the cluster at the same time。

Command	Description	CLI mode
cluster timer <interval-time>	Configure the time interval for sending handshake	Configuration mode

	messages. The default is 10 seconds.	
cluster holdtime <hold-time>	Configure the effective retention time of the device. Default 60 seconds	Configuration mode

1.107.9 Configure cluster member management

The user can manually specify the candidate devices to be added to the cluster on the management device, or manually delete the candidate devices in the cluster

The specified member device. The join / delete operation of cluster members must be performed on the management device, otherwise an error will be returned

Error prompt information。

Command	Description	CLI mode
cluster add member mac-address <mac-address>	Join the candidate devices to the cluster.	Configuration mode
cluster delete member mac-address <mac-address>	Remove member devices from the cluster.	Configuration mode

1.108 Configure member devices

1.108.1 Enable NDP function of system and port

Refer to NDP function of enabling system and port

1.108.2 Enable ntdp function of system and port

Refer to ntdp function of enabling system and port

1.108.3 Configure manual collection of ntdp information

Refer to configuring manual collection of ntdp information **Enable cluster function**

1.109 Configure access cluster members

After the NDP, ntdp and cluster functions are configured correctly, the member devices in the cluster can be configured, managed and monitored through the management device. You can switch to the specified member device operation interface on the management device to configure and manage the member device。

Command	Description	CLI mode
cluster switch-to member <member-number>	Switch from the management device operation interface to the member device operation interface.	Normal mode, privileged mode

NOTE：

Telnet connection is used for the mutual switching between cluster management equipment and member equipment, which shall be noted during switching

meaning：

- *before switching, the opposite equipment needs to execute the "telnet server enable" command to enable the telnet function, otherwise the switching will fail。*

switch from the management device to the member device. If the member number n does not exist, an error message will be displayed

If the telnet user of the device requested to log in is full, the handover will fail。

1.110 集群管理显示与维护

Command	Description	CLI mode
show ndp[interface <ifname>]	Display NDP configuration information	Normal mode, privileged mode
reset ndp statistics [interface <ifname>]	Clear NDP statistics	Configuration view
show ntdp	Display system ntdp information	Normal mode, privileged mode
show ntdp device-list	Displays the device information collected by ntdp	Normal mode, privileged mode

show ntdp single-device mac-address <mac-address>	Displays ntdp details for the specified device	Normal mode, privileged mode
show cluster	Displays the status and statistics of the cluster to which the device belongs	Normal mode, privileged mode
show cluster topology	Display cluster topology information	Normal mode, privileged mode
show cluster candidates [mac-address <mac-address>]	Display candidate device information	Normal mode, privileged mode
show cluster members [<member-number>]	Displays cluster member information.	Normal mode, privileged mode

1.111 Typical configuration examples of cluster management

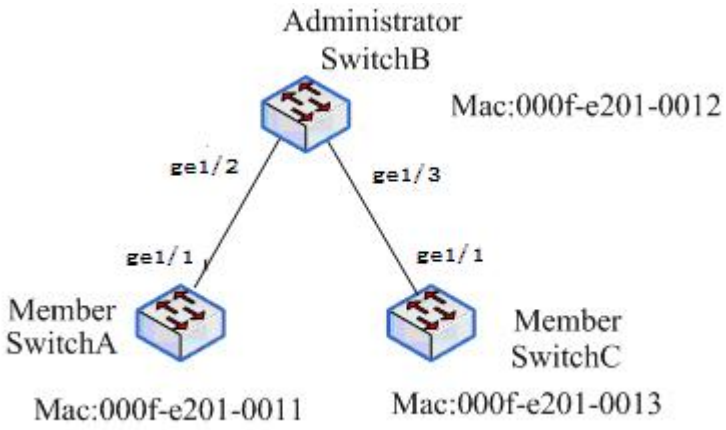
1. Networking requirements

The cluster ABC is composed of three switches, and its management VLAN is VLAN 10. Switch B is the management device

（Administrator）； Switch a and switch C are member devices.

The base ip address of the entire cluster address pool is 10.0.0.1, supporting 8 devices.

2. Networking diagram：



3. Configuration steps：

Configure member device switchA

configuration management VLAN。

[SwitchA] cluster management-vlan 10

[SwitchA] interface ge1/1

[SwitchA-ge1/1] switch access vlan 10

Enable global NDP function and NDP function on port GE1 / 1。

[SwitchA] ndp global enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ndp enable

Enable global ntdp function and ntdp function on port GE1 / 1。

[SwitchA] ntdp global enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ntdp enable

Enable cluster function。

[SwitchA] cluster enable

Configure member devicesSwitchC

Since the configuration of member devices is the same, the configuration on switch C is similar to that of switch a, and the configuration process is slightly different.

Configuration management device switchb

#Configuration management VLAN。

[SwitchB] cluster management-vlan 10

[SwitchB] interface ge1/2

[SwitchB-ge1/2] switch access vlan 10

[SwitchB] interface ge1/3

[SwitchB-ge1/3] switch access vlan 10

Enable global NDP and ntdp functions, and enable NDP and ntdp functions on ports GE1 / 2 and GE1 / 3 respectively。

[SwitchB] ndp global enable

[SwitchB] ntdp global enable

[SwitchB] interface ge1/1

[SwitchB-ge1/2] ndp enable

[SwitchB-ge1/2] ntdp enable

[SwitchB] interface ge1/3

[SwitchB-ge1/3] ndp enable

[SwitchB-ge1/3] ntdp enable

Configure the aging time of NDP message sent by the device on the receiving

device to be 200 seconds。

[SwitchB] ndp timer aging 200

Configure the time interval for sending NDP message to be 70 seconds。

[SwitchB] ndp timer hello 70

The maximum number of hops for configuring topology collection is 2。

[SwitchB] ntdp hop 2

Configure the delay time of forwarding topology collection request message at the first port of the collected device to be 150ms。

[SwitchB] ntdp timer hop-delay 150

Configure the delay time of other ports of the collected device to forward topology collection request message to 15ms。

[SwitchB] ntdp timer port-delay 15

The time interval for configuring topology collection is 3 minutes。

[SwitchB] ntdp timer 3

Enable cluster function。

[SwitchB] cluster enable

Configure the private IP address range of the member device as 10.0.0.1～10.0.0.9。

[SwitchB] cluster ip-pool 10.0.0.1 8

Configure the current device as the management device, and establish a cluster named ABC. Members will automatically join the cluster。

[SwitchB] cluster autobuild abc

After adding all the switches you want to add, you can turn off the auto join cluster function

[SwitchB]cluster stop auto-add member

SNTP Configuration

This chapter mainly includes the following contents：

- Introduction
- Configure SNTP
- Display SNTP

1.112 SNTP introduction

At present, the communication protocol is widely used on the Internet to realize network time synchronization, that is, NTP (Network Time Protocol). Another protocol is a simplified version of NTP protocol, that is, SNTP (Simple Network Time Protocol)

NTP protocol can span various platforms and operating systems and use very precise algorithms, so it is hardly affected by network delay and jitter, and can provide 1-50ms accuracy NTP also provides authentication mechanism with high security level However, NTP algorithm is complex and requires high system requirements

SNTP (Simple Network Time Protocol) is a simplified version of NTP. In its implementation, a simple algorithm is used to calculate the time, and the performance is high The accuracy can generally reach about 1 second, which can basically meet the needs of most occasions

Since the SNTP message and NTP message are completely consistent, the SNTP client implemented by this switch can be fully compatible with NTP server

1.113 Configure SNTP

1.113.1 Default SNTP settings

project	Default value
SNTP status	Disable close SNTP service
NTP Server	no
Synchronization interval of SN	1800 seconds
Local time zone	+8, East 8

Open or closeSNTP

Configuraiton as below:

Switch# configure terminal

Enter global configuration mode

Switch(config)# sntp enable

Open SNTP

Switch(config)# sntp disable

Close SNTP

1.113.2 Configure SNTP server ground 址

Since SNTP message and NTP message are completely consistent, SNTP client can be fully compatible with NTP server There are many NTP servers on the network. You can choose one with less network delay as the NTP server on the switch

The specific NTP server address can be logged in http://www.time.edu.cn/ or http://www.ntp.org/ Get o

For example, 192.43.244.18 (time. NIST. Gov)

The switch can be configured with up to three server addresses. The switch first uses the first server address to synchronize the time. If the synchronization cannot be reached, the second server address will be used, and so on.

The configuration of adding a server address is as follows:

Switch# configure terminal

Enter global configuration mode

Switch(config)# sntp server 210.72.145.44

Add the SNTP server IP. If the switch already has three server addresses, it will fail to add. You need to delete the address before adding

The configuration for deleting the server address is as follows：

Switch(config)# no sntp server

Delete all server addresse

Switch(config)# no sntp server 210.72.145.44

Delete a server addre

1.113.3 Configure the interval of SNTP synchronization clo

SNTP client needs to synchronize the clock with NTP server in order to correct the clock

The configuration is as follows:

Switch# configure terminal

Switch(config)# sntp interval 60

Set the interval of timing synchronization clock in seconds, ranging from 60 seconds to 65535 seconds The default value is 1800 seconds, which is set to 60 seconds here

Switch(config)# no sntp interval

The interval of timing synchronization clock is restored to the default 1800 seconds

1.113.4 Configure local time zone

The time obtained after communication through SNTP protocol is Greenwich mean time (GMT). In order to prepare for hunting the local time, you need to set the local area to adjust the standard time. By default, the local time zone of the switch is Dongba District, which is also the time zone of China.

The configuration is as follows:

Switch# configure terminal

Switch(config)# sntp time-zone -8

Set the local time zone to West Zone 8

Switch(config)# no sntp time-zone

The local time zone is restored to the eighth east zone

1.114 SNTP information display

Configuration as below:

Switch# show sntp

Switch# show running-config

ConfigureIGMP

This chapter mainly includes the following content：

- IGMP intrduction
- IGMP configuration
- IGMP configuration example

1.115 IGMP introduction

IGMP (Internet Group Management Protocol) is a part of multicast technology. It runs between the host and its directly connected multicast router. On the one hand, the host reports the multicast group it wants to join or leave to the local router. On the other hand, the multicast router can periodically query whether the local host is in the active receiving state for a specific group. IGMP protocol currently has three versions, version 1 (rfc1112), version 2 (rfc2236) and version 3 (rfc3376). IGMP is based on the query response mode. The multicast router uses the query message cycle to query whether the host in the subnet has a specific group it wants to receive. The host uses the report message to notify the local router of the multicast group it wants to join or leave, that is, the membership report. When the host wants to join a specific group, it does not need to wait for the periodic query message, and can immediately send the group membership report to the router. When the router queries the membership of the host in the subnet, the host uses the suppression mechanism to send the report message by delaying a random value between 1 and 10 seconds. When receiving the same group report message from other hosts, the host suppresses the sending of its own group member report, so as to reduce the IGMP traffic in the subnet. When there are multiple routers in the subnet, it is necessary to compare the IP addresses to select one as the inquirer to avoid too many IGMP query messages in the subnet. Version 1 only supports query and report. When a group member leaves, the multicast router will stop forwarding the multicast data stream only after waiting for the group information to timeout. The inquirer depends on other protocols for election. Version 2 supports the immediate departure of group members by adding a departure message. When the last group member leaves the group, it sends a departure message to the router, and the router sends a specific group query message to determine whether there are other receiving hosts in the subnet. When the corresponding group membership message is still not received after sending the configured number of retransmissions, the group becomes invalid, Stop forwarding multicast data stream.

Version 2 effectively reduces the departure delay through the departure mechanism. Version 2 provides a searcher election mechanism. When the general query message is received by other routers in the subnet, they select the one with the smallest IP address as the searcher by comparing their own IP address, and start a timer. Each time the query message is received, the timer resets. When the timer terminates, the new election process begins. In order to adjust the response time of the suppression mechanism of the host, the maximum response time field is added in the message of version 2. The inquirer can control the suppression response time of the host by adding this value to the query message. When the host receives the query message, it uses the maximum response time to generate a delay with the machine to start the timer, When the same group membership message of other hosts is received within this delay time, its own report message is inhibited. Version 3 supports specific source multicast. Query messages are divided into general query, specific group query and specific group specific source query; The report message expands the original group address field into group record entries. Each group record contains the group address and its corresponding source address list. Whether to join a specific source or not is distinguished by the group record type. Igmpv3 cooperates with pim-ssm to realize source specific multicast. SPT is directly established from source to receiver without the need of convergence point RP。

1.116 IGMP configuration

IGMP functions are mostly related to interfaces. Configure the corresponding parameters and timer values of each interface, and carry out relevant configuration in interface mode。

IGMP configuration includes：

- Start IGMP function of interface
- Configure the group filter access control list for the interface
- Configure the access control list filtered by the interface leaving the group
- Number of specific group queries for the configuration interface
- Configure the specific group query interval of the interface
- Configure the non querier timer time of the interface
- Configure the query timer interval of the interface
- Configure the maximum response time of the interface
- Configure interface parameters

- Configure the protocol version of the interface

1.116.1 Start IGMP function of interface

Mode: interface configuration mode

Command: IP IGMP Open IGMP protocol on the interface

Command: no IP IGMP Turn off IGMP protocol on the interface

Default: do not open IGMP protocol;

Use this command to start the interface to send and receive IGMP protocol messages. If the IP multicast routing command has started the multicast function support in the global configuration mode, the IGMP protocol function of the corresponding interface will be automatically started when the IP PIM spark mode command starts the PIM SM Protocol function in the interface configuration mode. Similarly, in the interface configuration mode, the no IP PIM spark mode command will automatically turn off the IGMP protocol function of the corresponding interface。

1.116.2 Configure the group filter access control list for the interface

Mode: interface configuration mode

Command: IP IGMP access group {< ACL ID > | < ACL name >}

Configure the group filter access control list for the interface

Command: no IP IGMP access group

Delete the group filter access control list for this interface

Parameter: < ACL ID > indicates the standard access control list number, which is an integer number between 1 and 99< ACL name > is the standard access control list name. Use ACL to filter the multicast address table learned by the interface. See the Command Reference Manual for ACL configuration details.

Default: group filtering ACL is not configured

1.116.3 Configure the access control list filtered by the interface leaving the group

Mode: interface configuration mode

Command: IP IGMP immediate leave group list {< acl-id1 > | < acl-id2 > | < ACL name >}

Configure the access control list filtered by the interface leaving the group

Command: no IP IGMP immediate leave

Delete the outgoing group filter access control list of this interface

Parameter: < ACL Id1 > indicates the standard access control list number, which is an integer number between 1 and 99< Acl-id2 > is the number of the extended range of the standard access control list, which is an integer number between 1300 and 1999< ACL name > is the standard access control list name. The ACL can be used to filter the multicast addresses that need to be filtered when the interface receives the departure messages of version 2 and version 3. Refer to the Command Reference Manual for ACL configuration details.

Default: leave group filtering ACL is not configured

1.116.4 Number of specific group queries for the configuration interface

Mode: interface configuration mode

Command: IP IGMP last member query count < count >

Configure the number of interface specific group queries

Command: no IP IGMP last member query count

The number of queries for a specific group of the recovery interface is the default value

Parameter: < count > indicates the number of specific group queries or specific source queries that need to be sent when receiving the departure message, which is an integer between 2-7. It is considered that the group has no receiving host until the group report message is not received during this period.

Default: 2

1.116.5 Configure the specific group query interval of the interface

Mode: interface configuration mode

Command: IP IGMP last member query interval < interval >

Configure the specific group query interval of the interface

Command: no IP IGMP last member query interval

The specific group query interval of the recovery interface is the default value

Parameter: < interval > indicates the time interval of a specific group query or a specific group source query. It is an integer between 1000-25500, in milliseconds; When a departure message is received, it is necessary to send a specific group or a specific

source query of a specific group for multiple times. This command configures the sending interval of multiple query messages. Until no group report message is received after multiple queries are sent, it is considered that the group or the source of the group has no receiving host.

Default: 1 seconds

1.116.6 Configure the non querier timer time of the interface

Mode: interface configuration mode

Command: IP IGMP query timeout < time >

Configure the non querier timer time of the interface

Command: no IP IGMP query timeout

The non querier timer time of the recovery interface is the default value

Parameter: < time > indicates the end time of the non inquirer timer, which is an integer between 60-300. When there are multiple switches on the subnet, one needs to be selected as the inquirer to send the query message. During network initialization, all switches send query messages by default. When receiving query messages from other switches, compare each other's IP addresses and select the one with the smaller IP address as the query. If they are not the query, start a timer. The timer is reset every time the query message is received. If the timer terminates, re select the query.

Default: 255 seconds

1.116.7 Configure the query timer interval of the interface

Mode: interface configuration mode

Command: IP IGMP query interval < interval >

Configure the query timer interval of the interface

Command: no IP IGMP query interval

The query timer interval of the recovery interface is the default value

Parameter: < interval > indicates the time interval of the query timer, which is an integer between 1-18000. When the interface starts IGMP protocol, it will start a query timer to send query messages to the subnet regularly; If there are multiple switches, it is necessary to elect a searcher. The searcher uses the timer to send query messages periodically. The non searcher closes the timer and starts a timeout timer. When the

timeout timer expires, the searcher is re elected.

Default: 125 seconds

1.116.8 Configure the maximum response time of the interface

Mode: interface configuration mode

Command: IP IGMP query Max response time < time >

Configure the maximum response time carried by the interface when sending query message

Command: no IP IGMP query Max response time

The maximum response time carried by the recovery interface when sending query message is the default value

Parameter: < time > indicates the maximum response time value to be carried by the interface when sending version 2 or version 3 query message, which is an integer between 1-240, with the unit of seconds, but the unit of the maximum response time in the query message is 0.1 seconds. IGMP uses the query response mode to obtain the information of the corresponding group of receiving hosts on the subnet. When a switch sends a query message, multiple hosts on the network will respond to the group report message. In order to avoid the congestion of many IGMP messages, a maximum response time value is carried in the query message, and the host receiving the query message generates a random value according to the maximum response time, The random value delay is used to send the response message. When the consistent group report message sent by other hosts is received during this delay, the group report message of the group to be sent is restrained, which effectively avoids the conflict of IGMP group reports at the same time. It should be noted that the maximum response time range of version 3 is larger than that of version 2, and the maximum response time range of version 2 is less than 128.

Default: 10 seconds

1.116.9 Configure interface parameters

Mode: interface configuration mode

Command: IP IGMP robustness variable < value >

Configure interface parameters

Command: no IP IGMP robustness variable

Restore the vitality parameter of the interface to the default value

Parameter: < value > indicates the vitality parameter of the interface, which is an

integer number between 2 and 7. The vitality parameter describes the robustness of the protocol. When the network environment is bad, the adaptability of the protocol to packet loss, and the configured vitality parameter value affects the number of retransmissions and the interval of relevant timers. The query message of version 3 contains QRV value, which is used to synchronize the vitality parameters locally configured by non inquirers.

Default: 2

1.116.10 Configure the protocol version of the interface

Mode: interface configuration mode

Command: IP IGMP version < version >

Configure the protocol version of the interface

Command: no IP IGMP versionl

The protocol version of the recovery interface is the default value

Parameter: < version > indicates the IGMP version number used, which is an integer number between 1 and 3.

Default: 3

1.117 IGMP configuration

(1) configuration

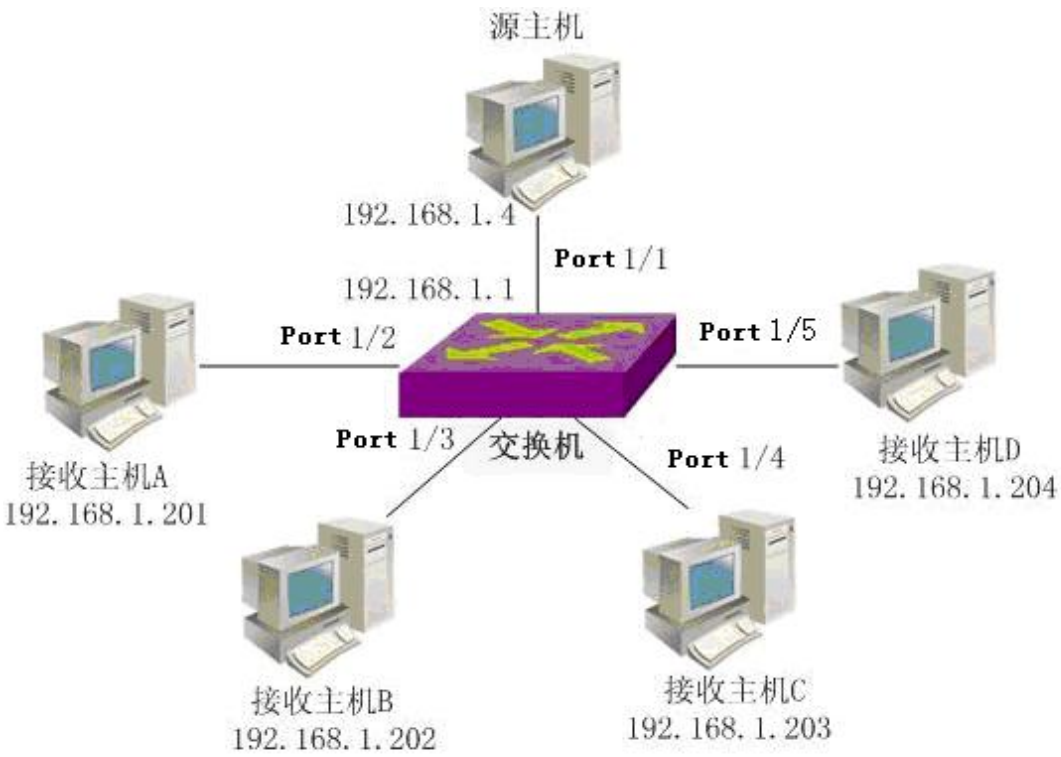
IGMP generally works together with multicast routing protocol (eg: PIM-SM). See PIM-SM configuration example. Starting multicast function (IP multicast routing) and PIM-SM protocol (IP PIM spark mode) of interface will automatically start corresponding IGMP protocol without configuring IP IGMP command separately. When receiving the multicast on demand service flow, you can view the corresponding IGMP group information and interface status.

When the source host and the receiving host are in the same subnet, the multicast data flow does not need to be forwarded across network segments, and the three-layer multicast routing is unnecessary, IGMP protocol and IGMP snooping can be started separately to realize multicast in the subnet. Note that the PIM-SM protocol must be started when writing the hardware table of layer 3 multicast.：

Switch# configure terminal

Switch(config)#interface vlan2

Switch(config-vlan2)#ip address 192.168.1.1/24
Switch(config-vlan2)#ip igmp
Switch(config-vlan2)#ip pim sparse-mode passive
Switch(config-vlan2)#interface ge1/1
Switch(config-ge1/1)#switch access vlan 2
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switch access vlan 2
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#switch access vlan 2
Switch(config-ge1/3)#interface ge1/4
Switch(config-ge1/4)#switch access vlan 2
Switch(config-ge1/4)#interface ge1/5
Switch(config-ge1/5)#switch access vlan 2



(2) verification

Use the following command to view IGMP information：

show ip igmp group

show ip igmp interface

Configure PIM-SM

This chapter mainly includes the following contents：

- PIM-SM introduction
- PIM-SM configuration
- PIM-SM configuration example

1.118 PIM-SM introduction

PIM-SM (Sparse Mode Protocol Independent Multicast - Sparse Mode) is a part of multicast technology. It is used for network topology discovery. It is a protocol running between routers. Compared with unicast point-to-point transmission, multicast point-to-multipoint transmission is committed to establishing a distribution tree, so that the source data flow can be transmitted along the distribution tree to the group member hosts that need to be received. There are two forms of distribution tree. One is based on the source. Each source has a distribution tree for each group. The shortest path is from the source to the group members. This active tree is also called the shortest path tree SPT; The other is to share an information distribution point. All sources of a group share a tree. The information of the source needs to be registered at this convergence point (RP: rendezvous point) before it can be transmitted down the distribution tree to the receiving host. This shared tree is also known as RPT. The distributed tree technology of PIM-SM

uses the form of one-way shared tree, that is, the data flow can only flow from the source to the receiver, not vice versa. The design goal of PIM-SM is to apply to Wan, that is, the receivers are sparsely distributed in the network, which is different from the diffusion pruning mode of dense mode. PIM-SM uses join pruning mode to establish a shared tree, that is, the receiving host uses explicit join mode (traditional IP multicast mode, the receiving end starts membership). The shared tree is a distribution tree shared by all sources of a group. When different sources need to push data streams, the source needs to register at the aggregation point, and then the aggregation point pushes the data to the receiver. The tree from source to aggregation point is the shortest path tree started by the data. When multiple sources register at the convergence point to forward data streams, the convergence point will become the bottleneck of the network. At this time, PIM-SM allows each source and group to switch to their own shortest path tree without passing through the convergence point. If in a small network, one convergence point is competent. If in a larger network, it is necessary to configure multiple RPS to share tasks, but the static configuration method does not adapt to the dynamic changes of the network. Therefore, PIM-SM provides RP bootstrap mechanism. Multiple candidate BSRs and candidate RPS are configured in the network. The candidate BSR elects the BSR. The candidate RP regularly sends its own group mapping information to the BSR. The BSR collects the RP information and arranges it into bootstrap information, which is regularly diffused in the network. Each router will save a bootstrap information. When a group member joins, look up the bootstrap information, find the RP corresponding to the group and send a join message to the RP direction. If there is no RP corresponding to the group in the bootstrap information, use the hash algorithm to map the group to a RP and send a join message to the RP direction. The assertion mechanism and network sharing mechanism of pim-dr are considered at the same time. Specify that the router Dr should be applied to the process of joining the distribution tree, and the assertion should be applied to the process of forwarding data flow. PIM-SM has become the first choice of intra domain multicast routing protocol because of its exquisite design; Later, pim-ssm is extended to enable users to receive services directly from multicast sources. This model has more outstanding advantages than traditional PIM-SM.

Aiming at the application of multicast protocol on layer 3 switch, the concept of multicast security is proposed. Multicast technology can be divided into three parts: one is multicast source discovery, the other is multicast receiver discovery, and the third is topology discovery. One part of multicast protocol is the protocol between host and router, such as IGMP; One part is the protocol between routers, such as PIM-SM. Multicast protocol, whether between host and router or between router and router, uses three-layer interface to describe the input and output direction of multicast routing; For a layer-3

switch, if a layer-3 interface is the output interface of a multicast route, then all layer-2 ports in the VLAN corresponding to the layer-3 interface will be output ports. As there is only one VOD host in the downstream VLAN, other output ports in the VLAN are unnecessary. Therefore, IGMP snooping protocol runs in layer 2, which is responsible for monitoring IGMP messages from a port and recording them. When there is a data stream, it is only sent to the requested port when it is output from the VLAN. That is, the information of layer 2 ports needs to be recorded on the layer 3 switch. Similarly, between routers, in order to maintain the multicast distribution tree, it is necessary to send a join pruning message. If the sending and receiving ports of PIM protocol messages are also monitored, the output interface of the multicast routing table will also record the corresponding layer-2 ports. When a data stream flows through the multicast tree, it will only be sent to the ports where the join message arrives in the VLAN, not to all ports in the VLAN. The layer-2 protocol that monitors PIM protocol messages is called PIM snooping. With IGMP snooping and PIM snooping, the multicast routing protocol running on the router can run well on the layer 3 switch. The entries in the multicast routing table will be shown as follows:

Multicast source address multicast group address input interface output interface list output port list

When there is an on-demand data stream, we will see that the branch of the multicast distribution tree from the source to the receiving host is along the layer 2 port where the protocol message once appeared, rather than flooding in the VLAN corresponding to the layer 3 interface.

IGMP snooping and PIM snooping are dynamic monitoring protocols, which record the layer-2 port information according to the protocol message. Currently switch v3 Version 0 only provides the static configuration function of refining multicast routing entries to layer 2 ports. For this function module, we call it multicast security. Through static configuration commands, it specifies that the output of a multicast data stream is only sent to the specific layer 2 port in the VLAN corresponding to the output interface. By default, the data flow will be output to all layer-2 ports in the VLAN corresponding to the output interface。

1.119 PIM-SM configuration

PIM-SM protocol needs to be started one by one on each interface after the layer 3 multicast function is started, and its relevant commands are in global configuration mode and interface configuration mode.

The configuration of PIM-SM includes：

Start multicast routing function

Configure multicast routing table capacity

Configure TTL value of multicast interface

Start interface PIM SM function

Configure passive mode of interface

Configure interface priority

The configuration interface Hello message does not contain genid information

Configure interface Hello timer interval

Configure the holding time of neighbors on the interface

Configure neighbor list filtering of the interface

Configure the source address of unicast registration message

Configure the number limit of registered messages

Check RP when configuring registration

Configure registration inhibit timer time value

Configure and register Kat timer time value

Configure registration source address filtering

Configure the checksum of the registered message in Cisco mode

Configure static RP address

Configure candidate RP

Configure ignore RP set priority

Configure c-rp-adv message in Cisco mode

Configure candidate BSR

Configure JP timer interval

Configure SPT (shortest path tree) switching

Configure SSM (source specific multicast)

1.119.1 Start multicast routing functio

Mode: global configuration mode

Command: IP multicast routing Enable multicast routing

Command: no IP multicast routing Turn off multicast routing function

Default: do not start multicast routing function; Use this command to start multicast routing function and PIM-SM and IGMP protocols。

1.119.2 Configure multicast routing table capacity

Mode: global configuration mode

Command: IP multicast route limit < limit > [threshold]

Configure the capacity and alarm threshold of multicast routing table

Command: no IP multicast route limit

Restore the capacity and alarm threshold of multicast routing table to the default value

Parameter: < limit > indicates the capacity of multicast routing table, which is an integer number between 1-2147483647; [threshold] indicates the alarm threshold of the multicast routing table, which is an integer number between 1-2147483647. It can be configured optionally. When the multicast routing table exceeds the alarm threshold, the switch will display a prompt message.

Default: 2147483647

1.119.3 Configure TTL value of multicast interface

Mode: interface configuration mode

Command: IP multicast TTL threshold < threshold >

Configure TTL value of multicast interface

Command: no IP multicast TTL threshold

Recovery multicast interface TTL value is invalid

Parameter: < threshold > indicates the TTL value of the multicast interface, which is an integer between 0-255, and 256 is an invalid value. This command configures the TTL value of the interface and is used to maintain the output interface list of the multicast routing table. When the configured TTL value is between 0-255, the value will be passed to the actual multicast interface. When the value is 256, the actual multicast interface uses its own default TTL value of 1.

Default: 256

1.119.4 Start interface PIM SM function

Mode: interface configuration mode

Command: IP PIM spark mode

Start interface PIM SM Protocol

Command: no IP PIM spark mode

Close interface PIM SM Protocol

Default: the interface does not start the PIM SM Protocol. Use this command to start the PIM SM Protocol function of the interface, send and receive protocol messages, and participate in RP election when bootstrapping is configured. When the interface starts PIM

SM, IGMP protocol will be started accordingly. There is no need to configure IP IGMP command。

1.119.5 Configure passive mode of interface

Mode: interface configuration mod

Command: IP PIM spark mode passive

Configure the interface to passive mode

Command: no IP PIM spark mode passive

The active mode of the cancelled interface is the recovery state of the passive interface

Default: the PIM SM Protocol is not started. When the PIM SM function of the interface is started by using the IP PIM spark mode command, it is in the active state, and the interface sends and receives protocol messages normally; When the configuration is in passive mode, the interface does not send protocol messages, does not participate in the registration process, does not participate in the RP election process, and only quietly monitors protocol messages。

1.119.6 Configure interface priority

Mode: interface configuration mode

Command: IP PIM Dr priority < priority >

Configure the priority of interface participating in Dr election

Command: no IP PIM Dr priority [priority]

Restore interface priority to default

Parameter: < priority > indicates the priority of the interface participating in Dr election, which is an integer number between 0-4294967294. When there are multiple switches on the shared network, one is elected as Dr through the Hello protocol, which is responsible for sending the join pruning message to the upstream. In the election of DR, the priority shall be compared first and the one with higher priority shall be selected; With the same priority, select the one with the larger IP address as the Dr.

Default: 1

1.119.7 The configuration interface Hello message does not contain genid information

Mode: interface configuration mode

Command: IP PIM exclude genid

The configuration interface Hello message does not contain the genid domain

Command: no IP PIM exclude genid

The default message recovery interface is configured as hello genid

Default: contains the genid domain; Type 20 in the Hello message option list is the option value of generation ID, which is an unsigned 32-bit value randomly generated during interface startup. It is used to quickly identify whether there is neighbor restart and reduce the delay of relearning RP set information and adding pruning state due to router restart. The switch retains the genid value in the Hello message, and will update this value after receiving a new Hello message. If the genid changes, it is considered that the neighbor restarts and needs to inform it of relevant information in time, instead of waiting for the timer to terminate before learning by itself, which reduces the convergence time when the network changes。

1.119.8 Configure interface Hello timer interva

Mode: interface configuration mode

Command: IP PIM Hello interval < interval

Configure the Hello timer interval of the interface

Command: no IP PIM Hello interval

The recovery interface Hello timer interval is the default value

Parameter: < interval > indicates the interval of Hello message sent by the interface, which is an integer between 1-65535. The setting of Hello timer interval will affect the holdtime value, which is 3.5 times that of Hello interval. When the value is not configured or the configured value is less than hello interval, it needs to be calculated according to Hello interval.

Default: 30 seconds

1.119.9 Configure the holding time of neighbors on the interface

Mode: interface configuration mode

Command: IP PIM Hello holdtime < value >

Configure the holding time of neighbors sending Hello messages

Command: no IP PIM Hello holdtime

The recovery neighbor retention time is the default value

Parameter: < value > indicates the survival time of neighbors, which is an integer number between 1-65535; If the Hello message is not received within the hold time, it is considered that the neighbor no longer exists. When configuring this value, it must be greater than the value of Hello interval. If it is less than the value of Hello interval, 3.5

times of Hello interval will be used as the value of hold time

Default: 105 seconds (3.5 times the Hello interval)

1.119.10 Configure neighbor list filtering of the interface

Mode: interface configuration mode

Command: IP PIM neighbor filter {< ACL ID > | < ACL name >}

Configure the neighbor list filtering ACL of the interface

Command: no IP PIM neighbor filter {< ACL ID > | < ACL name >}

Cancel neighbor list filtering of interface

Parameter: < ACL ID > indicates the number of the standard access control list, which is an integer number between 1 and 99< ACL name > indicates the standard access control list name. Use ACL to filter the neighbor list of the interface. When the neighbor is filtered by ACL, it will be deleted from the neighbor list of the interface. Refer to the Command Reference Manual for ACL configuration details.

Default: neighbor filtering ACL is not configured

1.119.11 Configure the source address of unicast registration message

Mode: global configuration mode

Command: IP PIM register source {< IP > | < if name >}

Configure the source address or interface name of unicast registration message

Command: no PIM register source

Cancel the configuration of registered source address

Parameter: < IP > indicates the source address of unicast registration message, in dotted decimal format< If name > indicates the source interface name of unicast registration message, which is the layer 3 interface name (eg: vlan2). The address used to register the message source.

Default: the source address of the registration message is not configured, and the interface address of the received packet is used。

1.119.12 Configure the number limit of registered message

Mode: global configuration mode

Command: IP PIM register rate limit < limit >

Configure the threshold of the number of registered messages received within one second

Command: no IP PIM register rate limit

Cancel registration message quantity limit check

Parameter: < limit > indicates the maximum number of registered messages that can be received within 1 second, which is an integer number between 1-65535. The registration message actually encapsulates the data packet. When the source registers, there will be a large data flow impacting the first hop router of the source. At this time, the data flow of PIM SM Protocol can be limited to avoid a large burden on the router. Because PIM SM only needs data flow to trigger SPT establishment from source to RP, the restriction mechanism can be used. When limiting the data flow, check the number of data packets within 1 second. If the arrival interval of two data packets exceeds 1 second, there is no limit.

Default: no limit on the number of registered messages is configured (the threshold value is 0)

1.119.13 Check RP when configuring registratio

Mode: global configuration mode

Command: IP PIM register RP reachability

Check whether RP is reachable when configuring registration

Command: no IP PIM register RP reachability

There is no need to check whether the RP is reachable when configuring registration

Default: there is no need to check whether the RP is reachable during registration

1.119.14 Configure registration inhibit timer time value

Mode: global configuration mode

Command: IP PIM register suppression < value >

Configure registration inhibit timer time value

Command: no IP PIM register suppression

The resume registration suppression timer time is the default value

Parameter: < value > indicates the time value of the registration suppression timer, which is an integer number between 1-65535.

Default: 60 seconds

1.119.15 Configure and register Kat timer time value

Mode: global configuration mod

Command: IP PIM RP register Kat < value >

Configure the Kat timer time of (s, g) entries registered and created on RP

Command: no IP PIM RP register Kat

The Kat timer time of recovery (s, g) is the default value

Parameter: < value > indicates the time value of Kat timer of (s, g) entries created by source registration on RP, which is an integer number between 1-65535.

Default: 185 seconds（3 * register-suppression + register-probe）

1.119.16 Registration address configuration

Mode: global configuration mode

Command: IP PIM accept register list {< acl-id1 > | < acl-id2 > | < ACL name >

Configure the source filter list of registration message

Command: no IP PIM accept register

Source filter list of unregistered message

Parameter: < ACL Id1 > indicates the number of the extended access control list, which is an integer between 100 and 199< Acl-id2 > indicates the number of the extended part of the extended access control list, which is an integer number between 2000-2699< ACL name > indicates the name of the access control list. The access control list can be used to filter the source address registered to the RP. if the source address on the RP is filtered by ACL, the corresponding (s, g) entry will be deleted from the multicast routing table. Refer to the Command Reference Manual for ACL configuration details.

Default: ACL of registration source is not configured

1.119.17 Configure the checksum of the registered message in Cisco mode

Mode: global configuration mode

Command: IP PIM Cisco register checksum [group list {< ACL Id1 > | < ACL Id2 > | < ACL name >}]

Configure the checksum of the registered message as Cisco mode

Command: no IP PIM Cisco register checksum [group list {< ACL Id1 > | < ACL Id2 > | < ACL name >}]

The checksum of unregistered message is Cisco mode

Parameter: < ACL Id1 > indicates the number of the standard access control list, which is an integer number between 1-99< Acl-id2 > indicates the number of the extended part of the standard access control list, which is an integer number between 1300 and 1999< ACL name > indicates the name of the standard access control list. The checksum of Cisco mode is to calculate the checksum of the whole registration message (including the data packet part), while the checksum of general registration message only includes the header of PIM SM protocol message and the header of registration message. If the access control list is configured, the ACL is required to filter the corresponding group address when sending the registration message. The Cisco checksum can be used through the ACL, but the general checksum can not be used through the ACL.

Default: Cisco checksum is not configured

1.119.18 Configure static RP address

Mode: global configuration mode

Command: IP PIM RP address < IP > [< acl-id1 > | < acl-id2 > | < ACL name >]

Configure static RP

Command: no IP PIM RP address < IP > [< acl-id1 > | < acl-id2 > | < ACL name >]

Cancel static RP configuration

Parameter: < IP > indicates the address of static RP, in dotted decimal format< ACL Id1 > indicates the number of the standard access control list, which is an integer number between 1 and 99< Acl-id2 > indicates the number of the extended part of the standard access control list, which is an integer number between 1300 and 1999< ACL name > indicates the name of the standard access control list.

Default: static RP is not configured

1.119.19 Configure candidate RP

Mode: global configuration mode

Command: IP PIM RP candidate < if name > [group list {< ACL ID > | < ACL name >} | interval < value1 > | priority < Value2 >]

The configuration interface is c-rp

Command: no IP PIM RP candidate [if name]

Cancel interface C-RP attribute

Parameter: < if name > indicates the name of the interface configured as C-RP, which is the name of the three-tier interface (eg: vlan2)< ACL ID > indicates the number of the standard access control list, which is an integer between 1 and 99< ACL name > indicates the name of the standard access control list< Value1 > indicates the time interval from

C-RP periodic unicast c-rp-adv message to BSR, which is an integer number between 1-16383< Value2 > indicates the priority of C-RP, which is an integer number between 0 and 255. It is included in the bootstrap information. It is used to flood in the domain for the selection of RP corresponding to the group.

Default: value1 defaults to 60 seconds; Value2 defaults to 192。

1.119.20 Configure ignore RP set priority

Mode: global configuration mode

Command: IP PIM ignore RP set priority

Configure to ignore priority and use hash algorithm mapping when searching RP in RP set

Command: no IP PIM ignore RP set priority

Configure to find RP usage priority in RP set

Default: find the priority order of RP in RP set

1.119.21 Configure c-rp-adv message in Cisco mode

Mode: global configuration mode

Command: IP PIM CRP Cisco prefix

Configure the c-rp-adv message to a format acceptable to Cisco BSR

Command: no IP PIM CRP Cisco prefix

Configure c-rp-adv message to standard RFC format

Default: c-rp-adv message is in standard RFC format. Cisco BSR does not receive c-rp-adv messages. The prefix CNT domain is 0. If there is no group address by default, the prefix CNT domain is 1. Fill in a 224.0.0.0 group address. The standard RFC defaults to 0 in the prefix CNT field if there is no group address. This command is compatible with BSR. It is a Cisco router and needs to send c-rp-adv messages that can be recognized by Cisco BSR.

1.119.22 Configure candidate BSR

Mode: global configuration mode

Command: IP PIM BSR candidate < if name > [< hash mask len > | < priority >]

Configure the interface, priority and mask length of hash calculation of the candidate BSR

Command: no IP PIM BSR candidate [if name]

Cancel the candidate BSR identity of the interface

Parameter: < if name > indicates the interface name of the candidate BSR, which is

the layer 3 interface name (eg: vlan2)< Hash mash len > indicates the mask length in the hash algorithm, which is an integer number between 0-32< Priority > indicates the priority of the candidate BSR when participating in the BSR election. It is an integer number between 0-255. When the candidate BSR is selected as BSR, its hash mask len and priority are transmitted in the bootstrap message.

Default: the default value of priority is 0; The default value of hash mask len is 10。

1.119.23 Configure JP timer interval

Mode: global configuration mode

Command: IP PIM JP timer < time >

Configure upstream join pruning timer interval

Command: no IP PIM JP timer [time]

Restore the upstream join pruning timer interval to the default time

Parameter: < time > indicates the time interval for the switch to periodically send the pruning message to the upstream, which is an integer number between 1-65535. The switch maintains the forwarding state of the multicast distribution tree through the JP timer. Join the JP timer interval with the holding time of pruning state of 3.5 times, and the holding time is included in the join pruning message.

Default: 60 seconds

1.119.24 Configure SPT switching

Mode: global configuration mode

Command: IP PIM SPT threshold [group list < ACL Id1 > | < ACL Id2 > | < ACL name >]

Configure SPT switching

Command: no IP PIM SPT threshold [group list < ACL Id1 > | < ACL Id2 > | < ACL name >]

Cancel SPT switching

Parameter: < ACL Id1 > indicates the number of the standard access control list, which is an integer number between 1-99< Acl-id2 > indicates the number of the extended part of the standard access control list, which is an integer number between 1300 and 1999< ACL name > indicates the name of the standard access control list. When SPT switching is configured, the access control list can be used to filter the (*, g) entries of the multicast routing table. SPT switching can be configured through ACL, but SPT switching cannot be configured if it fails.

Default: SPT switching is not configured

1.119.25 Configure SSM

Mode: global configuration mode

Command: IP PIM SSM {default | range {< ACL ID > | < ACL name >}}

Configure SSM (source specific multicast)

Command: no IP PIM SSM

Cancel SSM

Parameter: < ACL ID > indicates the number of the standard access control list, which is an integer number between 1 and 99< ACL name > indicates the name of the standard access control list.

Default: SSM is not configured

1.119.26 Configure multicast security

Mode: global configuration mode

Command: IP mroute < SRC addr > < GRP addr > < IIF name > < OIF name > remove < if name >

For a multicast route (s, g), a specific layer-2 port in the corresponding VLAN of an output interface does not forward data flow

Command: IP mroute < SRC addr > < GRP addr > < IIF name > < OIF name > Add < if name >

Add an output port of a multicast route (s, g) back to the output interface corresponding to its VLAN

Parameters: SRC addr indicates the multicast source address of multicast route (s, g)

GRP addr represents the multicast group address of multicast routing (s, g)

IIF name indicates the input interface of multicast routing (s, g)

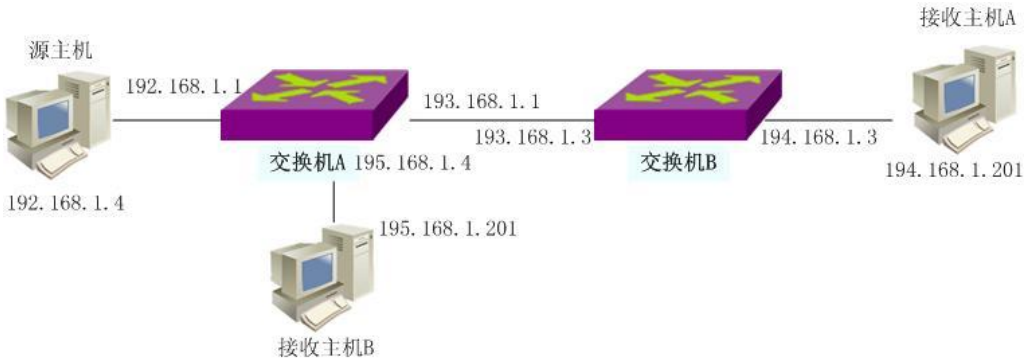
OIF name indicates the output interface of multicast routing (s, g)

If name indicates that the output interface of multicast routing (s, g) corresponds to the layer-2 port in the VLAN. The remove command shields the layer-2 port from the VLAN where the output interface is located, that is, the data flow forwarded from the output interface will not be forwarded from the layer-2 port. The add command adds the layer-2 port back to the VLAN where the output interface is located, that is, the data flow forwarded from the output interface will be forwarded from the layer-2 port.

Default: all layer 2 ports in the VLAN corresponding to the output interface will forward multicast data streams

1.120 PIM-SM Configuration example

(1) Configuration



Start PIM-SM protocol to enable the receiving host to receive multicast data stream from the source host。

On switch A：

Switch#configure terminal

Switch(config)#ip multicast-routing

Switch(config)#ip pim rp-address 193.168.1.3

Switch(config)#interface vlan2

Switch(config-vlan2)#ip address 192.168.1.1/24

Switch(config-vlan2)#ip pim sparse-mode

Switch(config-vlan2)#interface vlan3

Switch(config-vlan3)#ip address 193.168.1.1/24

Switch(config-vlan3)#ip pim sparse-mode

Switch(config-vlan3)#interface vlan5

Switch(config-vlan5)#ip address 195.168.1.1/24

Switch(config-vlan5)#ip pim sparse-mode

On switch B：

Switch#configure terminal

Switch(config)#ip multicast-routing

Switch(config)#ip pim rp-address 193.168.1.3

Switch(config)#interface vlan3

Switch(config-vlan3)#ip address 193.168.1.3/24

Switch(config-vlan3)#ip pim sparse-mode

Switch(config-vlan3)#interface vlan4

Switch(config-vlan4)#ip address 194.168.1.3/24

Switch(config-vlan4)#ip pim sparse-mode

(2) verification

Use the following command to view PIM-SM information：

show ip pim sparse-mode interface

show ip pim sparse-mode neighbor

show ip pim sparse-mode local-members

show ip pim sparse-mode mroute

show ip pim sparse-mode rp mapping

(3) Configure multicast security

The multicast security function module runs on the multicast routing protocol. First start the multicast routing protocol, and then configure the forwarding state of the layer-2 port of its output interface according to the specific origin of a multicast path. As shown in the figure below, vlan2 connects to the multicast source 192.168.1.4; There are four hosts in vlan3, which are connected to ports GE1 / 2, GE1 / 3, GE1 / 4 and GE1 / 5 respectively; As shown by the red arrow in the figure, only the host 193.168.202 on-demand broadcasts the programs of multicast group 224.91.91.2, and the other three hosts do not participate in multicast on-demand, so the data flow forwarded from the three layer-2 ports is unnecessary. GE1 / 2, GE1 / 4 and GE1 / 5 are shielded by configuring static multicast commands。

On the switch：

Switch#configure terminal

Switch(config)#ip multicast-routing

Switch(config)#ip pim rp-address 193.168.1.1

Switch(config)#interface vlan2

Switch(config-vlan2)#ip address 192.168.1.1/24

Switch(config-vlan2)#ip pim sparse-mode

Switch(config-vlan2)#interface ge1/1

Switch(config-ge1/1)#switchport access vlan 2

Switch(config-ge1/1)#interface vlan3

Switch(config-vlan3)#ip address 193.168.1.1/24

Switch(config-vlan3)#ip pim sparse-mode

Switch(config-vlan3)#interface ge1/2

Switch(config-ge1/2)#switchport access vlan 3

Switch(config-ge1/2)#interface ge1/3

Switch(config-ge1/3)#switchport access vlan 3

Switch(config-ge1/3)#interface ge1/4

Switch(config-ge1/4)#switchport access vlan 3

Switch(config-ge1/4)#interface ge1/5

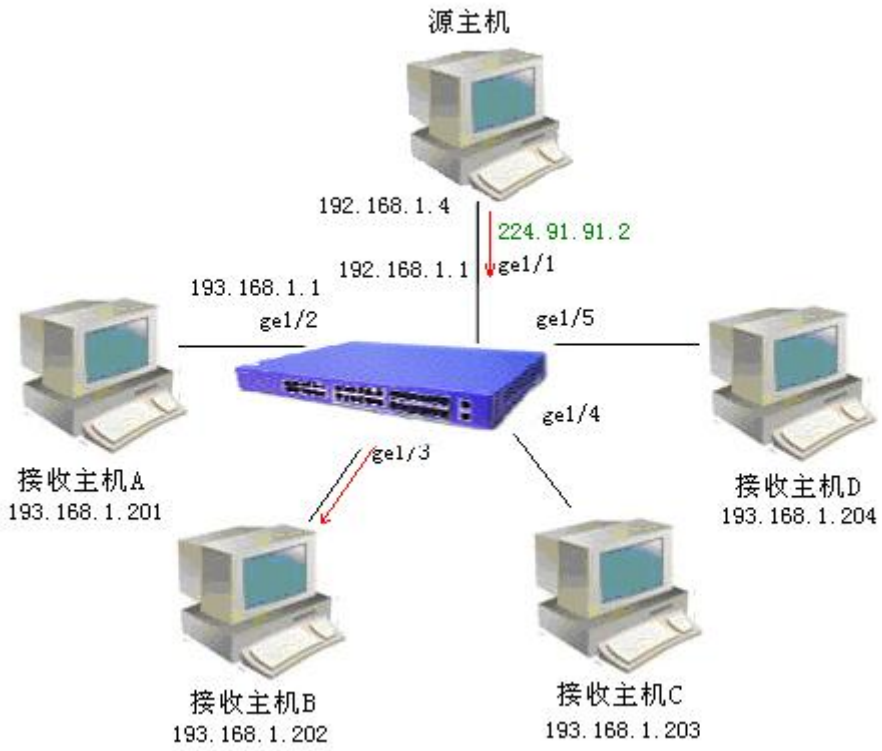
Switch(config-ge1/5)#switchport access vlan 3

Switch(config-ge1/5)#exit

Switch(config)#ip mroute 192.168.1.4 224.91.91.2 vlan2 vlan3 remove ge1/2

Switch(config)#ip mroute 192.168.1.4 224.91.91.2 vlan2 vlan3 remove ge1/4

Switch(config)#ip mroute 192.168.1.4 224.91.91.2 vlan2 vlan3 remove ge1/5



Configure RIP

This chapter mainly includes the following contents：

- RIP introduction
- RIP configuration
- RIP configuration example

1.121 RIP introduction

Rip (routing information protocol) is a dynamic routing protocol developed earlier. It uses distance vector algorithm and is mostly used in small networks. Rip protocol message is encapsulated in UDP message and uses UDP port 520. The main idea of RIP is to use hop to measure the distance to the host, and increase the hop by 1 for each router, so as to calculate the weight of the route and select the route. The maximum number of hops agreed by RIP is 15, and the number of hops 16 is marked as unreachable. Rip uses the method of broadcasting the entire routing table to make the routers in the network synchronize the routing information and update the message regularly every 30 seconds. If a routing entry does not receive the update message from the neighbor within 180 seconds, it will be marked as unreachable. If no effective update is received within 120 seconds, the route will be deleted.

Rip is easy to implement because of its simple idea, but it also brings the corresponding routing loop problem. In order to prevent the routing loop, rip introduces a horizontal segmentation mechanism to avoid deception between routers. Horizontal segmentation means that route updates will not be published from the received interface. The horizontal segmentation with toxic inversion is to publish the route update from the received interface, but the weight is marked as unreachable, so that the neighbor router can quickly identify the loop without waiting for the weight to increase to unreachable.

The routing entry in the routing table shall include the destination address (host or network), next hop address, forwarding interface, routing weight, timer (the timer is reset when receiving the routing update) and routing mark.

When rip starts, it will immediately send a full table request message in the form of broadcast (RIP-1) or multicast (RIP-2), and the adjacent routers will send back their complete routing table in response to the request message. After receiving the response message, the router will process the route one by one and modify its own routing table. When there is a new route, a trigger update message will be generated immediately. After

a series of updating process, rip converges finally, and each router in the network maintains the latest and consistent routing information. After the network is stable, rip still broadcasts the local routing table to the neighbors every 30 seconds. Each router maintains its own routing information according to the received routing update message and selects the most preferred route. Rip uses the timeout mechanism to process the routing entries that have not been updated for a long time to ensure the real-time and correct routing.

Rip is mostly used in campus networks and relatively continuous regional networks with simple structure. Rip is not competent for complex large-scale networks。

1.122 RIP configuration

After starting rip protocol, you can configure all functions and attributes of rip. Rip configuration is mostly in RIP configuration mode and interface configuration mode.

Rip configuration includes:

Start rip and enter rip configuration mode

Enable rip interface

Configure unicast message transmission

Configure the working state of the interface

Configure default routing weights

Configure management distance

Configure timer

Configuration version

Introducing external routing

Configure routing filtering

Configure additional routing weights

Configure rip version of interface

Configure the transceiver status of the interface

Configure horizontal segmentation

Message authentication

Configure interface weights

1.122.1 Start rip and enter rip configuration mode

Mode: global configuration mode

Command: router rip

Start rip and enter rip configuration mode

Command: no router rip

Close rip protocol

Default: do not run rip protocol

1.122.2 Enable rip interface

When rip works, it can specify some interfaces, configure its network as rip network, and send and receive rip protocol messages on it.

Mode: Rip configuration mode

Command: network < network address >

Enable rip interface

Command: no network < network address >

Close rip interface

Parameter: there are two forms: a.b.c.d/m and a.b.c.d. the former specifies the network IP and mask length, and the latter specifies the network IP and mask.

Default: disabled on all interfaces after rip protocol is started

After the rip protocol is started, the network segment it works on must be specified. Rip can only run on the interface of the specified network segment. For those interfaces that are not in the specified network segment, rip neither receives the sending route nor forwards the interface route. In RIP view, those interfaces that are not in the specified network segment do not exist. The parameter network address is the enabled or disabled network address, which can be configured as the interface IP address. The network command enables the interface of the network segment of the address. For example, if the IP address of an interface is 192.160.1.1, use the command network 192.160.1.1/24, and use the command show running config to see network 192.160.1.0/24。

1.122.3 Configure unicast message transmission

Rip protocol version 1 uses broadcast to exchange messages, and version 2 uses multicast (224.0.0.9) to exchange messages. When running rip protocol on a link that does not support broadcasting, it is necessary to specify a specific unicast address to exchange messages

Mode: Rip configuration mode

Command: neighbor < IP address >

Configure peer unicast IP address

Command: no neighbor < IP address >

Cancel the setting of peer unicast IP address

Parameter: IP address is the specified unicast IP address

Default: Rip protocol does not send messages to any unicast address

1.122.4 Configure the working state of the interfac

Rip protocol runs in some networks. It may only need rip interface routing and does not want to broadcast rip routing on this interface. Use the network command to specify the rip protocol message to be sent and received on the interface, and know the route of the interface. Use the passive interface command to only know the route of the interface and block the broadcast of the interface.

Mode: Rip configuration mode

Command: passive interface < if name >

Configure the interface to be passive

Command: no passive interface < if name >

Cancel interface passive state

Parameter: if name is the agreed three-tier interface name (for example: vlan1, vlan2...)

Default: all enabled rip interfaces are not in passive state

1.122.5 Configure default routing weights

When introducing an external route, you need to specify a route weight; When the routing weight is not specified, this default routing weight is used.

Mode: Rip configuration mode

Command: default metric < metric >

Set the default route weight when introducing external routes

Command: no default metric [Metric]

When the external route is restored, the default route weight is 1

Parameter: metric value is between 1 and 16, greater than 1 and less than 16.

Default: the metric value is 1. Use the no default metric command to restore to the default value。

1.122.6 Configure management distance

Each protocol has an agreed priority. Management distance is the priority of routing when using routing strategy. When there are two same routes (from different routing protocols) to the same destination, the smaller the management distance, the route of the protocol is preferred.

Mode: Rip configuration mode

Command: distance < distance >

Set management distance value

Command: no distance [distance]

The recovery management distance is the default value

Parameter: the value of distance is between 1 and 255

Default: the distance value is 120. Use the no distance command to restore to the default value。

1.122.7 Configure timer

Rip protocol has three timers. One is that the complete routing table broadcasts to all rip interfaces every 30 seconds. The other is that if each route in the rip routing table does not receive an update in 180 seconds, it will be marked with metric of 16. The third is that if each route in the rip routing table is marked with metric of 16 and is not effectively updated in 120 seconds, it will be deleted from the routing table.

Mode: Rip configuration mode

Command: timers basic < update > < timeout > < garbage >

Set three timer values

Command: no timers basic

The recovery timer is the default

Parameters: the first parameter update is the timer for regularly updating the whole rip routing table, the second parameter timeout is the timer for each route timeout without updating, and the third parameter garbage is the timer to be deleted after each route is marked as invalid; The value range of the three timers is 5 ~ (231-1).

Default: update every 30 seconds; When timeout is 180 seconds, it is marked as invalid; Garbage is deleted in 120 seconds

1.122.8 Configuration version

Rip protocol currently has version 1 (rfc1058) and version 2 (rfc2453). The configured version value will be reflected in the version field of protocol message.

Mode: Rip configuration mode

Command: version < version >

Set rip protocol to version 1 or version 2

Command: no version [version]

Restore the rip protocol version to the default value

Parameter: version can be 1 or 2

Default: version 2

1.122.9 Introducing external routing

Rip allows users to introduce the routing information of other protocols into the routing table of rip. The routing protocols (types) that rip can introduce include connected, static, OSPF, IS-IS and BGP.

Mode: Rip configuration mode

Command: redistribute {kernel | connected | static | OSPF | Isis | BGP} [Metric < metric > | route map < route map name >]

Introducing other protocol routes

Command: no redistribute {kernel | connected | static | OSPF | Isis | BGP} [Metric < metric > | route map < route map name >] Cancel incoming route

Parameter: the first parameter is the name of the imported other protocols, including direct connection, static, OSPF, is is and BGP; The second parameter is the weight set during import, with a value between 1 and 16; The third parameter is the name of the referenced route map. Route map is configured in the global configuration mode. Please refer to the command manual.

Default: Rip protocol does not introduce any external protocol

1.122.10 Configure routing filtering

Rip provides route filtering function, which filters the received routes and published routes through the specified access control list and address prefix list, and configures policy rules.

Mode: Rip configuration mode

Command: distribute list < ACL name > {in | out} [if name]

Use access list to filter the input and output of the interface

Command: no distribute list < ACL name > {in | out} [if name]

Cancel access list filtering

Parameter: ACL name indicates the name of the referenced access list; If name indicates the rip interface applied to; In and out indicate whether the application is in the direction of receiving routes or publishing routes.

Command: distribute list prefix < pre name > {in | out} [if name]

Filter using prefix list

Command: no distribute list prefix < pre name > {in | out} [if name]

Cancel using prefix list filtering

Parameter: pre name indicates the name of the referenced prefix list; If name indicates the rip interface applied to; In and out indicate whether the application is in the direction of receiving routes or publishing routes.

Default: Rip protocol does not filter any received and sent routes

Access list and prefix list are configured in global configuration mode. Please refer to the command manual。

1.122.11 Configure additional routing weight

Additional routing weight is an offset value added to the routing weight of rip protocol during input and output. It does not directly change the weight of the route in the routing table, but adds an offset when the interface receives and sends the route.

Mode: Rip configuration mode

Command: offset list < ACL name > {in | out} < offset > [if name]

Use access list to add an offset to the weight of interface input-output route

Command: no offset list < ACL name > {in | out} < offset > [if name]

Cancel the offset of the weight of the input-output route

Parameter: ACL name indicates the access list name of the reference; In and out indicate whether the application is in the input or output direction; Offset represents the value of the offset, which is between 0 and 16; If name indicates the rip interface applied to.

Default: when receiving a message, the additional weight of each route is 1, and when sending a message, the additional weight of each route is 0。

1.122.12 Configure rip version of interface

Rip is divided into two versions: RIP-1 and RIP-2. The version of rip message processed by the enabled rip protocol interface can be specified. The receiving direction can be divided into receiving only RIP-1 messages, receiving only RIP-2 messages, and receiving both RIP-1 and RIP-2 messages. In the sending direction, it can be divided into sending RIP-1 message, sending RIP-2 message (in broadcast mode), sending RIP-2 message (in multicast mode), sending both RIP-1 and RIP-2 messages. RIP-2 has two ways of sending messages: broadcast and multicast. Using multicast can not only avoid the host not running rip in the same network from not receiving rip broadcast messages,

but also avoid the host running RIP-1 from wrongly processing RIP-2's route with subnet mask.

Mode: interface configuration mode

Command: receive {version 124eip}

Set the interface to receive only version 1 messages or only version 2 messages

Parameter: Version 1 or version 2

Command: IP rip receive version {1 2 | 2 1}

The setting interface can receive both version 1 and version 2 messages

Parameter: can write 1 2 or 2 1

Command: no IP rip receive version [1 | 2 | 1 2 | 2 1]

The message received by the recovery interface is set to the default value

Default: version 2 multicast mode

Command: IP rip send version {1 | 2 | 1-compatible}

Set the interface to send only version 1 messages or only version 2 messages

Parameter: Version 1 or version 2; 1-compatible means that the version 2 interface sends a message compatible with version 1, that is, broadcast message rather than multicast.

Command: IP rip send version {1 2 | 2 1}

Setting the interface can send both version 1 and version 2 messages

Parameter: can write 1 2 or 2 1

Command: no IP rip send version [1 | 2 | 1-compatible | 1 2 | 2 1]

Set the message sent by the recovery interface to the default value

Default: version 2 multicast mode

1.122.13 Configure the transceiver status of the interface

After enabling the rip interface by using the network command in the rip mode, you can also specify the status of sending and receiving protocol messages, whether to receive protocol messages or send protocol messages in the interface mode.

Mode: interface configuration mode

Command: IP rip receive packet

Configure interface to receive protocol message

Command: no IP rip receive packet

The configuration interface does not receive protocol messages

Command: IP rip send packet

Configure interface to send protocol message

Command: no IP rip send packet

The configuration interface does not send protocol messages

Default: enable to receive and send protocol messages

Note the difference. The network command starts a network to run rip protocol. The interface in the network sends and receives protocol messages, and the interface route is included in the routing table. The passive interface command is to make the interface not send and receive protocol messages after the network command takes effect, but the interface route is still included in the routing table. The IP rip receive packet and IP rip send packet commands also specify whether the interface receives or sends protocol messages after the network command takes effect。

1.122.14 Configure horizontal segmentation

Horizontal segmentation means that the route received from this interface is not sent from this interface. Horizontal segmentation with toxic inversion means that the route received from this interface is still sent from this interface, but its metric value is marked as 16. Horizontal segmentation can avoid loops to a certain extent. The horizontal segmentation with toxic inversion is more efficient than ordinary horizontal segmentation, and direct labeling is not reachable. However, in nBMA network, it is necessary to prohibit horizontal segmentation to obtain the correct route.

Mode: interface configuration mode

Command: IP rip split horizon [poisoned]

Start the horizontal division function of the interface or with toxic inversion

Command: no IP rip split horizon

The horizontal division function of the interface is prohibited

Parameters: no poisoned parameter means to start the normal horizontal segmentation function, and with poisoned parameter means to start the horizontal segmentation function with toxic inversion.

Default: horizontal segmentation with toxic inversion

1.122.15 Message authenticatio

RIP-1 does not support message authentication, while RIP-2 supports message authentication. There are two authentication methods, plaintext authentication and MD5 authentication. The simultaneous interpreting of unencrypted authentication data in the plaintext authentication system can not provide security guarantee and can not be applied to the network with higher security requirements. The setting of password can be divided into ordinary key and key chain. The ordinary key saves an independent string. The key

chain manages the ID, content, received lifetime and sent lifetime of the key. See the Command Reference Manual for key chain management.

Mode: interface configuration mode

Command: IP rip authentication mode {text | MD5}

Set authentication mode plaintext or MD5

Command: no IP rip authentication mode [text | MD5]

Cancel authentication

Parameter: text is plaintext authentication, MD5 authentication.

Default: no authentication

Command: IP rip authentication string < password >

Set password string for authentication

Command: no IP rip authentication string [password]

Password string for de authentication

Parameter: 16 byte authentication passwor

Command: IP rip authentication key chain < key chain name >

Set the key chain for authentication

Command: no IP rip authentication key chain [key chain name] key chain to cancel authentication

Parameter: the name of the referenced key chain; The key chain is configured in the global configuration mode. Please refer to the command manual。

1.122.16 Configure interface weight

Mode: interface configuration mode

Command: IP rip metric < metric >

Configure interface weights

Command: no IP rip metric

Restore the interface weight to the default value

Parameter: the metric value is between 1-16, indicating the weight to be added to the routing entry learned by the interface.

Default: 1

1.122.17 Display information

Mode: normal mode or privileged mode

Command: show ip protocols

Displays information about all running protocols

Command: show ip protocols rip

Display rip protocol information

Command: show ip rip

Show rip routes

Command: show ip rip database

Show rip database

Command: show ip rip database count

Displays the number of rip database entries

Command: show ip rip interface [if name]

Display rip interface information

Parameter: if name is the agreed three-tier interface name

Mode: privileged mode

Command: show running config

Displays the current configuration of the switch, including rip configuration.

Show rip command

Displays the current configuration of rip protocol。

1.123 RIP Configuration example

(1) Configuration

The three switches are connected in pairs, with 6 network segments respectively. Rip protocol is enabled to realize the interworking between the three PCs.

On switch 1：

Switch# configure terminal

Switch(config)#router rip

Switch(config-rip)#network 192.168.1.0/24

Switch(config-rip)#network 10.1.1.0/24

Switch(config-rip)#network 10.1.2.0/24

On switch 2：

Switch# configure terminal

Switch(config)#router rip

Switch(config-rip)#network 192.168.2.0/24

Switch(config-rip)#network 10.1.2.0/24

Switch(config-rip)#network 10.1.3.0/24

On switch 3：

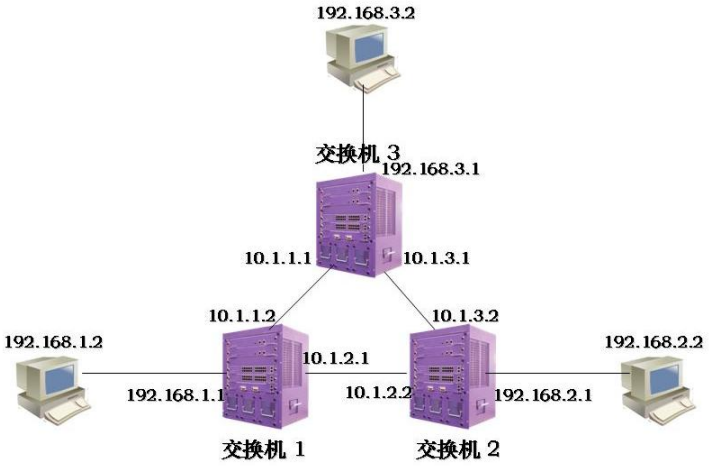
Switch# configure terminal

Switch(config)#router rip

Switch(config-rip)#network 192.168.3.0/24

Switch(config-rip)#network 10.1.1.0/24

Switch(config-rip)#network 10.1.3.0/24



(2) verification

Use the following command to view rip information：

show ip protocols rip

show ip rip database

show ip rip interface

Configure RIPng

This chapter mainly includes the following contents：

- RIPng introduction
- RIPng configuration
- RIPng configuration example

1.124 RIPng introduction

RIPng is a relatively simple internal gateway protocol, which is the application of rip in IPv6 network. RIPng is mainly used in smaller networks, such as campus networks and regional networks with simple structure. Since the implementation of RIPng is relatively simple, and it is much easier than OSPFv3 and IS-IS for IPv6 in configuration and maintenance management, RIPng is still widely used in practical networking

With the construction of IPv6 network, dynamic routing protocol is also needed to provide accurate and effective routing information for IPv6 message

forwarding. Therefore, on the basis of retaining the advantages of rip, IETF forms Rip (RIP next generation) for IPv6 network modification. RIPng is mainly used to provide routing function in IPv6 network. It is an important protocol of routing technology in IPv6 network.

Differences between RIPng and rip

In order to realize the application in IPv6 network, RIPng modifies the original rip protocol:

- RIPng uses port 521 of UDP (RIP uses port 520) to send and receive routing information.
- The destination address of RIPng uses a 128 bit prefix length (mask length).
- RIPng uses a 128 bit IPv6 address as the next hop address.
- RIPng uses the link local address fe80:: / 10 as the source address to send RIPng routing information update message.
- RIPng sends routing information periodically by multicast, and uses ff02:: 9 as the router multicast address within the local range of the link.
- RIPng message is composed of header and multiple route table entries. In the same RIPng message, the maximum number of RTE is determined according to the MTU value of the interface。

1.125 RIPng configuration

After starting RIPng protocol, you can configure various functions and attributes of RIPng. RIPng is mostly configured in RIPng configuration mode and interface configuration mode.

- RIPng configuration includes:
- Start RIPng and enter RIPng configuration mode
- Enable RIPng interface
- Configure specific neighbors to send updates
- Configure the working state of the interface

- Configure default routing weights
- Configure timer
- Introducing external routing
- Configure routing filtering
- Configure additional routing weights
- Configure horizontal segmentation
- Configure interface weights

Start RIPng and enter RIPng configuration mod

Mode: global configuration mode

Command: router IPv6 rip

Start RIPng and enter RIPng configuration mode

Command: no router IPv6 rip

Close RIPng protocol

Default: RIPng protocol is not run

1.125.1 Enable RIPng interface

When RIPng works, some interfaces can be specified, and the network it is in can be configured as RIPng network, on which RIPng protocol messages can be sent and received.

Mode: interface configuration mode

Command: IPv6 Router rip

Enable RIPng interface

Command: no IPv6 Router rip

Close RIPng interface

Parameter: none.

Default: disabled on all interfaces after RIPng protocol is started

After RIPng protocol is started, its working interface must be specified, and RIPng can only run on the specified interface。

1.125.2 Configure specific neighbors to send updates

Specify neighbors and send updates to specific neighbors.

Mode: Rip configuration mode

Command: neighbor < neighbor address > < ifname >

Configure IPv6 addresses for specific neighbors

Command: neighbor < neighbor address > < ifname >

Cancel specific neighbor configuration

Parameter: neighbor address is the IPv6 address of a specific neighbor

1.125.3 Configure the working state of the interface

RIPng protocol runs in some networks. It may only need RIPng interface routing and does not want to broadcast RIPng routing on this interface. Use the passive interface command to only know the route of the interface and block the broadcast of the interface.

Mode: RIPng configuration mode

Command: passive interface < if name >

Configure the interface to be passive

Command: no passive interface < if name >

Cancel interface passive state

Parameter: if name is the agreed three-tier interface name (for example: vlan1, vlan2...)

1.125.4 Configure default routing weights

When introducing an external route, you need to specify a route weight; When the routing weight is not specified, this default routing weight is used.

Mode: RIPng configuration mode

Command: default metric < metric >

Set the default route weight when introducing external routes

Command: no default metric [Metric]

When the external route is restored, the default route weight is 1

Parameter: metric value is between 1 and 16, greater than 1 and less than 16.

Default: the metric value is 1. Use the no default metric command to restore to the default value。

1.125.5 Configure timer

RIPng protocol has three timers. One is that the complete routing table broadcasts to all RIPng interfaces every 30 seconds. The other is that each route in RIPng routing table is marked with metric of 16 if it does not receive update in 180 seconds. The third is that each route in RIPng routing table is deleted from the routing table if it is marked with metric of 16 and not effectively updated in 120 seconds.

Mode: RIPng configuration mode

Command: timers basic < update > < timeout > < garbage >

Set three timer values

Command: no timers basic

The recovery timer is the default

Parameters: the first parameter update is the timer for regularly updating the entire RIPng routing table, the second parameter timeout is the timer for each route timeout without updating, and the third parameter garbage is the timer to be deleted after each route is marked as invalid; The value range of the three timers is 5 ~ (231-1).

Default: update every 30 seconds; When timeout is 180 seconds, it is marked as invalid; Garbage is deleted in 120 second。

1.125.6 Introducing external routing

RIPng allows users to introduce the routing information of other protocols into the routing table of rip. The routing protocols (types) that RIPng can introduce include connected, static, OSPF, IS-IS and BGP.

Mode: RIPng configuration mode

Command: redistribute {kernel | connected | static | ospf6 | Isis | BGP} [Metric < metric > | route map < route map name >]

Introducing other protocol routes

Command: no redistribute {kernel | connected | static | ospf6 | Isis | BGP} [Metric < metric > | route map < route map name >] Cancel incoming route

Parameter: the first parameter is the name of the imported other protocols, including direct connection, static, OSPF, is is and BGP; The second parameter is the weight set during import, with a value between 1 and 16; The third parameter is the name of the referenced route map. Route map is configured in the global configuration mode. Please refer to the command manual.

Default: RIPng protocol does not introduce any external protocols

1.125.7 Configure routing filtering

RIPng provides the function of route filtering. It filters the received routes and published routes and configures policy rules through the specified access control list and address prefix list.

Mode: RIPng configuration mode

Command: distribute list < ACL name > {in | out} [if name]

Use access list to filter the input and output of the interface

Command: no distribute list < ACL name > {in | out} [if name]

Cancel access list filtering

Parameter: ACL name indicates the name of the referenced access list; If name indicates the RIPng interface applied to; In and out indicate whether the application is in the direction of receiving routes or publishing routes.

Command: distribute list prefix < pre name > {in | out} [if name]

Filter using prefix list

Command: no distribute list prefix < pre name > {in | out} [if name]

Cancel using prefix list filtering

Parameter: pre name indicates the name of the referenced prefix list; If name indicates the RIPng interface applied to; In and out indicate whether the application is in the direction of receiving routes or publishing routes.

Default: RIPng protocol does not filter any received and sent routes

Access list and prefix list are configured in global configuration mode. Please refer to the command manual。

1.125.8 Configure additional routing weight

The additional routing weight is an offset value added to the routing weight of RIPng protocol during input and output. It does not directly change the weight of the route in the routing table, but adds an offset when the interface receives and sends the route.

Mode: RIPng configuration mode

Command: offset list < ACL name > {in | out} < offset > [if name]

Use access list to add an offset to the weight of interface input-output route

Command: no offset list < ACL name > {in | out} < offset > [if name]

Cancel the offset of the weight of the input-output route

Parameter: ACL name indicates the access list name of the reference; In and out indicate whether the application is in the input or output direction; Offset represents the value of the offset, which is between 0 and 16; If name indicates the RIPng interface applied to.

Default: when receiving a message, the additional weight of each route is 1, and when sending a message, the additional weight of each route is 0。

1.125.9 Configure horizontal segmentation

Horizontal segmentation means that the route received from this interface is not sent from this interface. Horizontal segmentation with toxic inversion means that the route received from this interface is still sent from this interface, but its metric value is marked as

16. Horizontal segmentation can avoid loops to a certain extent. The horizontal segmentation with toxic inversion is more efficient than ordinary horizontal segmentation, and direct labeling is not reachable. However, in nBMA network, it is necessary to prohibit horizontal segmentation to obtain the correct route.

Mode: interface configuration mode

Command: IPv6 rip split horizon [poisoned]

Start the horizontal division function of the interface or with toxic inversion

Command: no IPv6 rip split horizon

The horizontal division function of the interface is prohibited

Parameters: no poisoned parameter means to start the normal horizontal segmentation function, and with poisoned parameter means to start the horizontal segmentation function with toxic inversion.

Default: horizontal segmentation with toxic inversion

1.125.10 Configure interface weights

Mode: interface configuration mode

Command: IPv6 rip metric offset < metric >

Configure interface weight

Command: no IPv6 rip metric offset < metric >

Restore the interface weight to the default value

Parameter: the metric value is between 1-16, indicating the weight to be added to the routing entry learned by the interface.

Default: 1

1.125.11 Display information

Mode: normal mode or privileged mod

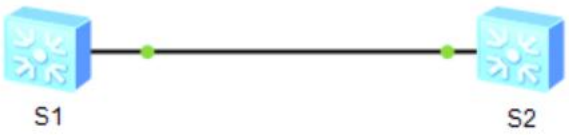
Command: Show IPv6 rip

Displays information about the current system RIPng

Command: Show IPv6 route rip

Displays the currently active RIPng routing information

1.126 RIPng configuration example



S1 switch is configured as follows

```
Switch(config)#
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 address 3ffe:506::1/64
Switch(config-vlan1)#exit
Switch(config)#router ipv6 rip
Switch(config-router)#exit
Switch(config)#int vlan1
Switch(config-vlan1)#
Switch(config-vlan1)#ipv6 router rip
Switch(config-vlan1)#
```

S2 switch is configured as follows

```
Switch(config)#
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 address 3ffe:506::2/64
Switch(config-vlan1)#exit
Switch(config)#router ipv6 rip
Switch(config-router)#exit
Switch(config)#int vlan1
Switch(config-vlan1)#
Switch(config-vlan1)#ipv6 router rip
Switch(config-vlan1)#
```

Configure OSPF

This chapter mainly includes the following contents：

- OSPF introduction
- OSPF configuration
- OSPF configuration example

1.127 OSPF introduction

OSPF (open shortest path first) is a protocol based on link state algorithm. It can support large-scale networks and has fast convergence speed.

Routers running OSPF protocol maintain link state database (LSDB), which describes the topology of the whole autonomous system like a map. When the databases of all routers are synchronized, each router calculates the shortest route to other destination nodes in the autonomous system from its own perspective and maintains it in its own routing table. When the topology in the network changes, the router only needs to encapsulate the changed link state in the link state update (LSU) message and broadcast it. All routers will synchronize the local database again and recalculate the route. Each router publishes the link state broadcast (LSA) it sees and gathers it to form the topology description LSDB of the whole network. After transforming it into a weighted directed graph, it can use the SPF algorithm to calculate the routing table.

In the broadcast network, each router needs to broadcast its own status information to other routers, and multiple pairwise adjacency relationships will be established, which will bring a large number of unnecessary message transmission. To this end, OSPF has agreed on a designated router (DR) and a backup designated router (BDR). The router sends the link information to Dr, which collects and arranges it, and then sends it to all routers. It effectively reduces the number of adjacency between routers in broadcast network.

OSPF supports five protocol messages:

Hello message is periodically broadcast to neighbors to discover and maintain neighbors and conduct Dr election. It contains some interface attribute values. Some parameters in Hello message must be consistent before establishing neighbors.

DD message (database description) uses DD message to describe its own LSDB during synchronization, including the head of each LSA. Through LSA head, one LSA can be uniquely determined, and the peer router can judge whether it has this LSA; If not,

request a complete LSA again.

LSR message (link state request) after two routers exchange DD messages, they will know which LSAS are missing locally in the opposite router. At this time, it is necessary to send LSR message to request a complete LSA. You only need LSA head when requesting.

LSU message (link state update) is a collection of multiple LSAS.

Lsack message (link state acknowledgement) is to confirm the received LSU message to ensure reliable transmission of link information. Confirm with LSA head.

Router ID concept: the unique identification of the router in the autonomous system.

Area: if OSPF operates in a large network, due to the large increase in the number of routers, it will lead to a very large LSDB, increase the synchronization time and routing calculation time, and occupy a lot of storage space and CPU resources. And the larger the network, the more frequent the topology changes, so that the network is often in change. The router needs to spend a lot of time transmitting messages and calculating routes, which unnecessarily occupies the network bandwidth. Therefore, OSPF introduces the concept of region to divide routers into different regions. LSDB only synchronizes and calculates routes in the region. The routing interaction between regions is completed by the boundary router (ABR). In this way, the number of routers in the region will be limited, and the LSDB will be limited to a small capacity. The time for calculating the route will be greatly reduced, and the convergence will be fast when the topology changes. The region concept effectively groups a large-scale network and undertakes the routing function of a small range within each region. Routes between regions interact on the backbone region (the region with region ID 0). Therefore, all non backbone areas must be connected to the backbone area, that is, ABR has at least one interface to connect to the backbone area. If a non backbone area cannot be connected with the backbone area in the network planning, a virtual link must be configured to establish a logical path, that is, an ABR in the backbone area and an ABR in the non backbone area establish a point-to-point link through a transmission area. Then the inter domain routing information on the backbone area will also be published to the non backbone area through the virtual link。

1.128 OSPF Configuration

After the OSPF protocol is started, enter the OSPF configuration mode to set the corresponding properties and functions. OSPF configuration commands are mostly in OSPF configuration mode and interface configuration mode.

OSPF configuration includes:

Start OSPF and enter OSPF mode

Enable interface

Specify host

Configure router ID

Configure adjacency points

Prohibit the interface from sending messages

Configure SPF timer

Configure management distance

Introducing external routing

Configure the network type of the interface

Configure Hello message sending interval

Configure neighbor router expiration time

Configure retransmission interval

Configure interface delay

Configure the priority of interface in Dr election

Configure the cost of sending messages on the interface

Whether to fill in MTU value for DD message sent by configuration interface

Configure interface message authentication

Configure regional virtual link

Configure regional routing aggregation

Configure regional message authentication

Stub area configuration

Configure NSSA area

Configure external route aggregation

Configure default weights for external routes

1.128.1 Start OSPF and enter OSPF mode

OSPF protocol can run multiple copies, which are identified by process ID; When starting OSPF protocol, it is necessary to specify which process number is started; If there are no parameters, the process number is 0.

Mode: global configuration mode

Command: router OSPF [process ID]

Start the OSPF process with process ID and enter its mode

Command: no router OSPF [process ID]

Close OSPF process with process ID

Parameter: the value of process ID is between 1 and 216-1, indicating the OSPF process number started; If there is no parameter process ID, OSPF with process number 0 will be started.

Default: do not run OSPF protocol

1.128.2 Enable interface

The value of OSPF protocol is that it introduces the idea of layering to divide a complete autonomous system into different regions in order to establish a conceptual hierarchical network model. The area is logical, and the routers in the autonomous system are grouped artificially. When different interfaces of the router belong to different regions, that is, cross regions, it is called boundary router ABR. Each network segment that starts OSPF protocol can only belong to a specific area, that is, each interface running OSPF protocol on the router must belong to the specified area. The area is identified by area ID, and the area with area No. 0 is the backbone area. The routing information between different regions is transmitted through the border router. Different from Rip protocol, when running OSPF protocol on the interface, its region must be specified。

Mode: OSPF configuration mode

Command: network < network address > area < area ID >

The OSPF protocol runs on the specified interface in the specified area

Command: no network < network_ address> area <area-id>

Turn off OSPF on a specific interface in a specific area

Parameter: network address has two forms: a.b.c.d/m and a.b.c.d. the former specifies the network IP and mask length, and the latter specifies the network IP and mask. Area ID also has two forms: a.b.c.d and integer. The former uses dotted decimal format, and the latter takes values between 0 ~ (232-1).

Default: the interface is not enabled after the OSPF protocol is started

1.128.3 Specify host

Mode: OSPF configuration mode

Command: host < IP address > area < area ID > [cost < cost >]

Configure host routing

Command: no host < IP address > area < area ID > [cost < cost >] Cancel host routing

Parameter: IP address uses a.b.c.d format to represent a designated host in a certain area. It is a stub type in the link representation of the router. Area ID is the same as described in the network command. Cost means to specify the cost of the link. It is an optional parameter.

Default: cost. If it is not configured, it defaults to 0

1.128.4 Configure router ID

The router ID is a 32-bit unsigned integer, which is the unique identification of a router in the autonomous system. The router ID can be configured manually. During configuration, it is necessary to ensure that the IDs of any two routers in the autonomous system are different. If not configured, the router uses the IP address of the loopback interface; If loopback has no IP address, select the highest address from the IP addresses of the current interface as the ID. In order to ensure the stable operation of OSPF, the router ID should be divided and configured manually during network planning.

Mode: OSPF configuration mode

Command: OSPF router ID < router ID >

Configure router ID

Command: no OSPF router ID

Cancel router ID

ID: router ID >

Command: no router ID [router ID]

Parameter: router ID uses a.b.c.d format

Default: after the OSPF protocol is started, the router ID will be automatically generated according to the rules. The rules are as follows: first, select the router ID configured by the command; If not, select the IP address of loopback; If not, select the highest IP address of the current interface; 0.0.0.0 if none.

The functions of the two groups of commands are the same。

1.128.5 Configure adjacency points

The OSPF protocol interaction protocol message uses the multicast address 224.0.0.5 or 224.0.0.6 through multicast. When OSPF protocol runs on a link that does not support broadcasting, such as nBMA, some configurations must be made to use unicast to interact with protocol messages. At this time, you can manually specify the IP address and corresponding attribute value of the opposite end.

Mode: OSPF configuration mode

Command: neighbor < IP address > [priority < prio > | poll interval < deadtime > | cost < cost >]

Specify the pair of adjacent pins and set the properties

Command: no neighbor < IP address > [priority < prio > | poll interval < deadtime > | cost < cost >] cancel the adjacent contact and attribute setting of the opposite end

Parameter: IP address of the opposite end, in a.b.c.d format; Prio is the peer priority, with a value between 0 and 255; Deadtime is the timing of the end-to-end down. If the

timing is terminated, no Hello message will be sent to the end-to-end. The value is between 1 ~ 216-1; Cost is the cost of the link to the opposite end, which is between 1 ~ 216-1.

Default: priority is 1 (0 will not participate in Dr election); Poll interval is 120 seconds; Cost is 10。

1.128.6 Prohibit the interface from sending messages

When in a simple network, the interface of OSPF protocol only represents a network segment between two devices for data transmission, set the interface to passive state and block the Hello message broadcast on its link, which does not affect the knowledge of the interface route.

Mode: OSPF configuration mode

Command: passive interface < if name >

Configure the interface to be passive

Command: no passive interface < if name >

Cancel interface passive state

Parameter: if name is the name of the three-tier interface (for example: vlan1, vlan2...)

Default: after the OSPF protocol is started, the enabled interfaces are not in passive state

Specify the interface running OSPF protocol as passive state, and the direct route of the interface can still be published, but the OSPF message on the interface will be blocked, and the interface cannot establish neighbor relationship. In some networking cases, it can effectively save network resources。

1.128.7 Configure SPF calculation time

When the link state database LSDB of OSPF changes, the shortest path needs to be recalculated. If the shortest path is calculated immediately for each change, it will occupy a lot of resources and affect the efficiency of the router. By configuring the two values of delay and hold to adjust the time interval of SPF calculation, we can restrain the too frequent SPF calculation caused by the frequent changes of the network, so as to avoid occupying a lot of system resources in one time and affecting the operation efficiency of the router.

SPF calculation has a timer, which starts the next calculation according to the inhibition time each time. When SPF calculation needs to be started when the timer terminates, recalculate the inhibition time from the last SPF calculation to this time. If the

configured inhibition time has been exceeded, use the configured delay time to start the timer. If the configured inhibit time has not been exceeded, the configured inhibit time is used to calculate the required delay time. If the delay time is less than the configured delay time, use the configured delay time; otherwise, directly use the calculated delay time to start SPF calculation

Mode: OSPF configuration mode

Command: timers SPF < delay > < hold >

Configure the delay and hold values of SPF calculation interval

Command: no timers SPF

Restore to default

Parameter: delay indicates the delay time required to calculate SPF; Hold indicates the time to suppress between two SPF calculations.

Default: delay is 5S; Hold is 10 seconds

1.128.8 Configure management distance

Multiple routing protocols can be run on the router at the same time. How to choose from the routing information learned by multiple routing protocols requires the use of management distance. When different protocols find the same route, the one with small management distance is preferred.

Mode: OSPF configuration mode

Command: distance < distance >

Configure management distance

Command: no distance < distance >

The recovery management distance is the default value

Command: distance OSPF {intra area < distance > | inter area < distance > | external < distance >}

Configure different types of management distances

Command: no distance OSPF

Restore the three types of management distance to the default value

Parameter: distance is between 1 and 255; Intra area refers to the management distance of routes in the domain; Inter area refers to the management distance of inter domain routing; External indicates the management distance of the external route.

Default: the management distance of OSPF protocol is 110; The management distance of intra domain route, inter domain route and external route is 0.

1.128.9 Introducing external routing

Multiple dynamic routing protocols can be run on the router, and routing information can be shared between different routing protocols. OSPF regards the route learned by other routing protocols as the route outside the autonomous system, which is introduced by the autonomous system boundary router ASBR. When introducing an external route, you can specify attributes such as weight and weight type.

OSPF is divided into four types: intra domain routing and intra domain routing; The third is the external route of type-1, and the fourth is the external route of type-2. These two types of routes describe the route to the destination outside the autonomous system. The route of type-1 is from other IGPS. OSPF believes that it has high reliability and is comparable with the route weight in the autonomous system. Therefore, the cost of this kind of external route is the sum of the cost from the router itself to ASBR and the cost from ASBR to the destination. The route of type-2 is from other eGPS. OSPF believes that its reliability is not very high, and its cost is far greater than that in the autonomous system, so it is not comparable. Therefore, the cost of this kind of external route only uses the cost from ASBR to the destination, and ignores the cost from the router itself to ASBR.

Mode: OSPF configuration mode

Command: redistribute {kernel | connected | static | rip | Isis | BGP} [Metric < metric > | metric type < type > | route map < route map name > | tag < tag >]

Command: no redistribute {kernel | connected | static | rip | Isis | BGP} [Metric < metric > | metric type < type > | route map < route map name > | tag < tag >]

Parameter: the first required parameter is the type of external route that can be introduced, including direct connection, static, rip, IS-IS and BGP; The second parameter is the weight value set when introducing external route, which is between 0 ~ 224-1; The third parameter is the introduction of two types of external routes, which are divided into type-1 and type-2. Type-1 is IGP route and type-2 is EGP route; The third parameter is the name of the referenced route map. The route map is configured in the global configuration mode. Please refer to the command manual; The fourth parameter is tag, which is between 0 and 232-1. It is an external routing attribute.

Default: no external routing protocols are introduced

1.128.10 Configure the network type of the interface

OSPF protocol takes its own router as the perspective. Each router describes its adjacent network topology and passes it to other routers. OSPF divides the network types of interface links into four types according to the link layer protocol types: one is the broadcast type (the link layer protocols are Ethernet, FDDI, etc.); The second is nBMA non

broadcast multiple access type (link layer protocols are fr, ATM, HDLC, X.25, etc.); The third is the point to multipoint type. No link layer protocol will be regarded as the point to multipoint type by default. The point to multipoint type must be forcibly configured by other network types. The most common approach is to change the non fully connected nBMA to point to multipoint network. The fourth is the point-to-point type (the link layer protocols are PPP, LAPB and POS).

On broadcast networks without multiple access capability, the interface can be configured as nBMA type. When not all routers are directly accessible in nBMA network, the interface can be configured as point to multipoint type.

The nBMA network agreed in OSPF protocol is fully connected, non broadcast and multi-point reachable. Point to multipoint networks are not necessarily fully connected. NBMA needs to select Dr, and there is no DR in point to multipoint network. NBMA network multicast message through designated neighbor unicast message and point-to-multipoint network multicast message.

Mode: interface configuration mode

Command: ip ospf network < type >

Configure the network type of the interface link

Command: no ip ospf network

The network type of the recovery interface link is the default value

Parameter: Type: you can select broadcast, non broadcast, point to point, point to multipoint [non broadcast]; The first type is broadcast network, the second type is non broadcast network, i.e. nBMA, the third type is point-to-point network, and the fourth type is point-to-multipoint network; Point to multipoint networks are divided into broadcast and non broadcast networks. Non broadcast neighbors cannot be found automatically and must be specified.

Default: broadcast network

1.128.11 Configure Hello message sending interval

Hello message is used to send to neighbor router periodically, find and maintain neighbor relationship, and elect DR and BDR. The interval of Hello message can be configured manually, but attention should be paid to keeping the interval of Hello timer between neighbors in the network consistent. The value of Hello timer is inversely proportional to the convergence speed of router and network load.

Mode: interface configuration mode

Command: ip ospf Hello interval < seconds >

Configure the interval of Hello timer

Command: no ip ospf Hello interval

Restore the Hello timer interval to the default value

Parameter: the value of seconds is between 1 and 216-1, indicating the time interval between two Hello message sending.

Default: on broadcast network and point-to-point network, the Hello interval is 10 seconds; More than 30 seconds between nBMA and hello network.

1.128.12 Configure neighbor router expiration time

Mode: interface configuration mod

Command: ip ospf dead interval < seconds >

Configure neighbor expiration time

Command: no ip ospf dead interval

Recovery neighbor failure time is the default value

Parameter: the value of seconds is between 1 and 216-1, which means that the neighbor is considered invalid if no Hello message is received after seconds; Every time a hello message is received, the neighbor's dead timer will be updated.

Default: the failure time of neighbors on broadcast network and point-to-point network is 40 seconds; On nBMA network and point to multipoint network, the neighbor failure time is 120 seconds; When the network type is modified, the Hello interval and dead interval will use the default values。

1.128.13 Configure retransmission time

OSPF is a reliable link state protocol, which is reflected in the fact that the LSU messages it interacts with need the response LSU ack from the opposite end. When receiving the confirmation message, the party considers that the link state update is received. If no acknowledgement message is received within the retransmission interval, the LSA will be retransmitted to the neighbor. The retransmission interval can be configured manually. It needs to be longer than the time for a message to be transmitted back and forth between two routers. If it is set too small, it will cause unnecessary retransmission.

Mode: interface configuration mode

Command: ip ospf retransmit interval < seconds >

Configure the retransmission interval of the interface

Command: no ip ospf retransmit interval

The recovery retransmission interval is the default value

Parameter: the value of seconds is between 1 and 216-1, which indicates the interval of retransmission when the opposite end does not receive LSA.

Default: retransmission interval 5S

1.128.14 Configure interface delay

In the link state update message LSU, each link state broadcast LSA has a time domain. Before transmission, it is necessary to increase the transmission delay of the transmitting interface. This parameter mainly considers the time required for the interface to send messages, especially on low-speed networks.

Mode: interface configuration mode

Command: ip ospf transmit delay < seconds >

Set the transmission delay of the interfac

Command: no ip ospf transmit delay

The transmission delay of the recovery interface is the default value

Parameter: the value of seconds is between 1 and 216-1, indicating that the delay value needs to be increased in the age domain of the LSA sent by the interface.

Default: the transmission delay of the interface is 1s

1.128.15 Configure the priority of interface in Dr election

In order to avoid repeated point-to-point transmission of link information in the broadcast network, it is necessary to elect the designated router DR and BDR to be responsible for broadcasting the link information in the network segment. The priority of the interface indicates its qualification in the election of Dr. in case of election conflict, the one with higher priority shall be considered first. If the priority is 0, they will not participate in the election. If the priority is greater than 0, they are candidates. Each router contains its own priority information and its own DR in its own Hello message, broadcasts in the broadcast network, and finally selects the one with higher priority to become Dr. If the priorities are equal, the higher the router ID will prevail.

When Dr fails, the router in the network needs to go through a process of re electing Dr, which takes a time, and during this time, it will cause routing calculation errors. The concept of BDR is to make a smooth transition to the new Dr. BDR is the backup of Dr. it is selected at the same time in the Dr election. It also establishes an adjacency relationship with other routers in the network. Only the information collection and publishing node in the network is in Dr rather than BDR. BDR only maintains the synchronization of adjacency. When the Dr fails, the BDR will immediately become a DR and be responsible

for collecting information in the network segment. At this time, a new process will be started to elect the BDR, but the election of the BDR will not affect the calculation of the route.

Mode: interface configuration mode

Command: ip ospf priority < prio >

Configure the priority of interface in Dr election

Command: no ip ospf priority

Restore interface priority to default

Parameter: the value of prio is 0 ~ 255, which indicates the priority in Dr selection. When it is 0, it indicates that it does not participate in the election.

Default: priority is 1

1.128.16 Configure the cost of sending messages on the interface

In the network, the traffic is controlled by configuring different links at different costs. The cost of the interface represents the cost of sending messages from the interface. If it is not configured manually, OSPF will automatically calculate the interface cost according to the interface baud rate.

Mode: interface configuration mode

Command: ip ospf cost < cost >

Command: no ip ospf cost

Parameter: the value of cost is between 1 and 216-1, indicating the proxy value of the message sent on the interface.

Default: interface cost 10

1.128.17 Whether to fill in MTU domain for DD message sent by configuration interface

Mode: interface configuration mode

Command: ip ospf MTU ignore

Set not to check MTU value in DD message

Command: no ip ospf MTU ignore

Cancel not checking MTU value in DD message

Default: check MTU value in DD message

1.128.18 Configure interface message authentication

The message authentication of OSPF protocol on the interface supports plaintext mode and MD5 mode.

Mode: interface configuration mode

Command: ip ospf authentication < mode >

Configure authentication mode

Command: no ip ospf authentication

Cancel authentication

Parameter: no parameter indicates plaintext authentication; Message digest indicates MD5 authentication; Null indicates no authentication

Command: ip ospf authentication key < password

Configure plaintext authentication password string

Command: no ip ospf authentication key

Cancel plaintext authentication password string

Parameter: password indicates the password string of plaintext authentication

Command: ip ospf message digest key < key ID > MD5 < password >

Configure MD5 authentication password

Command: no ip ospf message digest key < key ID >

Cancel MD5 authentication password

Parameter: the value of key ID is between 1 and 255, which is used to sort in the key chain; Password indicates the password string.

Default: no authentication is configured

1.128.19 Configure regional virtual lin

OSPF protocol adopts the layered idea to divide the routers in the autonomous system into different groups. These groups are called regions. All regions are not equal and parallel, but have hierarchical relations. Among them, 0.0.0.0 region is the most special, which is the backbone region. Other non backbone regions must exchange inter domain routes through the backbone region. Therefore, all non backbone areas must be connected with the backbone area, that is, at least one interface on the ABR is in area 0. If some areas cannot guarantee the physical path with the backbone area due to the limitation of network topology, virtual links need to be configured to ensure the logical path. Both ends of the virtual link are ABR, and the middle passes through a non backbone area, which is called the transmission area. When configuring the virtual link, it is necessary to specify the ID of the transmission area and the ID of the opposite ABR, and it must be configured on the ABR at both ends before it can take effect.

When the route of the transmission area is calculated and the virtual link is activated, it is logically equivalent to forming a point-to-point connection between two endpoints. Therefore, the parameters of the interface can be configured on its physical interface and the authentication function can be started.

The unicast message is transmitted between ABRs. The router forwarding the unicast message in the transmission area will forward it as an ordinary IP message. Therefore, it can only be understood that a logical link is provided in the transmission area, and protocol messages can be exchanged between two ABRs.

Mode: OSPF configuration mode

Command: Area < area ID > virtual link < router ID >

Configure the transmission area and peer ID of the virtual link

[authentication <mode> |

Configure the authentication mode of virtual link

authentication-key <password> |

Configure virtual link plaintext authentication password

message-digest-key <key-id> md5 <password> |

Configure virtual link MD5 authentication password

hello-interval <seconds> |

Configure the Hello interval of virtual link

dead-interval <seconds> |

Configure virtual link neighbor failure time

retransmit-interval <seconds> |

Configure virtual link retransmission interval

transmit-delay <seconds> |

Configure virtual link interface delay

Command: no area < area ID > virtual link < router ID >

[authentication <mode> |

authentication-key <password> |

message-digest-key <key-id> md5 <password> |

hello-interval <seconds> |

dead-interval <seconds> |

retransmit-interval <seconds> |

transmit-delay <seconds>]

Cancel virtual link setting

Parameter: area ID refers to the ID of the transmission area. It can use dotted decimal format a.b.c.d or integer format. The value is between 0 ~ 232-1. Router ID refers to the ID of the peer router of the virtual link, in a.b.c.d format. Authentication and sending

interface properties are optional. Please refer to relevant command descriptions.

Default: virtual link is not configured

1.128.20 Configure regional routing aggregation

Mode: OSPF configuration mode

Command: Area < area ID > range < IP prefix > [advertise | not advertise]

Configure aggregation scope

Command: no area < area ID > range < IP prefix > [advertise | not advertise]

Cancel aggregation

Parameter: area ID refers to the area ID, which specifies the aggregation of routes in the area. You can use dotted decimal format a.b.c.d or integer format, and the value is between 0 ~ 232-1. IP prefix uses the prefix format a.b.c.d/m to represent the aggregation range. The optional parameters advertise and not advertise indicate whether to broadcast the aggregation range, that is, IP prefix. The original network routes will be broadcast。

1.128.21 Configure regional message authentication

The authentication type of all routers in an area shall be consistent. The authentication password strings of all routers in a network segment shall be consistent. The configuration area authentication only starts the authentication function (plaintext or MD5), and the password uses the corresponding configuration value of the interface. Refer to interface message authentication configuration.

Mode: OSPF configuration mode

Command: Area < area ID > authentication [message digest]

Configure regional authentication mode

Command: no area < area ID > authentication

Cancel regional certification

Parameter: area ID indicates the area ID and specifies the area to be authenticated; You can use dotted decimal format a.b.c.d or integer format, with values between 0 ~ 232-1. Optional parameters: none indicates plaintext authentication, and message digest indicates MD5 authentication.

Default: do not start zone authentication

1.128.22 Stub area configuration

Mode: OSPF configuration mode

Command: Area < area ID > stub [no-summary]

Configure the router in the stub area

Command: no area < area ID > stub [no summary]

Cancel the properties of the router in the stub area

Command: Area < area ID > default cost < cost >

Configure the default cost of ABR broadcast routing connected to the stub area

Command: no area < area ID > default cost

Restore default cost to default value

Parameter: area ID refers to area ID, indicating which area attribute is stub; You can use dotted decimal format a.b.c.d or integer format, with values between 0 ~ 232-1. No summary means that inter domain routes are not injected into the stub area.

The first group of commands is to configure the router located in the stub area, and the second group of commands is to configure the ABR with the interface connected to the stub area.

Default: the stub area is not configured

1.128.23 Configure NSSA area

Mode: OSPF configuration mode

Command: Area < area ID > NSSA [options]

Configure NSSA properties

Command: no area < area ID > NSSA [options]

Cancel NSSA zone properties

Parameters: area ID refers to area ID. see the command manual for options.

Default: the NSSA area is not configured

1.128.24 Configure external route aggregation

The routes introduced from other protocols are broadcast one by one in the LSU of type-5. Use the aggregation command to specify a prefix range. The routes covered in this range are suppressed and only the aggregated route is broadcast. When the number of external routes is huge, it can effectively reduce the scale of LSDB.

Mode: OSPF configuration mode

Command: summary address < IP prefix > [not advertise | tag < tag >]

Configure aggregation scope and properties

Command: no summary address < IP prefix > [not advertise | tag < tag >]

Disaggregate external routes

Parameter: IP prefix uses the address prefix format a.b.c.d/m to represent the routing

range to be aggregated; Not advertised means that the aggregated route will not be broadcast; Tag is the set tag value. The value is between 0 and 232-1. The default value is 0.

Default: do not aggregate externally introduced routes

1.128.25 Configure default weights for external routes

When introducing an external route, if the redistribute command does not specify a metric value, the default weight is used.

Mode: OSPF configuration mode

Command: default metric < metric >

Configure the default weight when introducing external routes

Command: no default metric [Metric]

The default weight is the default value when restoring the introduction of external routes

Parameter: metric value between 0 ~ 224-1

Default: the default weight is 1

1.128.26 display information

Mode: normal mode or privileged mode

Command: show ip protocols

Command: show ip protocols OSPF

Display OSPF protocol information

Command: show ip ospf [process ID]

Display OSPF process information

Parameter: instance ID is the process number,

The value is between 0 - (216-1).

Command: show ip ospf border routes

Display ABR information

Command: show ip ospf database < type >

Display LSDB information

Parameter: type refers to all types of LSA and summary information. See the command manual for details.

Command: show ip ospf interface [if name]

Display OSPF interface information

Parameter: if name is the agreed three-tier interface name

Command: show ip ospf route [count]

Display OSPF routing table

Parameter: count indicates the total number of entries in the display routing table

Command: show ip ospf virtual links

Display OSPF virtual connection information

Command: show ip ospf neighbor [options]

Display OSPF neighbor information

Parameter: options. See the command manual for details

Mode: privileged mode

Command: show running config

Displays the current configuration of the switch, including OSPF configuration.

Command: show running config OSPF

Displays the current configuration of OSPF protocol。

1.129 OSPF Configuration example

(1) Configuration

The three switches are connected in pairs, with 6 network segments respectively. OSPF protocol is enabled to realize the interworking between the three PCs. The interface is required to be in the same area area 0。

On the switch 1：

Switch#configure terminal

Switch(config)#router ospf 100

Switch(config-ospf-100)#network 10.1.1.0/24 area 0

Switch(config-ospf-100)#network 10.1.2.0/24 area 0

Switch(config-ospf-100)#network 192.168.1.0/24 area 0

On the switch 2：

Switch#configure terminal

Switch(config)#router ospf 100

Switch(config-ospf-100)#network 10.1.2.0/24 area 0

Switch(config-ospf-100)#network 10.1.3.0/24 area 0

Switch(config-ospf-100)#network 192.168.2.0/24 area 0

On the switch 3：

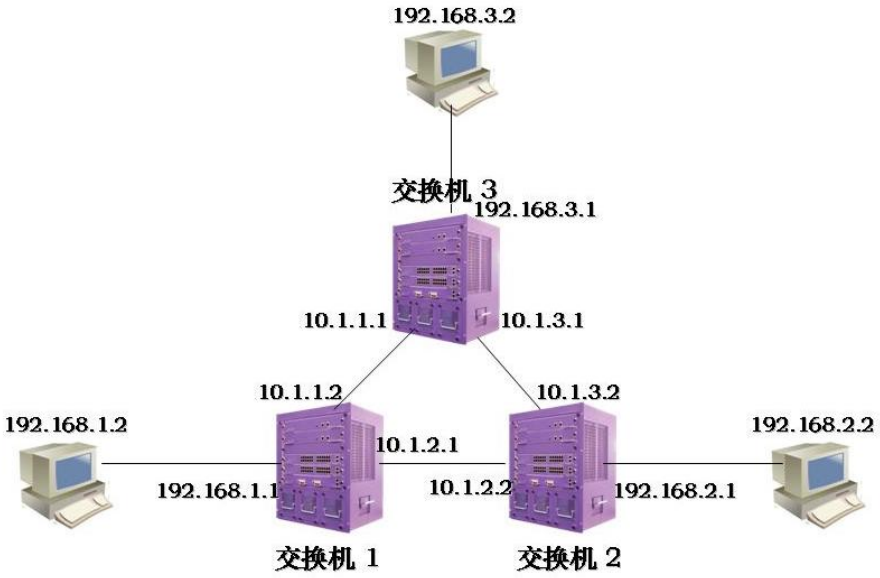
Switch#configure terminal

Switch(config)#router ospf 100

Switch(config-ospf-100)#network 10.1.1.0/24 area 0

Switch(config-ospf-100)#network 10.1.3.0/24 area 0

Switch(config-ospf-100)#network 192.168.3.0/24 area 0



(2) verification

show ip ospf database

show ip ospf interface

show ip ospf neighbor

show ip route ospf

show ip ospf route

Configure OSPFv3

This chapter mainly includes the following contents：

- OSPFv3 introduction
- OSPFv3 configuration
- OSPFv3 confiuration example

1.130 OSPFv3 introduction

OSPF (open shortest path first) is an internal gateway protocol based on link state developed by IETF

Interior gateway protocol.

At present, OSPF version 2 is used for IPv4 protocol and OSPF version 3 is used for IPv6 protocol.

- OSPFv3 is short for OSPF version 3.
- OSPFv3 is an OSPF routing protocol running on IPv6 (rfc5340, the same as rfc2740).
- OSPFv3 is modified on the basis of ospfv2 and is an independent routing protocol。

The main purpose of OSPFv3 is to develop a routing protocol independent of any specific network layer. To achieve this,

The internal router information of OSPFv3 has been redesigned.

OSPFv3 differs from ospfv2 in that：

- **OSPFv3 does not insert IP based data into the header of the message at the beginning of the packet and link state announcement (LSA) Data.**
- **OSPFv3 uses information independent of network protocol to perform key tasks that required IP message header data in the past Services, such as identifying the LSA that publishes routing data。**

Basic principle of OSPFv3

OSPFv3 is an OSPF routing protocol (rfc2740) running on IPv6. It is added on the basis of ospfv2

Strong, is an independent routing protocol。

- **working principle and of OSPFv3 in Hello message, state machine, LSDB, flooding mechanism, routing calculation, etc Ospfv2 is consistent.**
- **OSPFv3 protocol divides the autonomous system into one or more regions in the logical sense through LSA (link) Publish routes in the form of state advertisement.**
- **OSPFv3 relies on the interaction of OSPFv3 messages between devices in OSPFv3 area to achieve the unification of routing information.**
- **OSPFv3 message is encapsulated in IPv6 message and can be sent in the form of unicast and multicast。**

OSPFv3 Message type

Message type	**Message function**
Hello Message	**Send periodically to discover and maintain OSPFv3 neighbor relationship.**
DD Message（Database Description packet）	**Describes the summary information of the local LSDB, which is used for database synchronization between two devices.**
LSR Message（Link State Request packet）	**Used to request the required LSA from the other party.** **The device will send LSR message to OSPFv3 neighbors only after they successfully exchange DD message.**
LSU Message（Link State Update packet）	**Send the required LSA to the other party.**
LSAck Message（Link State Acknowledgment packet）	**Used to confirm the received LSA.**

LSA type

LSA **type**	LSA **function**
Router-LSA（Type1）	**The device will generate an LSA for the area where each OSPFv3 interface is running, which describes the link state and overhead of the device and propagates in the area to which it belongs.**
Network-LSA（Type2）	**Generated by Dr, it describes the link state of the**

	link and propagates in the area to which it belongs.
Inter-Area-Prefix-LSA（Type3）	**Generated by ABR, it describes the route of a network segment in the area and notifies other relevant areas.**
Inter-Area-Router-LSA（Type4）	**Generated by ABR, it describes the route to ASBR and notifies other relevant areas except the area where ASBR is located.**
AS-external-LSA（Type5）	**Generated by ASBR, it describes the route outside the as and notifies all areas (except stub area and NSSA area).**
NSSA LSA（Type7）	**enerated by ASBR, it describes the route to the outside of the as and propagates only in the NSSA area**
Link-LSA（Type8）	**Each device will generate a link LSA for each link, describe the link local address and IPv6 prefix address on this link, and provide the link options that will be set in the network LSA. It only propagates within this link.**
Intra-Area-Prefix-LSA（Type9）	**Each device and Dr will generate one or more such LSAS and propagate in its area** **● such LSA generated by the equipment, describing the IPv6 prefix address associated with the route LSA** **● such LSA generated by Dr, describing the IPv6 prefix address associated with the network LSA。**

1.131 OSPFv3 configuration

1.131.1 Start OSPFv3 and enter OSPFv3 configuration mode

OSPFv3 protocol can run multiple copies, which are identified by process ID; When starting OSPFv3 protocol, it is necessary to specify which process number is started; If there are no parameters, the process number is 0.

Mode: global configuration mode

Command: router IPv6 OSPF [process ID]

Start OSPFv3 process with process ID and enter its mode

Command: no IPv6 Router OSPF [process ID]

Close OSPFv3 process with process ID

Parameter: the value of process ID is between 1 and 216-1, indicating the OSPF process number started; If there is no parameter process ID, OSPFv3 with process number 0 will be started.

Default: OSPFv3 protocol is not running

1.131.2 Configure router ID

The router ID is a 32-bit unsigned integer, which is the unique identification of a router in the autonomous system. The router ID can be configured manually. During configuration, it is necessary to ensure that the IDs of any two routers in the autonomous system are different. If not configured, the router uses the IP address of the loopback interface; If loopback has no IP address, select the highest address from the IP addresses of the current interface as the ID. In order to ensure the stable operation of OSPFv3, the router ID should be divided and configured manually during network planning.

Mode: OSPFv3 configuration mode

Command: router ID < router ID >

Configure router ID

Command: no router ID

Cancel router ID

Command: router ID < router ID >

Command: no router ID [router ID]

Parameter: router ID uses a.b.c.d format

Default: after OSPFv3 protocol is started, the router ID will be automatically generated according to the rules. The rules are as follows: first, select the router ID configured by the command; If not, select the IP address of loopback; If not, select the highest IP address of the current interface; 0.0.0.0 if none.

The functions of the two groups of commands are the same.

1.131.3 Prohibit the interface from sending messages

When in a simple network, the interface of OSPFv3 protocol only represents a network segment between two devices for data transmission, set the interface to passive state and block the Hello message broadcast on its link, which does not affect the

knowledge of the interface route.

Mode: OSPFv3 configuration mode

Command: passive interface < if name >

Configure the interface to be passive

Command: no passive interface < if name >

Cancel interface passive state

Parameter: if name is the name of the three-tier interface (for example: vlan1, vlan2...)

Default: after OSPFv3 protocol is started, all enabled interfaces are not in passive state

Specify the interface running OSPFv3 protocol as passive state, and the direct route of the interface can still be published, but the OSPFv3 message on the interface will be blocked, and the interface cannot establish neighbor relationship. In some networking cases, it can effectively save network resources.

1.131.4 Configure SPF calculation time

When the link state database LSDB of OSPFv3 changes, the shortest path needs to be recalculated. If the shortest path is calculated immediately for each change, it will occupy a lot of resources and affect the efficiency of the router. By configuring the two values of delay and hold to adjust the time interval of SPF calculation, we can restrain the too frequent SPF calculation caused by the frequent changes of the network, so as to avoid occupying a lot of system resources in one time and affecting the operation efficiency of the router.

SPF calculation has a timer, which starts the next calculation according to the inhibition time each time. When SPF calculation needs to be started when the timer terminates, recalculate the inhibition time from the last SPF calculation to this time. If the configured inhibition time has been exceeded, use the configured delay time to start the timer. If the configured inhibit time has not been exceeded, the configured inhibit time is used to calculate the required delay time. If the delay time is less than the configured delay time, use the configured delay time; otherwise, directly use the calculated delay time to start SPF calculation.

Mode: OSPFv3 configuration mode

Command: timers SPF < delay > < hold >

Configure the delay and hold values of SPF calculation interval

Command: no timers SPF

Restore to default

Parameter: delay indicates the delay time required to calculate SPF; Hold indicates

the time to suppress between two SPF calculations.

Default: delay is 5S; Hold is 10 seconds

1.131.5 Configure management distance

Multiple routing protocols can be run on the router at the same time. How to choose from the routing information learned by multiple routing protocols requires the use of management distance. When different protocols find the same route, the one with small management distance is preferred.

Mode: OSPFv3 configuration mode

Command: distance < distance >

Configure management distance

Command: no distance < distance >

The recovery management distance is the default value

Command: distance OSPFv3 {intra area < distance > | inter area < distance > | external < distance >}

Configure different types of management distances

Command: no distance OSPFv3

Restore the three types of management distance to the default value

Parameter: distance is between 1 and 255; Intra area refers to the management distance of routes in the domain; Inter area refers to the management distance of inter domain routing; External indicates the management distance of the external route.

Default: the management distance of OSPFv3 protocol is 110; The management distance of intra domain route, inter domain route and external route is 0.

1.131.6 Introducing external routing

Multiple dynamic routing protocols can be run on the router, and routing information can be shared between different routing protocols. OSPFv3 regards the route learned by other routing protocols as the route outside the autonomous system, which is introduced by the autonomous system boundary router ASBR. When introducing an external route, you can specify attributes such as weight and weight type.

OSPFv3 has four types of routes. One is intra domain routing, and the other is inter domain routing. These two types of routes are in autonomous systems; The third is the external route of type-1, and the fourth is the external route of type-2. These two types of routes describe the route to the destination outside the autonomous system. The route of

type-1 is from other IGPS. OSPFv3 believes that it has high reliability and is comparable with the route weight in the autonomous system. Therefore, the cost of this kind of external route is the sum of the cost from the router itself to ASBR and the cost from ASBR to the destination. The route of type-2 is from other eGPS. OSPFv3 believes that its reliability is not very high, and its cost is far greater than that in the autonomous system, so it is not comparable. Therefore, the cost of this kind of external route only uses the cost from ASBR to the destination, and ignores the cost from the router itself to ASBR.

Mode: OSPFv3 configuration mode

Command: redistribute {kernel | connected | static | rip | Isis | BGP} [Metric < metric > | metric type < type > | route map < route map name > | tag < tag >]

Command: no redistribute {kernel | connected | static | rip | Isis | BGP} [Metric < metric > | metric type < type > | route map < route map name > | tag < tag >]

Parameter: the first required parameter is the type of external route that can be introduced, including direct connection, static, rip, IS-IS and BGP; The second parameter is the weight value set when introducing external route, which is between 0 ~ 224-1; The third parameter is the introduction of two types of external routes, which are divided into type-1 and type-2. Type-1 is IGP route and type-2 is EGP route; The third parameter is the name of the referenced route map. The route map is configured in the global configuration mode. Please refer to the command manual; The fourth parameter is tag, which is between 0 and 232-1. It is an external routing attribute.

1.131.7 Configure the network type of the interface

OSPFv3 protocol takes its own router as the perspective. Each router describes its adjacent network topology and passes it to other routers. OSPFv3 divides the network types of interface links into four types according to the link layer protocol types: one is the broadcast type (the link layer protocols are Ethernet, FDDI, etc.); The second is nBMA non broadcast multiple access type (link layer protocols are fr, ATM, HDLC, X.25, etc.); The third is the point to multipoint type. No link layer protocol will be regarded as the point to multipoint type by default. The point to multipoint type must be forcibly configured by other network types. The most common approach is to change the non fully connected nBMA to point to multipoint network. The fourth is the point-to-point type (the link layer protocols are PPP, LAPB and POS).

On broadcast networks without multiple access capability, the interface can be configured as nBMA type. When not all routers are directly accessible in nBMA network, the interface can be configured as point to multipoint type.

The nBMA network agreed in OSPFv3 protocol is fully connected, non broadcast and multi-point reachable. Point to multipoint networks are not necessarily fully connected.

NBMA needs to select Dr, and there is no DR in point to multipoint network. NBMA network multicast message through designated neighbor unicast message and point-to-multipoint network multicast message.

Mode: interface configuration mode

Command: IPv6 ospf network < type >

Configure the network type of the interface link

Command: no IPv6 ospf network

The network type of the recovery interface link is the default value

Parameter: Type: you can select broadcast, non broadcast, point to point, point to multipoint [non broadcast]; The first type is broadcast network, the second type is non broadcast network, i.e. nBMA, the third type is point-to-point network, and the fourth type is point-to-multipoint network; Point to multipoint networks are divided into broadcast and non broadcast networks. Non broadcast neighbors cannot be found automatically and must be specified.

Default: broadcast network

1.131.8 Configure Hello message sending interva

Hello message is used to send to neighbor router periodically, find and maintain neighbor relationship, and elect DR and BDR. The interval of Hello message can be configured manually, but attention should be paid to keeping the interval of Hello timer between neighbors in the network consistent. The value of Hello timer is inversely proportional to the convergence speed of router and network load.

Mode: interface configuration mode

Command: IPv6 OSPF Hello interval < seconds >

Configure the interval of Hello timer

Command: no IPv6 OSPF Hello interval

Restore the Hello timer interval to the default value

Parameter: the value of seconds is between 1 and 216-1, indicating the time interval between two Hello message sending.

Default: on broadcast network and point-to-point network, the Hello interval is 10 seconds; On nBMA network and point to multipoint network, the Hello interval is 30 seconds。

1.131.9 Configure neighbor router expiration time

Mode: interface configuration mode

Command: IPv6 OSPF dead interval < seconds >

Configure neighbor expiration time

Command: no IPv6 OSPF dead interval

Recovery neighbor failure time is the default value

Parameter: the value of seconds is between 1 and 216-1, which means that the neighbor is considered invalid if no Hello message is received after seconds; Every time a hello message is received, the neighbor's dead timer will be updated.

Default: the failure time of neighbors on broadcast network and point-to-point network is 40 seconds; On nBMA network and point to multipoint network, the neighbor failure time is 120 seconds; When the network type is modified, the Hello interval and dead interval will use the default values.

1.131.10 Configure retransmission time

O Spfv3 is a reliable link state protocol, which is manifested in that the LSU messages it interacts with need the LSU ack from the opposite end. When receiving the confirmation message, the party considers that the link state update is received. If no acknowledgement message is received within the retransmission interval, the LSA will be retransmitted to the neighbor. The retransmission interval can be configured manually. It needs to be longer than the time for a message to be transmitted back and forth between two routers. If it is set too small, it will cause unnecessary retransmission.

Mode: interface configuration mode

Command: IPv6 OSPF retransmit interval < seconds >

Configure the retransmission interval of the interface

Command: no IPv6 OSPF retransmit interval

The recovery retransmission interval is the default value

Parameter: the value of seconds is between 1 and 216-1, which indicates the interval of retransmission when the opposite end does not receive LSA.

Default: retransmission interval 5S

1.131.11 Configure interface delay

In the link state update message LSU, each link state broadcast LSA has a time domain. Before transmission, it is necessary to increase the transmission delay of the transmitting interface. This parameter mainly considers the time required for the interface to send messages, especially on low-speed networks.

Mode: interface configuration mode

Command: IPv6 OSPF transmit delay < seconds >

Set the transmission delay of the interface

Command: no IPv6 OSPF transmit delay

The transmission delay of the recovery interface is the default value

Parameter: the value of seconds is between 1 and 216-1, indicating that the delay value needs to be increased in the age domain of the LSA sent by the interface.

Default: the transmission delay of the interface is 1s

1.131.12 Configure the priority of interface in Dr election

In order to avoid repeated point-to-point transmission of link information in the broadcast network, it is necessary to elect the designated router DR and BDR to be responsible for broadcasting the link information in the network segment. The priority of the interface indicates its qualification in the election of Dr. in case of election conflict, the one with higher priority shall be considered first. If the priority is 0, they will not participate in the election. If the priority is greater than 0, they are candidates. Each router contains its own priority information and its own DR in its own Hello message, broadcasts in the broadcast network, and finally selects the one with higher priority to become Dr. If the priorities are equal, the higher the router ID will prevail.

When Dr fails, the router in the network needs to go through a process of re electing Dr, which takes a time, and during this time, it will cause routing calculation errors. The concept of BDR is to make a smooth transition to the new Dr. BDR is the backup of Dr. it is selected at the same time in the Dr election. It also establishes an adjacency relationship with other routers in the network. Only the information collection and publishing node in the network is in Dr rather than BDR. BDR only maintains the synchronization of adjacency. When the Dr fails, the BDR will immediately become a DR and be responsible for collecting information in the network segment. At this time, a new process will be started to elect the BDR, but the election of the BDR will not affect the calculation of the route.

Mode: interface configuration mode

Command: IPv6 OSPF priority < prio >

Configure the priority of interface in Dr election

Command: no IPv6 OSPF priority

Restore interface priority to default

Parameter: the value of prio is 0 ~ 255, which indicates the priority in Dr selection. When it is 0, it indicates that it does not participate in the election.

Default: priority is 1

1.131.13 Configure the cost of sending messages on the interface

In the network, the traffic is controlled by configuring different links at different costs. The cost of the interface represents the cost of sending messages from the interface. If it is not configured manually, OSPFv3 will automatically calculate the interface cost according to the interface baud rate.

Mode: interface configuration mode

Command: IPv6 OSPF cost < cost >

Command: no IPv6 OSPF cost

Parameter: the value of cost is between 1 and 216-1, indicating the proxy value of the message sent on the interface.

Default: interface cost 10

1.131.14 Whether to fill in MTU domain for DD message sent by configuration interface

Mode: interface configuration mode

Command: IPv6 OSPF MTU ignor

Set not to check MTU value in DD message

Command: no IPv6 OSPF MTU ignore

Cancel not checking MTU value in DD message

Default: check MTU value in DD message

1.131.15 Configure regional virtual link

OSPFv3 protocol adopts the layered idea to divide the routers in the autonomous system into different groups. These groups are called regions. All regions are not equal and parallel, but have hierarchical relations. Among them, 0.0.0.0 region is the most special, which is the backbone region. Other non backbone regions must exchange inter domain routes through the backbone region. Therefore, all non backbone areas must be connected with the backbone area, that is, at least one interface on the ABR is in area 0. If some areas cannot guarantee the physical path with the backbone area due to the limitation of network topology, virtual links need to be configured to ensure the logical path. Both ends of the virtual link are ABR, and the middle passes through a non backbone area, which is called the transmission area. When configuring the virtual link, it is necessary to

specify the ID of the transmission area and the ID of the opposite ABR, and it must be configured on the ABR at both ends before it can take effect.

When the route of the transmission area is calculated and the virtual link is activated, it is logically equivalent to forming a point-to-point connection between two endpoints. Therefore, the parameters of the interface can be configured on its physical interface and the authentication function can be started.

The unicast message is transmitted between ABRs. The router forwarding the unicast message in the transmission area will forward it as an ordinary IP message. Therefore, it can only be understood that a logical link is provided in the transmission area, and protocol messages can be exchanged between two ABRs.

Mode: OSPFv3 configuration mode

Command: Area < area ID > virtual link < router ID >

Configure the transmission area and peer ID of the virtual link

hello-interval <seconds>

Configure the Hello interval of virtual link

dead-interval <seconds> |

Configure virtual link neighbor failure time

retransmit-interval <seconds> |

Configure virtual link retransmission interval

transmit-delay <seconds> |

Configure virtual link interface delay

Command: no area < area ID > virtual link < router ID >|

hello-interval <seconds> |

dead-interval <seconds> |

retransmit-interval <seconds> |

transmit-delay <seconds>]

Cancel virtual link setting

Parameter: area ID refers to the ID of the transmission area. It can use dotted decimal format a.b.c.d or integer format. The value is between 0 ~ 232-1. Router ID refers to the ID of the peer router of the virtual link, in a.b.c.d format. Authentication and sending interface properties are optional. Please refer to relevant command descriptions.

Default: virtual link is not configured

1.131.16 Configure regional routing aggregation

Mode: OSPFv3 configuration mode

Command: Area < area ID > range < IPv6 prefix > [advertise | not advertise]

Configure aggregation scop

Command: no area < area ID > range < IPv6 prefix > [advertise | not advertise]

Cancel aggregation

Parameter: area ID refers to the area ID, which specifies the aggregation of routes in the area. You can use dotted decimal format a.b.c.d or integer format, and the value is between 0 ~ 232-1. IPv6 prefix uses the prefix format X: X:: X: X / m to represent the aggregation range. The optional parameters advertise and not advertise indicate whether to broadcast the aggregation range, that is, IPv6 prefix. The original network routes will be broadcast.

1.131.17 Configure stub area

Mode: OSPFv3 configuration mode

Command: Area < area ID > stub [no-summary]

Configure the router in the stub area

Command: no area < area ID > stub [no summary]

Cancel the properties of the router in the stub area

Command: Area < area ID > default cost < cost >

Configure the default cost of ABR broadcast routing connected to the stub area

Command: no area < area ID > default cost

Restore default cost to default valu

Parameter: area ID refers to area ID, indicating which area attribute is stub; You can use dotted decimal format a.b.c.d or integer format, with values between 0 ~ 232-1. No summary means that inter domain routes are not injected into the stub area.

The first group of commands is to configure the router located in the stub area, and the second group of commands is to configure the ABR with the interface connected to the stub area.

Default: the stub area is not configured

1.131.18 Configure default weights for external routes

The default value of the red metric command is not used when importing external weights.

Mode: OSPFv3 configuration mode

Command: default metric < metric >

Configure the default weight when introducing external routes

Command: no default metric [Metric]

The default weight is the default value when restoring the introduction of external route

Parameter: metric value between 0 ~ 224-1

Default: the default weight is 1

1.131.19 display information

Command: Show IPv6 OSPF [process ID

Display OSPFv3 process information

Parameter: instance ID is the process number,

The value is between 0 - (216-1).

Command: Show IPv6 OSPF database < type >

Display LSDB information

Parameter: type refers to all types of LSA and summary information. See the command manual for details.

Command: Show IPv6 OSPF interface [if name]

Display OSPFv3 interface information

Parameter: if name is the agreed three-tier interface name

Command: show ip ospf route

Display OSPF routing table

Command: Show IPv6 OSPF virtual links

Display OSPF virtual connection information

Command: Show IPv6 OSPF neighbor [options]

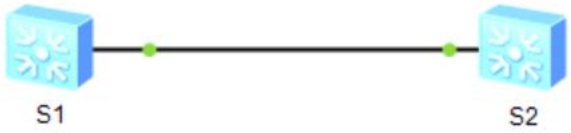
Display OSPF neighbor information

Parameter: options. See the command manual for detail

Mode: privileged mode

1.132 OSPFv3 Configuration example

The two switches are connected, as shown in the figure below。



S1 The switch configuration is as follows

```
Switch(config)#
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 address 3ffe:506::1/64
Switch(config-vlan1)#exit
Switch(config)#router ipv6 ospf
Switch(config-router)#router-id 1.1.1.1
Switch(config-router)#exit
Switch(config)#int vlan1
Switch(config-vlan1)#
Switch(config-vlan1)#ipv6 router ospf area
Switch(config-vlan1)#
```

S2 The switch configuration is as follows

```
Switch(config)#
Switch(config)#int vlan1
Switch(config-vlan1)#ipv6 address 3ffe:506::2/64
Switch(config-vlan1)#exit
Switch(config)#router ipv6 ospf
Switch(config-router)# router-id 5.5.5.5
Switch(config-router)#exit
Switch(config)#int vlan1
Switch(config-vlan1)#
Switch(config-vlan1)#ipv6 router ospf area 0
Switch(config-vlan1)#
```

Display the neighbor information of two OSPFv3

```
Switch#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface   Instance
ID
5.5.5.5           1   Full/DR         00:00:39    vlan1       0

Switch#
```

Configure BGP

This chapter mainly includes the following contents：

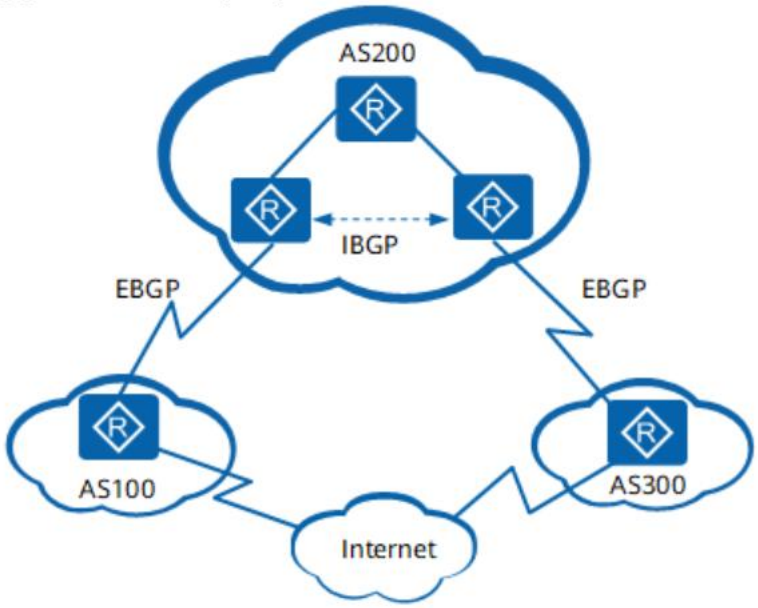
- PIM-SM introdution
- PIM-SM configuration
- PIM-SM configuration example

1.133 BGP introdution

Border Gateway Protocol BGP (border gateway protocol) is a distance vector routing protocol that realizes the reachability of routing between autonomous systems as (autonomous system) and selects the best route. The three versions released earlier are bgp-1 (rfc1105), bgp-2 (rfc1163) and bgp-3 (rfc1267). BGP-4 (rfc1771) was used in 1994. After 2006, the version used in unicast IPv4 network is BGP-4 (rfc4271), and the version used in other networks (such as IPv6) is MP-BGP (rfc4760).

BGP is divided into ebgp (external / external BGP) and iBGP (internal / internal BGP) according to the operation mode

The operation mode of BGP is shown in the following photo



• Ebgp: BGP running between different as is called ebgp. In order to prevent a loop between as, when BGP equipment receives the route sent by ebgp peer, it will discard the route with local as number.

• IBGP: BGP running in the same as is called iBGP. In order to prevent loop generation in as, BGP equipment does not announce the route learned from iBGP peers to other iBGP peers, and establishes full connection with all iBGP peers. In order to solve the problem of too many connections of iBGP peers, BGP designs routing reflector and BGP alliance.

There are five kinds of messages, six kinds of state machines and five principles in the interactive process of establishing, updating and deleting BGP peers.

BGP peers interact with each other through the following five types of messages, of which keepalive messages are sent periodically and the rest are triggered:

• Open message: used to establish BGP peer connection.

• Update message: used to exchange routing information between peers.

• Notification message: used to interrupt BGP connection.

• Keepalive message: used to maintain BGP connection.

• Route refresh message: used to request the peer to resend the routing information after changing the routing policy. Only BGP devices that support route refresh capability will send and respond to this message.

There are six state machines in the interaction process of BGP peers: idle, connect, active, open message sent (opensent), open message confirmed (openconfirm) and connection established (established). In the process of establishing BGP peers, the three commonly visible states are idle, active and established.

The BGP device adds the optimal route to the BGP routing table to form a BGP route. After the BGP device establishes the neighbor relationship with the peer, the following interaction principles shall be adopted:

• BGP route obtained from iBGP peer, BGP device only publishes to its ebgp peer.

• BGP routes obtained from ebgp peers, and BGP devices publish them to all ebgp and iBGP peers.

• When there are multiple valid routes to the same destination address, the BGP device only publishes the optimal route to the peer.

• When the route is updated, the BGP device only sends the updated BGP route.

• BGP device will receive all routes sent by peers.

BGP and IGP use different routing tables in the equipment. In order to realize the mutual communication between different as, BGP needs to interact with IGP, that is, BGP routing table and IGP routing table are introduced into each other.

BGP protocol itself does not find routes, so other routes need to be introduced into BGP routing table to realize routing interworking between as. When an as needs to publish routes to other as, the as edge router will introduce IGP routes into the BGP routing table. In order to better plan the network, when BGP introduces the route of IGP, it can use the route strategy to filter the route and set the route attribute, or set the Med value to guide the ebgp peer to judge the route when the traffic enters the as.

BGP supports import and network when introducing routes:

• The import method is to import the routes of rip, OSPF, Isis and other protocols into the BGP routing table according to the protocol type. In order to ensure the effectiveness of the introduced IGP route, the import mode can also introduce static route and direct route.

• The network method is to introduce the existing routes in the IP routing table into the BGP routing table one by one, which is more accurate than the import method

IGP introduces BGP routing

When an as needs to introduce routes from other as, the as edge router will introduce BGP routes into the IGP routing table. In order to avoid the impact of a large number of BGP routes on devices in as, when IGP introduces BGP routes, routing policies can be used to filter routes and set routing attributes

1.134 BGP configuration

1.134.1 Start BGP and enter BGP configuration mode

BGP protocol uses as number to identify; When starting BGP protocol, it is necessary to specify which autonomous system is started.

Mode: global configuration mode

Command: router BGP < as number >

Start the BGP protocol process and enter its mode

Command: no router BGP < as number >

Close the BGP protocol and delete its configuration

Parameter: as number value: 1-4294967295.

Default: BGP protocol is not run

1.134.2 Inject routing information into BGP protocol

At the beginning of running, the routing information of BGP is empty. There are two ways to inject routing information into BGP: manually inject routing information into BGP through network command. Through the interaction with IGP protocol, route information is injected from IGP. BGP publishes the injected route to its neighbors. This section mainly describes the manual injection of routing information.

Mode: BGP configuration mode

Command: network < network number > mask < mask > [route map < map tag >] [backdoor]

This command configures the network information to be announced by this BGP speaker.

Command: no network < network number > mask < mask > [route map] [backdoor]

This command deletes the set network information

1.134.3 Configure BGP timer

BGP uses keepalive timer to maintain effective connection with peers and holdtime timer to judge whether peers are effective. By default, the value of keepalive timer is 60 scores and the value of holdtime timer is 180 seconds. When a BGP connection is established between BGP speakers, both parties will negotiate the holdtime, and the holdtime with smaller value will be selected, while the selection of keepalive timer value will be based on the smaller of 1 / 3 of the negotiated holdtime and the configured keepalive value.

Mode: BGP configuration mode

Command: timers BGP < keepalive > < holetime >

This command is used to adjust the network timer of BGP.

Command: no timers BGP < keepalive > < holetime >

This command restores the default values。

1.134.4 Configure BGP and IGP synchronizatio

For the routing information that will cross this as to another as, it is allowed to publish the routing information to another as only when it is ensured that all routers in this as learn the routing information. Otherwise, if the router (running IGP protocol) in this as does not learn the routing information, when the data message passes through this as, it may discard the data message because these routers do not know the route, which will cause the routing black hole phenomenon.

Ensure that all routers in the as learn the routing information outside the as. We call it the synchronization of BGP and IGP. The simple way to realize synchronization is that BGP speaker redistributes all the routes learned by BGP protocol to IGP, so as to ensure that the router inside as can learn these routing information.

In two cases, the synchronization mechanism of BGP can be cancelled:

1. There is no routing information across this as (generally, this as is a terminal as);

2. All routers in this as run BGP protocol, and all BGP speakers establish full connection relationship (BGP speakers establish adjacency relationship)..

Mode: BGP configuration mode

Commands: synchronization

This command starts the synchronization mechanism of BGP and IGP routing information.

Command: no synchronization

This command cancels the synchronization mechanism between BGP and IGP。

1.134.5 Configure the interaction between BGP and IGP

Inject the route information generated by IGP protocol into BGP. By default, redistributing the default route is not allowed. If you want to redistribute the default route, use the following command to control it.

Mode: BGP configuration mode

Command: redistribute < protocol type > [route map < map tag >]

This command can redistribute the routing information of other routing protocols to

BGP.

Command: no redistribute < protocol type > [route map < map tag >]

This command deletes the function and its parameter configuration.

1.134.6 Selection of BGP optimal path

The selection of optimal routing is a very important part of BGP protocol. We will describe the selection process of BGP routing protocol in detail below:

If the routing table entry is invalid, it will not participate in the selection of the optimal route;.

Otherwise, elect local_ Routes with high pref attribute value;

Otherwise, select the route generated by the BGP speaker;

The routes generated by this BGP speaker include those generated by network command, redistribute command and aggregate command.

Otherwise, select the route with the shortest as length;

Otherwise, select the route with the lowest origin attribute value;

Otherwise, select the route with the lowest Med value

Otherwise, the priority of ebgp path is higher than that of iBGP path and as alliance, and the priority of iBGP path and as alliance is the same;

Otherwise, the route with the smallest IGP metric to the next hop is elected

Otherwise, in the route from ebgp, the election receives the earlier route;

Otherwise, the route with a smaller router ID of the BGP speaker of the route will be announced

Otherwise, the route with a large length of the election cluster;

Otherwise, the route with large neighbor address is elected.

Mode: BGP configuration mod

Command: BGP bestpath < as path ignore | compare confirmed aspath | compare routerid | don compare originator ID | Med [confirmed | missing as worst | remove recv Med | remove send Med] | tie break on age >

This command sets the election of BGP optimal route.

Command: no BGP bestpath < as path ignore | compare confirmed aspath | compare routerid | don compare originator ID | Med [confirmed | missing as worst | remove recv Med | remove send Med] | tie break on age >

This command deletes the election of BGP optimal route。

1.134.7 Configure BGP routing aggregation

BGP-4 supports CIDR, so it is allowed to create aggregation table entries to reduce

the size of BGP routing table. Of course, the BGP aggregation table entry is added to the BGP routing table only when there is a valid path within the aggregation range.

Mode: BGP configuration mode

Command: aggregate address < IP address > / < mask length > [as set | summary only]

This command sets the IPv4 / IPv6 aggregation routing table entry of BGP.

Command: no aggregate address < IP address > / < mask length > [as set | summary only]

This command deletes the aggregation routing table entry。

1.134.8 Configure BGP routing reflector

In order to speed up the convergence of routing information, all BGP speakers in an as will usually establish a full connection relationship (BGP speakers establish an adjacency relationship between two). When there are too many BGP speakers in the as, it will increase the resource overhead of BGP speakers, increase the workload and complexity of configuration tasks for network administrators, and reduce the expansion performance of the network.

In this regard, two methods of routing reflector and as alliance are proposed to reduce the number of iBGP peers in as. Routing reflector is a method to reduce the number of iBGP peer connections in autonomous system. A BGP speaker is set as a routing reflector, which divides iBGP peers in the autonomous system into two categories: client and non client.

The routing reflector is implemented in the as, and its rules are as follows:

Configure the routing reflector and specify its client. The routing reflector and its client form a group. Route Reflector

A connection relationship will be established between and the client.

The client of an intra group routing reflector should not establish a connection relationship with other BGP speakers outside the group.

In as, a complete connection relationship is established between iBGP peers of non clients. Here, the iBGP of non clients

Peers include the following situations: between multiple routing reflectors in a group; Routing reflectors and groups within a group

BGP speakers that do not participate in the routing reflector function (usually these BGP speakers do not support the routing reflector function); Between the routing reflectors in the group and the routing reflectors in other groups.

The processing rules of a route received by the route reflector are as follows:

The route update received from ebgp speaker will be sent to all clients and non

clients;

The route update received from the client will be sent to other clients and all non clients;

Routing updates received from iBGP non clients will be sent to all their clients.

Mode: BGP configuration mode

Command: neighbor [peer address | peer tag] route reflector client

This command configures the device as a routing reflector and specifies its client.

Command: no neighbor [peer address | peer tag] route reflector client

This command cancels the setting of the client。

1.134.9 Configure BGP's as Federation

Federation is another way to reduce the number of iBGP peer connections in autonomous systems.

An autonomous system is divided into several sub autonomous systems, and these sub autonomous systems are formed into an alliance by setting a unified alliance ID (i.e. alliance as number). For the outside of the alliance, the whole alliance is still considered as an as, and only the as number of the alliance is visible. Within the alliance, a complete iBGP peer connection is still established between BGP speakers within the sub autonomous system, and an ebgp connection is established between BGP speakers between the sub autonomous systems. Although the ebgp connection is established between the BGP speakers of the sub autonomous system, when exchanging information, for next_ Hop, Med and local_ Path attribute information such as pref remains unchanged..

Mode: BGP configuration mode

Command: BGP confirmation identifier < as number >

This command configures the identifier of the as Federation.

Command: no BGP confirmation identifier

This command cancels the identifier of the as Federation。

1.134.10 Configure BGP management distance

The management distance indicates the reliability of a routing information source, which ranges from 1 to 255. The greater the value of the management distance, the lower the reliability.

BGP sets different management distances for different sources of learned routing information, which are divided into external distance, internal distance and local distance:

External distance: learn the management distance from ebgp peers to routing.

Internal distance: learn the management distance from iBGP peers to routing.

Local distance: learned from peers, but it is considered that there are pipes that can learn better routing from IGP

Manage distances. These routes are usually represented by the network backdoor command.

Mode: BGP configuration mode

Command: distance BGP < external distance > < internal distance > < local distance >

This command sets different management distances for different types of BGP routes.

Command: no distance BGP < external distance > < internal distance > < local distance >

This command restores the default management distance。

1.134.11 Configure BGP routing update mechanism

BGP routing update mechanism includes two parts: regular scan update and event triggered update. Scheduled scan update means,

BGP uses a timer to start the scanning mechanism regularly and update the routing table. The event triggered update means that when the user configures BGP, resulting in the change of BGP configuration command or the change of the next hop of BGP route, it triggers BGP to start the scanning mechanism and update the routing table..

Mode: BGP configuration mode

Command: BGP scan time < time >

This command sets the time interval of regular scanning of BGP protocol.

Command: no BGP scan time [time]

The time interval for the command to resume the regular scanning of BGP protocol is 60 seconds。

1.134.12 Configure BGP local as

BGP's local as function is used to configure a local as different from BGP's real as (router BGP as) for a specific peer, which is similar to virtualizing a new as with the peer device, so that when the local BGP's real as changes, the BGP configuration of the peer device does not need to be changed to realize the establishment of BGP connection. This function is mainly

The migration and consolidation of as for large networks can ensure that the

configuration of equipment in other interconnected as will not be affected.

In the BGP protocol, when the local device establishes a BGP connection with the peer, it will announce the local as number to the peer device through the open message. The peer device will check whether the BGP as announced by the connection end is the same as the locally configured peer as. If not, it will reject the BGP connection. By default, the local as in the BGP connection is the real as of BGP. By configuring the local as for the peer, the local device will use the configured local as to replace the real as and establish the BGP connection when establishing the BGP connection with the peer

Mode: BGP configuration mode

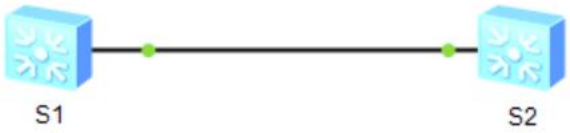
Command: neighbor [peer address | peer tag] local as < as number >

Set to configure a local as number for a BGP peer. At this time, the peer device can use the local as as its remoteas to establish a BGP connection with the device..

Command: no neighbor [peer address | peer tag] local as < as number >

This command deletes the configured local as。

1.135 BGP Configuration example



S1 The switch configuration is as follows

Switch(config)#

Switch(config)#int vlan1

Switch(config-vlan1)#ip address 192.168.0.1/64

Switch(config-vlan1)#exit

Switch(config)#router bgp 1

Switch(config-router)#bgp router-id 1.1.1.1

Switch(config-router)#neighbor 192.168.0.2 remote-as 1

Switch(config-router)#neighbor 192.168.0.2 interface vlan1

Switch(config-router)# neighbor 192.168.0.2 next-hop-self

Switch(config-router)#exit

S2 The switch configuration is as follows

```
Switch(config)#
Switch(config)#int vlan1
Switch(config-vlan1)#ip address 192.168.0.2/64
Switch(config-vlan1)#exit
Switch(config)#router bgp 1
Switch(config-router)#bgp router-id 2.2.2.2
Switch(config-router)#neighbor 192.168.0.1 remote-as 1
Switch(config-router)#neighbor 192.168.0.1 interface vlan1
Switch(config-router)# neighbor 192.168.0.1 next-hop-self
Switch(config-router)#exit

Display neighbor BGP information
Switch#show bgp neighbors
BGP neighbor is 192.168.0.2, remote AS 1, local AS 1, internal link
  BGP version 4, remote router ID 2.2.2.2
  BGP state = Established, up for 00:02:09
  Last read 00:02:09, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 7 messages, 0 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 192.168.0.1, Local port: 53557
Foreign host: 192.168.0.2, Foreign port: 179
Nexthop: 192.168.0.1
Nexthop global: fe80::82:44ff:fe13:4803
```

Nexthop local: ::

BGP connection: non shared network

Switch#

Configure VRRP

This chapter mainly includes the following contents：

- VRRP introduction
- VRRP configuration
- VRRP configuration example

1.136 VRRP introduction

VRRP is an important protocol for virtual router backup, which is called VRRP by default. This section gives a detailed description of VRRP protocol, mainly including the following contents：

VRRP overview

VRRP terminology

VRRP protocol interaction

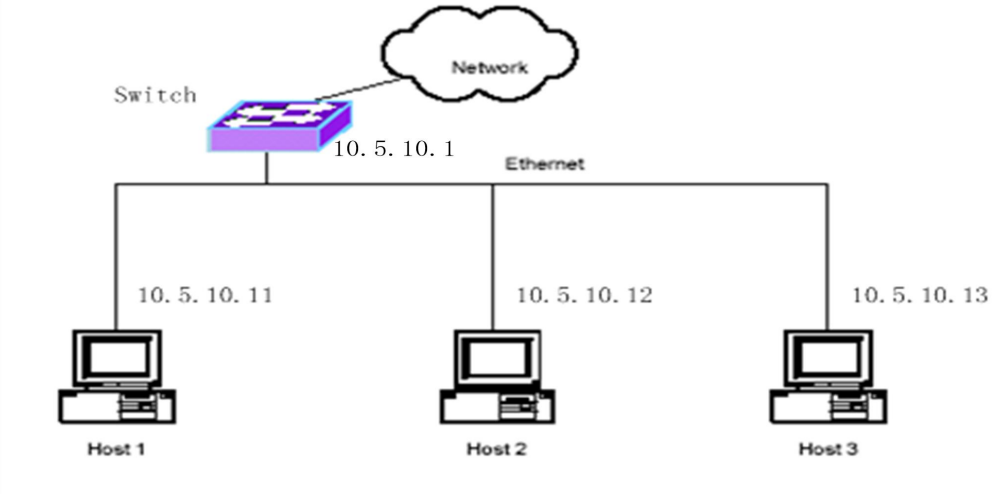
Election of virtual master route

Status of virtual router

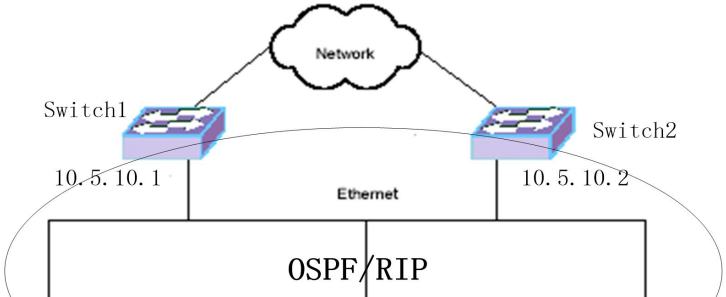
VRRP tracking

1.136.1 VRRP summary

The following figure is a typical intranet networking scheme. One interface of the switch is connected to the external network and the other interface is connected to the internal network. The IP address of the interface connected to the internal network is 10.5.10.1. Hosts 1, 2 and 3 are configured with IP addresses, which are all in network segment 10.5.10.0/24. A default gateway is configured on hosts 1, 2 and 3. The next hop points to the switch, and the IP address of the next hop is 10.5.10.1. In this way, when the host sends a message whose destination IP address is not in this network segment, it will match the default route and send it to the switch. Then the switch forwards the message, and the switch also forwards the message from the external network to the corresponding host. In this way, the host realizes the communication with the external network。



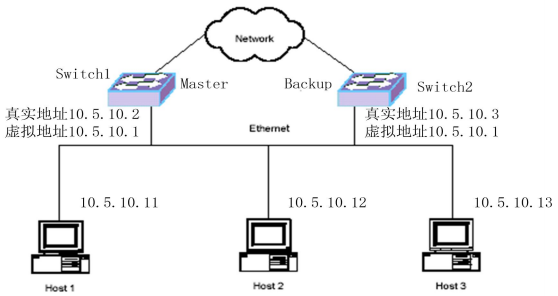
In the above networking scheme, the communication between the host and the external network can only pass through this unique switch. When the switch fails, all hosts will be disconnected from the external network. In order to solve this problem, one solution is to expand one switch to two or more switches, and run the dynamic routing protocol OSPF or rip between the host and the switch, as shown in the figure below。



When the host runs the dynamic routing protocol, the host can learn all the routes of the external network. When communicating with the external network, the host finds the route according to the destination IP address of the message to get the next hop to decide whether to send the message to Switch1 or switch2. When one of the switches fails, the route in the host can be re learned in a very short time, and the next hop of the route will point to the router without failure, so that the communication between the host and the external network will not be interrupted.

However, it is unrealistic to implement dynamic routing protocol on the host. For the host, the load of running dynamic routing protocol is too large. For the network, running dynamic routing protocol on the host will cause too much unnecessary data traffic on the network. Moreover, some hosts do not support dynamic routing protocol at all.

In order to fundamentally solve the problem of single point of failure, VRRP protocol is the best choice. VRRP protocol is specifically proposed to solve this problem. As shown in the figure below, Switch1 and switch2 form a virtual router. The real IP addresses of the interfaces of the two switches are different, but there is a common virtual IP address 10.5.10.1. The default gateway of the host is set to virtual IP address 10.5.10.1. When Switch1 is the virtual master switch, the communication between the host and the external network is forwarded through Switch1. However, when Switch1 fails, switch2 takes over from Switch1 as the virtual master switch, and the communication between the host and the external network is forwarded through switch2. Using VRRP protocol, the host only needs to set the default gateway without running other protocols on the host. The load of the host is small, and only a small amount of VRRP protocol flow needs to be added on the network。

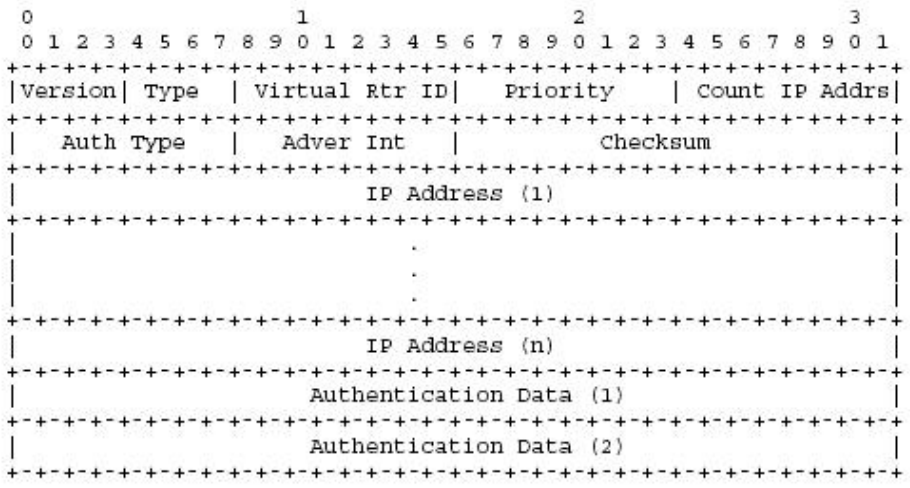


1.136.2 VRRP term

- Here are some frequently used terms:
- 1）VRR
- The abbreviation of Virtual Router Redundancy Protocol, virtual router redundancy protocol, is a fault-tolerant protocol of default gateway, which can improve the reliability of the network.
- 2）Virtual Router
- Virtual router, an abstract object based on subnet interface, includes a virtual router identifier (VRID) and an IP address. This (these) IP address is also called virtual IP address, which is used as the default gateway of the host.
- 3）VRRP Router
- VRRP router, that is, the router running VRRP protocol. A VRRP router can be added to a virtual router.
- 4）IP Address Owner
- IP address owner: a VRRP router whose virtual IP address is the same as the real IP address of the interface.
- 5）Virtual Router Master
- The virtual master router is responsible for forwarding the three-layer data packets passing through the virtual router and responding to the ARP request of the IP address of the virtual router. If a VRRP router is the IP address owner, it is always the virtual master router.
- 6）Virtual Router Backup
- The virtual backup router does not forward layer-3 data packets and does not respond to the ARP request of the virtual IP address. When the virtual main router fails, it takes over the work of the virtual main router.
- In order to better understand these terms, we should pay attention to the following points:
- A switch can include multiple interfaces, and VRRP protocol can be started on multiple interface subnets.
- A virtual router can exist on an interface subnet.
- A VRID identifies a virtual router。

1.136.3 VRRP Protocol interaction

The VRRP protocol package is encapsulated in the IP package, and the VRRP message header is shown in the figure below：



1) MAC header field of VRRP packet

Source MAC address: the virtual MAC address of the virtual router, which is 00-00-5e-00-01 - {VRID}. VRID is the identifier of the virtual router. For example, if the VRID of the virtual router is 1, the virtual MAC address is 00-00-5e-00-01-01.

Destination MAC address: VRRP multicast MAC address, 01-00-5e-00-00-12.

2) VRRP packet header field

Source IP address: the primary IP address of the interface that sends the VRRP packet.

Destination IP address: multicast IP address 224.0.0.18. Layer 3 forwarding is not allowed.

TTL: 255 to prevent remote VRRP packet attacks.

Protocol：112。

3) VRRP header field

Version：2。

Type: the type of VRRP package. Only one type is supported: 1 --- advertisement, VRRP notification package.

VRID: identifies a virtual router.

Priority: for this virtual router, the priority of the VRRP router sent.

Count IP addrs: the number of virtual IP addresses. A virtual router can have multiple virtual IP addresses.

Auth type: an authentication method between VRRP routers in a virtual router.

Advertisement interval: the interval between announcements. The default is 1 second.

Checksum: checksum, calculated from the version of VRRP header.

IP address (ES): one or more virtual IP addresses.

Authentication data: authentication data.

4) VRRP priority

Each VRRP router in a virtual router needs to be configured with a priority. The priority ranges from 0 to 255, of which 0 and 255 have special purposes. The configurable priority ranges from 1 to 254, and the default is 100. The higher the priority value, the higher the priority, and the more likely it is to become a virtual master router.

In a virtual router, when a VRRP router is the IP address owner, its priority is 255.

When the virtual master router needs to notify other backup routers that it is no longer the master router, send the VRRP packet with priority 0 to other backup routers, which can quickly trigger other backup routers to become the virtual master router.

5) VRRP certification

VRRP protocol provides three authentication methods. In actual use, different authentication methods can be selected according to the security requirements of the network.

0 --- No Authentication

No certification

1 --- Simple Text Password

Simple password authentication

2 --- IP Authentication Header

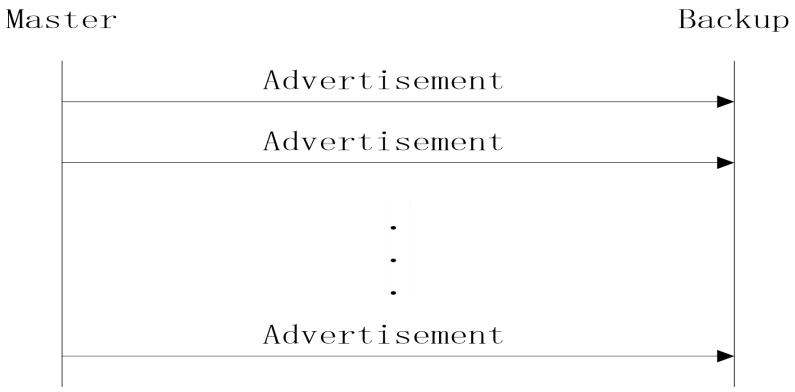
The IP authentication header calculates the message digest through HMAC-MD5 method

No authentication or simple password authentication can be used in the network with low security, and HMAC authentication method can be used in the network with high security.

For 0 and 2 authentication methods, the authentication data field is filled with 0, and for 1 authentication method, the authentication data field is filled with password. For the 2 authentication method, the message summary is filled in the IP authentication header field, that is, the ah field is added to the IP header.

6) VRRP package interaction

There is only one type of package in VRRP protocol, the advertisement package. In a virtual router, the virtual master router sends an announcement packet every advertisement interval (the default is 1 second). The virtual backup router determines whether state migration is required according to the VRRP notification packet received. The protocol interaction between master and slave is shown in the figure below：



1.136.4 Election of virtual master router

In a virtual router, the selection of the virtual master router is determined by the following factors:

IP address owner

If a VRRP router is the IP address owner (its interface IP address is the same as the virtual IP address), if the router works normally, it is the virtual master router.

VRRP priority

The VRRP router with the highest priority that works normally becomes the virtual master router. The configurable priority ranges from 1 to 254. The priority of the IP address owner's router is 255. When the virtual master router notifies the virtual backup router that it is no longer the master, priority 0 is given in the VRRP packet.

The actual IP address of the interface. When the priorities are the same, the VRRP router with a large actual IP address of the interface becomes the virtual master router.

Active / standby switching occurs in the virtual router under the following conditions:

1) When the virtual primary router fails, there will be active and standby switching. In this case, there are two possibilities

If the virtual master router is still active, it will send a VRRP packet with priority 0. After receiving this packet, the backup router will send it to skew_ When the VRRP packet of the virtual master router is not received within time, it will be switched to the virtual master router. In this case, the switching speed is relatively fast, and the switching can be realized within 1 second.

If the virtual master router cannot be active, the virtual backup router will switch to the virtual master router after it does not receive the VRRP packet of the virtual master router within the master down interval

Master_ Down_ Interval = (3 * Advertisement_Interval) + Skew_ Time

Skew_ Time = ((256 – Priority) / 256)

2) When the virtual master router is not an IP address owner, but now a router with an IP address owner joins the network, the router will become a virtual master router and there will be active standby switching.

3) When a VRRP router joins the network, if the priority of the router is higher than that of the virtual primary router and it is in the preemption mode (the configuration variable preempt_mode is true), the router will become the virtual primary router and there will be active standby switching.

1.136.5 Status of virtual router

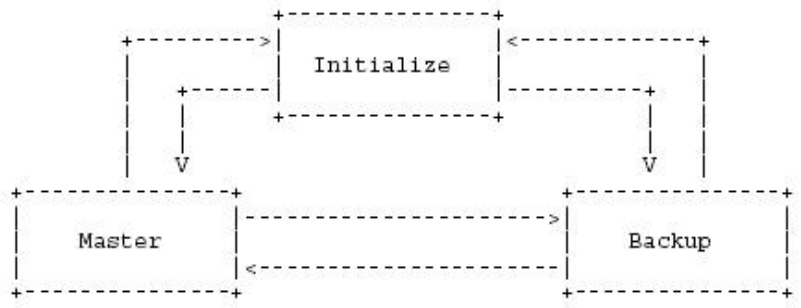
Each VRRP router in a virtual router executes a state machine. The migration of state machine is shown in the figure below：

1

I

event

becor



Otherwise, the router becomes a virtual backup router and migrates to the backup state.

The actions of the router after migrating to the master state are as follows:

Send a VRRP notification package.

Broadcast an ARP request, including the virtual IP address and the corresponding virtual MAC address.

Set up adver_ Timer timer with the interval of advertisement_ Interval。

After the router is migrated to the backup state, the actions are as follows

Set master_ Down_ Timer timer, the timing interval is master_ Down_ Interval。

2) Backup status

The purpose of backup status is to monitor the availability and status of the virtual master router and take over the work of the virtual master router at any time.

If you receive a shutdown event, cancel the master_ Down_ Timer timer, return to initialize state.

If master_ Down_ When the timer expires, it becomes the virtual master router and

migrates to the master state.

If you receive a VRRP notification package, there are several situations:

If the priority field in the VRRP package is 0, set master_ Down_ Timer, the timing interval is skew_ Time。

Otherwise, if the preempt_mode is false or the priority in the VRRP package > = the priority of the VRRP router, reset the master_ Down_ Timer, the timing interval is master_ Down_ Interval。

Otherwise, discard the VRRP package

3) Master status

The VRRP router in the master state is responsible for forwarding the three-layer data packets passing through the virtual router

If you receive a shutdown event, cancel the adver_ Timer timer, send a VRRP notification package with priority 0 and migrate to initialize state.

If adver_ When the timer expires, send a VRRP notification packet and reset the adver_ Timer timer.

If you receive a VRRP notification package, there are several situations

If the priority in the package is 0, send a VRRP notification package and reset the adver_ Timer。

Otherwise, if the priority in the packet is higher than that of the VRRP router or the priority is the same, but the IP address of the packet is greater than the primary IP address of the interface of the VRRP router, the adver will be cancelled_ Timer timer, set master_ Down_ Timer, migrate to the backup state.

Otherwise, discard the VRRP notification packet.

1.136.6 VRRP track

The VRRP protocol itself can only detect the internal faults of the virtual router, such as the link down of the interface where the virtual router is located or the crash of the VRRP router, but can not detect the external faults of the virtual router. When there are faults outside the virtual router, the virtual router cannot select the virtual main router according to these faults, which will cause the interruption of network data. VRRP tracking can solve this problem. VRRP router tracks the specified external events. When an external fault occurs, VRRP router changes its operation priority and reselects the virtual main router to ensure that the network data is not interrupted。

As shown in the figure below, when the external interface of the virtual master router Switch1 is link down, if the VRRP tracking function is not enabled, Switch1 cannot detect

this external fault, Switch1 continues to be the virtual master router, and the host cannot access the external network. If the VRRP tracking function is enabled, Switch1 can find external faults, modify its operation priority and re select the virtual master router. Switch1 is changed to a virtual backup router and switch2 is changed to a virtual master router, so that the host can continue to access the external network。

VRRP tracing includes interface tracing, route tracing and Ping tracing. Interface tracking is that VRRP router tracks the interface outside the virtual router. If an interface tracked is link down, it indicates that there is an external fault. Route tracking is that VRRP router tracks the route in the learned route table. If the route does not exist or the route exists but is not active, it indicates that an external fault has occurred. Ping tracking refers to the device tracked by VRRP router. If the device does not respond to Ping within the specified time, it indicates that there is an external fault. The virtual router can track the interface, route and Ping at the same time. For each type of tracking, it can track multiple events. As long as one of the tracked events fails, it indicates that the virtual router has an external failure. Only when all the tracked events are normal, it indicates that the virtual router has no external failure。

1.137 VRRP configuration

VRRP configuration includes the following contents:

Create and delete virtual routers

Configure the virtual IP address of the virtual route

Configure parameters of virtual router

Configure VRRP tracking

Start and shut down the virtual router

View VRRP information

1.137.1 Create and delete virtual routers

The virtual router is built on the subnet interface and needs to specify a VRID. The system does not create a virtual router by default.

When a virtual router is no longer needed, the virtual router can be deleted. If the virtual router has been started, the virtual router will be closed first and then deleted.

The commands to create and delete a virtual router are as follows：

Command	Description	CLI mode
router vrrp <vrid>	Create a virtual router and enter the VRRP configuration mode. If the virtual router already exists, directly enter the VRRP configuration mode. The parameter is VRID, ranging from 1 to 255。	Global configuration mode
no router vrrp [vrid]	Delete a virtual router. The parameter is VRID	Global configuration mode

1.137.2 Configure the virtual IP address of the virtual router

Virtual IP address must be configured on the virtual router. Theoretically, a virtual router can have one or more virtual IP addresses, but a virtual router only supports one virtual IP address when the switch is implemented. By default, the switch is not configured with a virtual IP address.

The commands to configure the virtual IP address of the virtual router are as follows

Command	Description	CLI mode
virtual-ip <virtual-ip> <backup | master>	Set the virtual IP address of the virtual router.	VRRP Configuration mode
no virtual-ip	Delete virtual IP address of virtual router。	VRRP Configuration mode

Note

- Configuring the virtual IP address of the virtual router can only succeed when the virtual router is turned off. It cannot succeed when the virtual router is started。
- The set virtual IP address must be in the same network segment as the primary IP address of the interface, otherwise the configuration will not succeed。

1.137.3 Configure parameters of virtual router

The parameters of virtual router include priority, preemption mode, notification interval, authentication method and authentication data. These parameters have default values, as shown in the table below：

parameter	Default value
priority	100
Preempt Mode	TRUE
Notification interval	1 seconds
Authentication method	No certification
Authentication data	None

During configuration, for the virtual router, the notification interval, authentication method and authentication data must be configured the same, while the priority and preemption mode parameters can be configured the same.

The priority is divided into configuration priority and operation priority. In most cases, the operation priority uses the configuration priority, but when the VRRP router is the owner of the IP address, the operation priority is 255 and the configuration priority is not used.

For the authentication method, the switch only realizes two methods: no authentication and simple password authentication, but does not realize the IP authentication header method.

The commands for configuring the parameters of the virtual router are shown in the following table：

Command	Description	CLI mode
priority < priority-value >	Set the priority of the virtual router. The priority range is 1 to 254.	VRRP onfiguration mode

preempt-mode {false | true}	Set the preemption mode of the virtual router. True means preemption and false means no preemption.	VRRP onfiguration mode
advertisement-interval <interval>	et the notification interval of the virtual router, ranging from 1 to 255, in seconds.	VRRP onfiguration mode
authentication none	Set the authentication method of virtual router as no authentication.	VRRP onfiguration mode
authentication simple-password <key>	The authentication method of setting the virtual router is simple password authentication, and the authentication data, namely password, should be set.	VRRP onfiguration mode

Note

- The parameters of configuring the virtual router can only succeed when the virtual router has been turned off. The configuration cannot succeed when the virtual router is started。

1.137.4 Configure VRRP tracking

At present, the switch only realizes the VRRP interface tracking function. VRRP router can track an interface, which can be layer-2 interface or aggregation interface. The switch does not have a tracked interface configured by default.

If the VRRP router is the IP address owner, the administrator can configure VRRP tracking, but in fact, VRRP tracking will not take effect, that is, even if the virtual router has an external failure, it will not reselect the virtual master router. If you want to use the VRRP tracking function, do not configure the virtual router as the IP address owner

When the administrator configures VRRP tracking, specifies a to be tracked, and starts the virtual router, VRRP tracking takes effect. When VRRP router finds a tracked interface link down, it considers that there is an external failure. Set the operation priority of virtual router to the value of source priority minus priority value. Through the interaction of VRRP protocol package, the virtual main router can be re selected. When the tracked

interfaces are all link up, the operation priority of the virtual router will be reset to the configuration priority after fault recovery.

The commands for configuring VRRP tracking are shown in the following table

Command	Description	CLI mode
circuit-failover <if-name> <priority-value>	Set the interface to be tracked by the virtual router.	VRRP onfiguration mode
no circuit-failover	Clear the tracked interface of the virtual router。	VRRP onfiguration mode

Note

Configuring VRRP tracing can only succeed when the virtual router is turned off. It cannot succeed when the virtual router is started。

1.137.5 Start and shut down the virtual router

After the virtual router is created and the virtual IP address and parameters are set, the virtual router does not really run and is still in the initialize state. Starting the virtual router will start the operation of the protocol, send a startup event to the protocol, and the state machine will migrate to the master state or backup state. Shutting down the virtual router will shut down the operation of the protocol, send a shutdown event to the protocol, and the state will move back to the initialize state

Before starting the virtual router, you must ensure that the virtual IP address has been configured. When the virtual router is started, if you need to modify the virtual IP address or parameters, you must first turn off the virtual router and then configure it. After the configuration is completed, start the virtual router.

The commands to start and shut down the virtual router are as follows：

Command	Description	CLI mode
enable	Start the virtual router.	VRRP onfiguration mode
disable	Turn off the virtual router.	VRRP onfiguration mode

1.137.6 View VRRP information

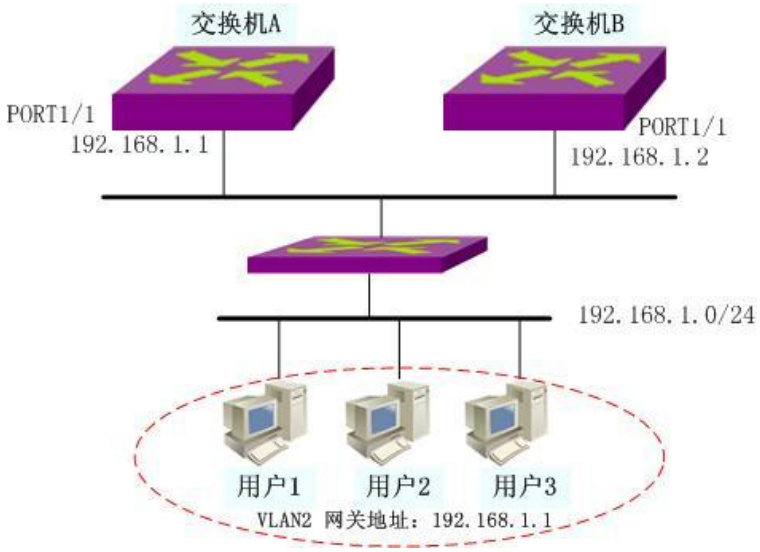
You can view the running status information and configuration information of VRRP through the command. The commands to view VRRP information are as follows：

Command	Description	CLI mode
show vrrp [vrid]	If no parameters are entered, the information of all virtual routers will be displayed.	Normal mode / privileged mode
show running-config	View the current configuration of the system, and you can view the configuration of VRRP.	privileged mode

1.138 VRRP Configuration example

(1) Configuration

Enable the VRRP function on two switches to provide three-layer routing redundancy for users in the LAN, eliminate routing faults in the network, and set switch 1 as the master switch and switch 2 as the backup switch。



Configuration on switch A

Switch#configure terminal

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

```
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#exit
Switch(config)#ip interface vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.1/24
Switch(config-vlan2)#exit
Switch(config)#router vrrp 1
Switch(config-vrrp)# virtual-ip 192.168.1.1 master
Switch(config-vrrp)#enable

Configuration on switch B
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#exit
Switch(config)#ip interface vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.2/24
Switch(config-vlan2)#exit
Switch(config)#router vrrp 1
Switch(config-vrrp)# virtual-ip 192.168.1.1 backup
Switch(config-vrrp)#enable vrrp
```

(2) verification:

View the information of VRRP through the following command：

```
show running-config
show vrrp
show vrrp 1
```

Configure VLLP

This chapter mainly includes the following contents：

- VLLP introduction
- VLLP Configuration
- VLLP configuration example

1.139 VLLP introduction

Vllp (VRRP layer-2 loop protection protocol) is a private protocol proposed to solve the problem of layer-2 loop in the application of VRRP protocol. When the vllp and the layer-3 switches use the protocol block to cut off the messages on the layer-2 and layer-3 loops and notify each other of the status of the two switches. If the timer of the port set to block state times out, it will be reset to forward state. Vllp protocol monitors and maintains the loop state of the port by immediately notifying the port state change and timer timeout, and ensures that the loop is cut off in time. Vllp protocol uses query response method to collect port status information. When two layer-3 switches running vllp protocol are started, one will be automatically selected as sender and the other as receiver. The sender is responsible for sending the query message regularly, and the receiver receives the query

message and sends back the response message. When the receiver has a port state change, it needs to actively send a link state change message to notify the sender of the corresponding change. Vllp protocol needs to work with VRRP protocol to start and maintain the status of relevant ports in VLAN. Vllp protocol only needs to run on VRRP switch, while layer 2 switch does not need to run any loop protection protocol.

Basic concepts of vllp protocol:

Vllp device: a vllp protocol entity running on a VLAN is called a vllp device.

Vllp port: the port that participates in vllp protocol interaction in the VLAN corresponding to the vllp device

Vllp equipment status: vllp equipment has two statuses: sender and receiver.

Sender: vllp equipment in sender status actively sends vllp query message periodically.

Receiver: vllp equipment in receiver status responds to query message; When the link state changes, actively send vllp link state change message.

Vllp port status: the vllp port has three STP statuses: disable, block and forward.

Main port: select a vllp port as the main port when the vllp device is in the sender state; A vllp sender has only one primary port. Vllp ports with high priority and mapping relationship can be preempted as primary ports.

Vllp port mapping relationship: there are vllp ports that interact with vllp protocol messages with opposite end switches.

Selection principle of vllp equipment receiver:

1. The one with high priority becomes the receiver;

2. Those with the same priority and large MAC address become recipients.

Main port election principle:

1. The port must be link up

2. The vllp port must have a mapping relationship

If there is no vllp port that meets the conditions, the main port does not exist;

If there are multiple vllp ports that meet the conditions, select the one with higher priority as the main port; If the priority is the same, select the first one to establish the mapping relationship as the primary port.

Vllp port status determination principle:

If the vllp device is the sender, the status of the main port must be forward;

The vllp device is the sender, the link state is link up, and the vllp port state without mapping relationship is forward

The vllp device is the sender, the link state is link up, and the vllp port state with mapping relationship is block;

The vllp device is the receiver, the link status is link up, and the vllp port status is

forward;

The vllp port with link down status is disabled.

Vllp protocol message is encapsulated in MAC frame

<table>
<tr><td colspan="5">Destination MAC Address (6 bytes)</td></tr>
<tr><td colspan="5">Source MAC Address (6 bytes)</td></tr>
<tr><td colspan="2">0x8100</td><td>Prio</td><td>Vlan ID (12 bits)</td><td>Ethernet Type (2 bytes)</td></tr>
<tr><td>Version</td><td>Type</td><td colspan="3">Port1(2 bytes)</td></tr>
<tr><td>Priority</td><td>Query Inter</td><td colspan="3">Main port</td></tr>
<tr><td colspan="5">Reserved (4 bytes)</td></tr>
<tr><td colspan="2">Port2</td><td>Link state</td><td colspan="2">STP state</td></tr>
</table>

There are three types of vllp protocol messages

Link status query message LQ

Link state response message La

Link state change message LC

Value range of each field in message format:

Des MAC: fixed at 00:09: CA: FF: FF: FF

SRC MAC: MAC of VLAN sending vllp protocol message

Ethernet type: fixed to 0x268

Version: currently 1

Type: LQ is 1; La is 2; LC is 3;

Port1: index value of the port sending vllp protocol message

Priority: vllp equipment priority, value 1 ~ 255

Query interval: interval of vllp sender query timer, 5 seconds by default

Main port: index value of vllp sender's main port, only in LQ message;

Reserved: the reserved domain is zero

Port2: the index value of the port whose state changes in LC message. The LQ is consistent with port2 and port1 in La message

Link state: the link state of port2. Link up is 1 and link down is 2;

STP state: the STP state of port2. Disable is 1, block is 2, and forward is 3

Vllp protocol principle:

Configure vllp equipment and start vllp protocol in a VLAN, and configure vllp equipment and start vllp protocol in the corresponding VLAN of the opposite end switch. At this time, the vllp protocol entity (vllp device) running on the VLAN constitutes a pair of

sender and receiver. When the protocol is started, both parties are senders and send LQ messages to each other. When the vllp device receives the LQ message, it will select the receiver according to the priority carried in the message and the opposite MAC address. The winning party becomes the receiver and will no longer send the LQ message, but respond to the LQ message of the sender. When the receiver's timer times out and has not received the LQ message, the receiver will return to the sender state and start sending the LQ message

In a VLAN that has started the vllp protocol, the port participating in the message interaction of the vllp protocol needs to be configured as a vllp port. The vllp port can be a valid layer-2 port (including the trunk group), but the members of the trunk are not allowed to be configured as vllp ports. Vllp protocol messages are sent and received through vllp port. The vllp port and the vllp port configured in the VLAN corresponding to the vllp protocol started by the opposite end switch form a pair of mapping relationship. They determine the mapping relationship with the opposite end port by sending query message, receiving response message or changing message, and calculate the possible loop in the network according to the mapping relationship and its own link state, The STP state of the vllp port is maintained according to the state determination principle of the vllp port, so as to prevent the loop in the topology.

Multiple vllp ports can be started in a VLAN that has started the vllp protocol. They may or may not have a physical link with the opposite switch. When the port belongs to multiple VLANs, the same vllp port will also appear in multiple vllp devices. Vllp protocol will dynamically collect the information of link state change of vllp port and STP state of opposite vllp port to calculate the loop in time and effectively prevent the occurrence of loop in the network.

When there are multiple VLANs with identical port configurations, but the vllp protocol needs to be started on multiple VLANs, each layer-2 port needs to send and receive multiple vllp protocol messages running on different VLANs, resulting in the burden of the switch. Therefore, the concept of auxiliary VLAN is proposed. That is, VLANs with exactly the same port configuration run the vllp protocol on only one VLAN, that is, the primary VLAN, while other VLANs are added to the instance of the primary VLAN as subsidiary VLANs. The result of the loop is calculated by the vllp protocol on the primary VLAN, and the port status in the instance is written. It should be noted that when configuring the auxiliary VLAN, ensure that the vllp ports of the main VLAN are in the auxiliary VLAN and all ports of the auxiliary VLAN are in the main VLAN. When the auxiliary VLAN is configured and the layer-2 port is added to the auxiliary VLAN, if the port is also in the main VLAN, the port state is uniformly managed by the main VLAN; If the port is not in the primary VLAN, the port status cannot be managed and an alarm message is prompted。

1.140 VLLP configuraton

After starting the vllp protocol, you can configure relevant attributes and create ports, and the relevant commands are in the vllp configuration mode.

Vllp configurations include：

- Create vllp device on layer 3 interface
- Enable vllp device
- Create vllp port on layer 2 interface
- Configure vllp device priority
- Configure vllp device query timer interval
- Configure attached VLANs
- Configure vllp port priority

1.140.1 Create vllp device on layer 3 interface

Mode: global configuration mode

Command: router vllp < if name > Create vllp device and enter vllp configuration mode

Command: no router vllp < if name > Delete vllp device

Parameter: if name is the agreed three-tier interface name (for example: vlan1, vlan2...)

Default: do not start vllp protocol

1.140.2 Enable vllp device

Mode: vllp configuration mode

Command: vllp enable Enable vllp device

Command: vllp disable Disable vllp devices

Default: the vllp device is not started after it is created

1.140.3 Create vllp port on layer 2 interface

Mode: vllp configuration mode

Command: vllp port < if name > Create vllp port

Command: no vllp port < if name > Delete vllp port

Parameter: if name is the agreed layer-2 interface name (for example: GE1 / 1, trunk1...)

Default: vllp protocol is not applied on the layer 2 port. When the layer-2 interface is a trunk member, vllp protocol cannot be applied.

1.140.4 Configure vllp device priority

Mode: vllp configuration mode

Command: vllp priority < priority > Configure vllp device priority

Command: no vllp priority [priority] Restore vllp device priority to default

Parameter: priority value is between 1 and 255. Priority is used for vllp devices to elect recipients.

Default: 100

1.140.5 Configure vllp device query timer interval

Mode: vllp configuration mode

Command: vllp query interval < interval > Configure local query timer interva

Command: no vllp query interval [interval] The recovery query timer interval is the default value

Parameter: interval value is between 1 and 255. When the vllp device is the sender or migrated back to the sender, the configuration value will take effect.

Default: 5 seconds

1.140.6 Configure attached VLANs

Mode: vllp configuration mode

Command: vllp dependency < if name > Configure attached VLANs

Command: no vllp dependency < if name > Delete attached VLAN

Parameter: if name is the agreed three-tier interface name (for example: vlan1, vlan2...)

Default: no attached VLANs are configured

1.140.7 Configure vllp port priority

Mode: vllp configuration mode

Command: vllp port < if name > priority < priority > Configure vllp port priority

Command: no vllp port < if name > priority [priority] Restore vllp port priority to default

Parameter: if name is the agreed layer-2 interface name (for example: GE1 / 1, trunk1...); The value of priority is between 1 and 255. Priority is used by vllp senders to select the primary port.

Default: 100

1.140.8 display information

Mode: normal mode or privileged mode

Command: show vllp

Displays the vllp device list of the vllp protocol

Command: show vllp < if name >

Displays the details of a vllp device

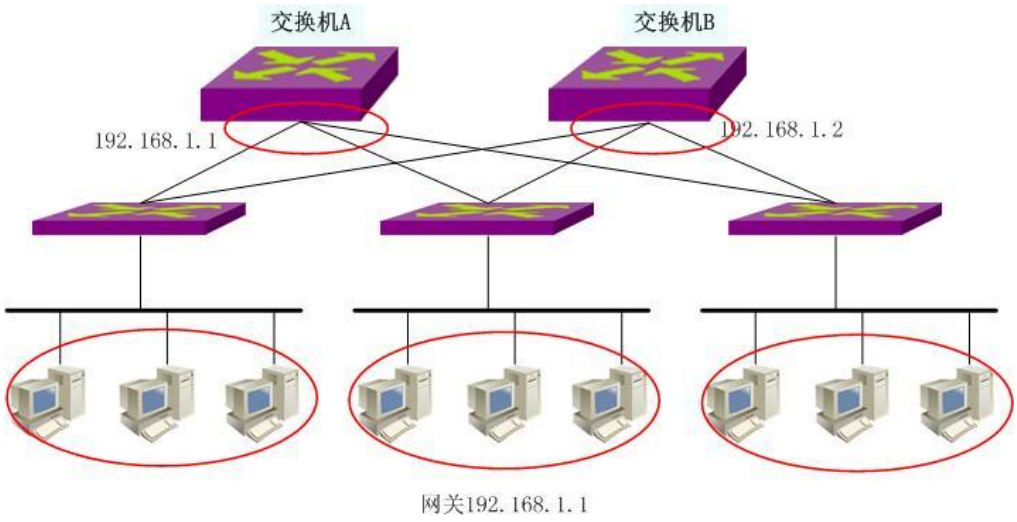
Parameter: if name is the agreed three-tier interface name (for example: vlan1, vlan2...)

Command: show vllp map

Displays the mapping relationship of each vllp port in the vllp protocol

1.141 VLLP Configuration example

(1) Configuration



Configuration on switch A

Switch#configure terminal

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

Switch(config)#ip interface vlan 2

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport access vlan 2

Switch(config-ge1/1)#interface ge1/2

Switch(config-ge1/2)#switchport access vlan 2

Switch(config-ge1/2)#interface ge1/3

Switch(config-ge1/3)#switchport access vlan 2

Switch(config-ge1/3)#interface vlan2

Switch(config-vlan2)#ip address 192.168.1.1/24

Switch(config-vlan2)#exit

Switch(config)#router vrrp 1

Switch(config-vrrp)# virtual-ip 192.168.1.1 master

Switch(config-vrrp)#enable

Switch(config-vrrp)#exit

Switch(config)#router vllp vlan2

Switch(config-vllp)#vlllp port ge1/1

Switch(config-vllp)#vllp port ge1/2

Switch(config-vllp)#vllp port ge1/3

Switch(config-vllp)#vllp enable

Configuration on switch B

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config)#ip interface vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#switchport access vlan 2
Switch(config-ge1/3)#interface vlan2
Switch(config-vlan2)#ip address 192.168.1.2/24
Switch(config-vlan2)#exit
Switch(config)#router vrrp 1
Switch(config-vrrp)# virtual-ip 192.168.1.1 backup
Switch(config-vrrp)#virtual-interface vlan1
Switch(config-vrrp)#enable
Switch(config-vrrp)#exit
Switch(config)#router vllp vlan2
Switch(config-vllp)#vlllp port ge1/1
Switch(config-vllp)#vllp port ge1/2
Switch(config-vllp)#vllp port ge1/3
Switch(config-vllp)# enable
```

(2) verification

Use the following command to view vllp information：

```
show vllp
show vllp <if-name>
show vllp map
```

Configure policy routing

This chapter mainly includes the following contents：

- Introduction to policy routing
- Policy routing configuration
- Example of policy routing configuration

1.142 Introduction to policy routing

Policy based route is a mechanism for routing according to the policies formulated by users. Different from forwarding simply by looking up the routing table according to the destination address of the IP message, the policy routing is set based on some attributes in the message information, such as destination address, source address and other information. Enrich router routing knowledge。

1.143 Policy routing configuration

Configuration includes the following:：

Create a new policy route

Insert a policy rout

Delete a policy rout

Move a policy route

View policy routing information

1.143.1 Create a new policy route

The following command creates a new policy route in global configuration mode:

policy route <ID> <SIP> <DIP> <next-hop>

ID: indicates the newly created policy routing rule ID, ranging from 1 to 100.

Sip, dip: there are three input methods for source and destination IP:

1) A.b.c.d wildcard can control the IP address from a network segment;

2) Any is equivalent to a.b.c.d 255.255.255.25

3) Host a.b.c.d is equivalent to a.b.c.d 0.0.

Wildcard: decide which bits need to be matched, '0' means to be matched, '1' means not to be matched

Next hop: indicates the host address of the next hop. The format is a.b.c.d

1.143.2 Insert a policy route

The following command inserts a new policy route in global configuration mode

policy route insert <ID> <SIP> <DIP> <next-hop> before <EXIST_ ID>

ID: indicates the newly inserted policy rule ID, ranging from 1 to 100.

Sip, dip: there are three input methods for source and destination IP:

1) A.b.c.d wildcard can control the IP address from a network segment

2) Any is equivalent to a.b.c.d 255.255.255.255

3) Host a.b.c.d is equivalent to a.b.c.d 0.0.0

Wildcard: decide which bits need to be matched, '0' means to be matched, '1' means not to be matched.

Next hop: indicates the host address of the next hop. The format is a.b.c.d

EXIST_ ID: indicates which rule to insert before, range 1-100。

1.143.3 Delete a policy route

The following command deletes a policy route in global configuration mode:

no policy route <ID>

ID: indicates the ID of the policy rule to be deleted, ranging from 1 to 100。

1.143.4 Move a policy route

The following command routes the mobile policy to the destination in the global configuration mode:

policy route move <ID> (before|after) <TO_ ID>

ID: indicates the rule to be moved.

(before|after): indicates before or after the moving target rule：

1.143.5 View policy routing information

The following commands are executed in normal mode or privileged mode to view all policy routing information：

show policy route

1.144 Example of policy routing configuration

Configure the source IP address as 192.168.3.100 and use the gateway of 192.168.0.20.

Switch#configure terminal

Switch#(config)#policy route 1 host 192.168.3.100 any 192.168.0.20

Configure the destination IP address as 192.168.10.100 and use the gateway of 192.168.2.1.

Switch#configure terminal

Switch#(config)#policy route 2 any host 192.168.10.100 192.168.2.1

Configure the source IP address as 192.168.3.100 and the destination IP address as 10.10.10.100. Go to the gateway of 192.168.5.1.

Switch#configure terminal

Switch#(config)#policy route 3 host 192.168.3.100 host 10.10.10.100 192.168.5.1

Configure system log

This chapter mainly includes the following contents：

- Introduction to system log
- System log configuration

1.145 Introduction to system log

The system log module is an important part of the switch. It is used to record the operation of the whole system, abnormal behavior and user operation behavior, and help the administrator understand and monitor the working condition of the system in time. The system log module manages all the log information of the system from the running modules, collects, classifies, stores, displays and outputs the log information

In the logging system, there is also an important function of debugging. With the cooperation of system log and debugging, it can help administrators or other technicians monitor the operation of the network, debug and diagnose the faults in the network. The administrator can easily select the content to be debugged, and locate and solve the equipment or network faults by observing the log information output by debugging.

This section mainly includes the following contents:：

- Format of log information
- Storage of logs
- Display of logs
- Debugging tool

1.145.1 Format of log information

The format of log information is as follows:

Timestamp priority: module name: log content

There is a space between timestamp and priority, a colon and a space between priority and module name, and a colon and a space between module name and log content.

An example of the format of log information is as follows:

2006/05/20 13:56:34 Warning: MSTP: Port up notification received for port ge1/2

In this log message, the timestamp is 2006 / 05 / 20 13:56:34; The priority is warning; Module name is MSTP; The log content is port up notification received for port GE1 / 2.

1) Time stamp

Format of timestamp: year / month / day hour: minute: second.

The 24-hour system is adopted, from 0 to 23.

The timestamp records the generation time of this log information and uses the system time of the switch. The system time has been set when the switch leaves the factory and can be modified by the administrator. The system time can still run after the equipment is powered off.

2) Priority

Priority records the importance of this log information. According to the importance of the log information, the log information is divided into four levels. The order of priority from high to low is: critical, warning, informational and debugging. The priority is described in the following table：

priority	describe
Critical	Serious error
Warning	General errors, warnings, very important tips
Informational	Important tips, general tips, diagnostic information
Debugging	debug information

3）Module name

The module name records the module generated by this log information. The following table lists some main modules that generate log information：

Module name	describe
CLI	Command line interface module
MSTP	Multi instance spanning tree protocol module
VLAN	VLAN functional module
ARP	ARP functional module
IP	IP functional module
ICMP	ICMP functional module
UDP	UDP functional module
TCP	TCPfunctional module

4）Log content

The log content is a phrase or sentence that represents the main idea of the log information. The administrator can know what happened to the system by reading the log content。

1.145.2 Storage of logs

There are three ways to store logs:：

- Logs are stored in memory。
- Log stored in NVM。
- Logs are stored in the server。

According to the priority of logs, there are four log tables in memory. Each table stores log information of one priority, that is, the logs are divided into four categories according to the priority of logs, and each type of logs is stored in a separate log table. Each log table has 1K entries, which can store 1K log information. When the log table is full, the subsequent logs cover the log information with the longest time. There is a problem with this storage method. When the system is restarted, these log information is gone. The administrator can't see the log information and locate the problem when the system crashes.

For important log information, such as critical and warning log information, these log information can be stored in the NVM of the system. After the system is restarted, the log information in NVM can be retained, which is convenient for the administrator to locate the problem when the system crashes. However, one problem with this storage method is that due to the capacity limitation of NVM, the log information entries stored in NVM are very limited

Another good way is to store the log information in the server. It can be realized by using syslog protocol. The log information can be sent to the server in real time. The server saves these log information and displays it on an interface. This storage method is not only convenient for users to view log information, but also has a huge capacity, which can store a large amount of log information on the server.

At present, the system only supports storing log information in memory, not in NVM or server。

1.145.3 Display of logs

There are two ways to display logs: manual display and real-time display. Manual display means that the user displays the log information by entering commands. Real time display means that when the log information is generated, the log information is directly output to the terminal, and the user can see it in time.

For the manual display mode, users can view all log information. The display order of log information is that the last generated log information is placed in the front, so that users can see the recent operation status of the switch first.

For the real-time display mode, the user must turn on the real-time display switch of the terminal. If the switch is on, the generated log information is not only written into the log table, but also output to the terminal. If the switch is off, the log information will not be displayed on the terminal in real time. At present, the system can only output the log information to the console terminal in real time, and does not support outputting the log information to the telnet terminal。

1.145.4 Debugging tool

Debugging is a diagnostic tool for equipment and network. It can track the data packet sending and receiving of the system and module, the change of the state machine of the module, etc., so that the administrator can understand and monitor the operation process of the system and module. If there are abnormal conditions in the network or equipment, it can be tracked through the debugging tool.

The debugging tool provides a wealth of switches. By controlling these switches, administrators can track what they are interested in. When an exception occurs in the device or network, the administrator can turn on the debugging switch related to the exception and find the problem by tracking the execution process of the system and module.

When a debugging switch is turned on, the system will generate relevant log information, which will be written to the corresponding log table. Generally, the priority of log information generated by debugging is informational. When the terminal real-time display switch is turned on, these log information will be output to the terminal in real time. When the debugging switch is turned off, the system will not generate relevant log information。

1.146 System log configuration

The system log configuration includes the following:：

- Configure terminal real-time display switch
- View log information
- Configure debugging switch
- View debugging information

1.146.1 Configure terminal real-time display switch

By default, the real-time display switch of the terminal is off, and the log information generated by the system is written into the log table, but will not be displayed on the terminal in real time. Some log information in the system is not limited by this switch. These log information will always be output to the console terminal in real time.

At present, the switch can only display log information in real time on the console terminal, but can not display log information in real time on the telnet terminal.

When the user uses the write command to store the current system configuration in the configuration file, the configuration of the terminal real-time display switch will not be stored in the configuration file of the system. After the system restarts, these configurations will be lost and need to be reconfigured.

The commands for configuring the terminal real-time display switch are shown in the table below：

Command	Description	CLI mode
log stdout	Turn on the terminal real-time display switch。	Global configuration mode
no log stdout	Turn off the terminal real-time display switch。	Global configuration mode

1.146.2 Set log level

The commands for setting the log level are shown in the following table：

Command	Description	CLI mode
log trap <[alerts | critical | debugging | emergencies | errors | informational | notifications | warnings]>	Set log level	Global configuration mode

1.146.3 View log information

The commands for viewing log information are shown in the following table：

Command	Description	CLI mode
show log	Show all log information。	Global configuration mode

1.146.4 Configure debugging switch

The system provides a wealth of debugging switches, involving multiple modules. Only the schematic commands of each module are listed here. For the complete format of the commands, see the command manual.

When the user uses the write command to store the current system configuration in the configuration file, the configuration of the debugging switch will not be stored in the configuration file of the system. After the system restarts, these configurations will be lost and need to be reconfigured.

The schematic commands for configuring the debugging switch are as follows：

Command	Description	CLI mode
debug ip …	Turn on the debugging switch related to the system sending and receiving IP packets.	Privileged mode
no debug ip …	Turn off the debugging switch related to the system sending and receiving IP packets.	Privileged mode
debug ip icmp …	Turn on the debugging switch related to sending and receiving ICMP packets.	Privileged mode
no debug ip icmp …	Turn off the debugging switch related to sending and receiving ICMP packets.	Privileged mode
debug ip arp …	Turn on the debugging switch related to sending and receiving ARP packets.	Privileged mode

no debug ip arp …	Turn off the debugging switch related to sending and receiving ARP packets.	Privileged mode
debug ip udp …	Turn on the UDP packet sending and receiving related switch.	Privileged mode
no debug ip udp …	Turn off the debugging switch related to UDP packets sent and received by the system.	Privileged mode
debug ip tcp …	Turn on the debugging switch related to the system sending and receiving TCP packets.	Privileged mode
no debug ip tcp …	Turn off the debugging switch related to sending and receiving TCP packets.	Privileged mode
debug mstp …	Turn on the debugging switch related to MSTP protocol diagnosis.	Privileged mode
no debug mstp …	Turn off the debugging switch related to MSTP protocol diagnosis.	Privileged mode
debug igmp snooping …	Turn on the debugging switch related to IGMP snooping function diagnosis.	Privileged mode
no debug igmp snooping …	Turn off the debugging switch related to IGMP snooping function diagnosis.	Privileged mode
debug dhcp snooping …	Turn on the debugging switch related to DHCP snoopin protocol diagnosis	Privileged mode
no debug dhcp snooping …	Turn off the debugging switch related to DHCP snoopin protocol diagnosis	Privileged mode
no debug all	Turn off all debugging switches of the system.	Privileged mode

1.146.5 View debugging information

The command to view debugging information is as follows：

Command	Description	CLI mode
show debugging [dhcp snooping | erps | igmp snooping | ip | mstp | rip]	Check the debugging switch configuration. If no parameters are entered, view the debugging switch configuration of all modules. If only one parameter is entered, view the debugging switch configuration of only one module. If the input parameter is IP, the debugging switch configuration of IP, ICMP, ARP, UDP and TCP modules will be checked.	Normal mode / privileged mode

1.147 Configure SYSLOG

SYSLOG includes the following:：

- SYSLOG introduction
- SYSLOG configuration
- SYSLOG configuration example

1.147.1 SYSLOG introduction

Syslog is a standard protocol for equipment log information management, which has been widely used because of its simple design. The syslog system is divided into three parts. One is to define each sub module to distinguish the log information

generated by different modules; Define different log information levels to observe the health of the device. Various log information of the equipment is collected according to this agreement. The second is the configuration file, which defines how to handle the collected log information. It can be saved locally, sent to the designated server on the network, distributed to the designated login users, etc; The configuration file determines how to save the log information generated by the device. The third is to send syslog protocol message according to the message format defined by RFC. It can be seen that in our switch system, the working convention of the whole syslog is the system log module. The first part of syslog protocol is completed by each functional sub module in the switch, and sends each level of log information to the system log module. Maintain four levels of log tables in the system log module. The second part of syslog protocol distributes log information uniformly by the system log module. First, it is displayed on the serial port terminal in real time or manually through the terminal display switch; Second, save four levels of log tables in memory; Third, save high-level log information on NVM to avoid losing important log records in case of power failure; Fourth, send the log to the remote server through syslog message for storage, collection and sorting. The syslog sub module in the system log module only realizes the third part of the function and transmits the system log to the server。

1.147.2 SYSLOG configuation

SYSLOGThe configuration command contains：

- Open syslog server address
- Close syslog server address
- Open syslog protocol

Command	Description	CLI mode
syslog open <server-ip>	Open syslog server address; The parameter server IP is the server IP address	Global configuration mode
syslog close	Close syslog server address	Global configuration mode
log syslog	Open syslog protocol	Global configuration mode

1.147.3 SYSLOG configuration example

（1） Configuration

Configure the syslog server IP address as 192.168.0.201, and configure the switch as follows：

Switch#configure terminal

Switch(config)#syslog open 192.168.0.201

Switch(config)# log syslog

（2） Verfication

Switch#show syslog

Syslog is opened!

server ip address: 192.168.0.201

udp destination port: 514

severity level: debugging

local device name: switch

IPv6 Basic configuration

The switch supports basic IPv6 functions, including IPv6 layer 2 Forwarding and IPv6 nd functions. This chapter describes how to configure IPv6, mainly including the following contents：

- IPv6 introduction
- Configure IPv6 basic functions
- Configure IPv6 Neighbor Discovery Protocol
- Display and maintenance of IPv6

1.148 IPv6 introduction

IPv6 (Internet Protocol version 6) is the second generation standard protocol of network layer protocol, also known as IPng (IP next generation). It is a set of specifications designed by IETF (Internet Engineering Task Force) and an upgraded version of IPv4. The most significant difference between IPv6 and IPv4 is that the length of IP address increases from 32 bits to 128 bits。

1.148.1 IPv6 Protocol features

1 Simplified header format

By reducing or moving some fields in IPv4 message header to extended message header, the length of IPv6 basic message header is reduced. IPv6 uses a fixed length of basic message header, which simplifies the processing of IPv6 messages by forwarding equipment and improves the forwarding efficiency. Although the length of IPv6 address is four times that of IPv4 address, the length of IPv6 basic message header is only 40 bytes, which is twice the length of IPv4 message header (excluding option field)。

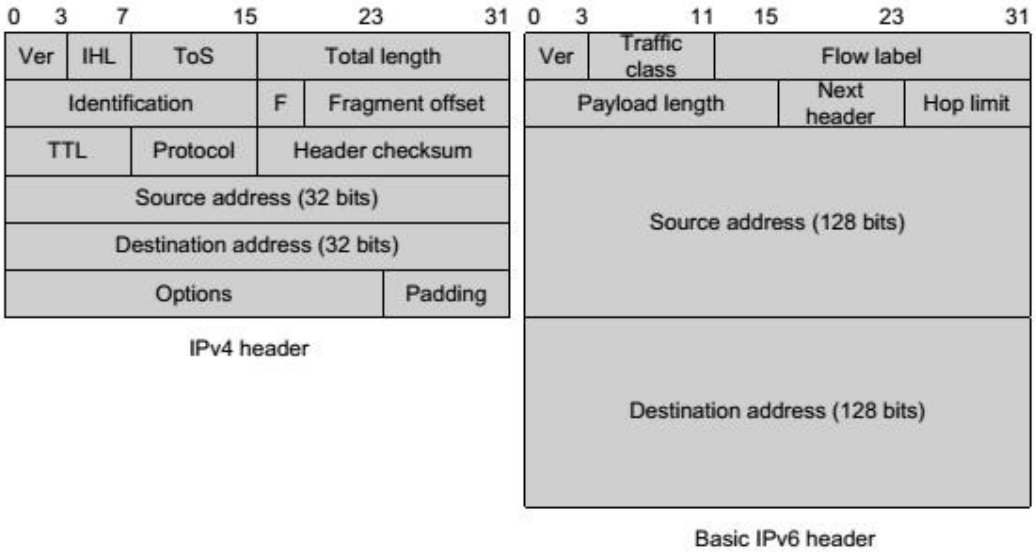


Figure 1-1 format comparison of IPv4 message header and IPv6 basic message header

2 Sufficient address space

The length of source address and destination address of IPv6 is 128 bits (16 bytes). It can provide more than 3.4 × 1038 possible address spaces can fully meet the needs of multi-level address division and address allocation of public networks and private networks within institutions。

3 Hierarchical address structure

The address space of IPv6 adopts a hierarchical address structure, which is conducive to fast route search. At the same time, with the help of route aggregation, it can effectively reduce the system resources occupied by IPv6 route table。

4 Address auto configuration

In order to simplify host configuration, IPv6 supports stateful address configuration and stateless address configuration:

1) Stateful address configuration refers to obtaining IPv6 address and related information from server (such as DHCP server)

2) Stateless address configuration refers to that the host automatically configures IPv6 address and related information according to its own link layer address and prefix information published by the router.

At the same time, the host can also form a link local address according to its own link layer address and default prefix (fe80:: / 10) to realize communication with other hosts on the link。

5 Built in security

IPv6 takes IPSec as its standard extension header, which can provide end-to-end security features. This feature also provides a standard for solving network security problems and improves the interoperability between different IPv6 applications。

6 Support QoS

The flow label field of IPv6 message header realizes the identification of traffic, allowing the equipment to identify the message in a first-class message and provide special processing。

7 Enhanced neighbor discovery mechanism

The neighbor discovery protocol of IPv6 is realized through a group of ICMPv6 (Internet control message protocol for IPv6) messages, which manages the information interaction between neighbor nodes (i.e. nodes on the same link). It replaces ARP (address resolution protocol), icmpv4 router discovery and icmpv4 redirect messages, and provides a series of other functions。

8 Flexible extended message header

IPv6 cancels the option field in IPv4 message header and introduces a variety of extended message headers, which not only improves the processing efficiency, but also greatly enhances the flexibility of IPv6 and provides good expansion ability for IP protocol. The option field in IPv4 message header is only 40 bytes at most, while the size of IPv6 extended message header is only limited by the size of IPv6 message。

1.148.2 IPv6 Address introduction

1. IPv6 address representation

IPv6 addresses are represented as a series of 16 bit hexadecimal numbers separated by colons (:). Each IPv6 address is divided into 8 groups. The 16 bits of each group are represented by four hexadecimal numbers, and the groups are separated by colons, such as 2001:0000:130f: 0000:0000:09c0:876a:130b.

In order to simplify the representation of IPv6 address, "0" in IPv6 address can be processed in the following ways:

1) The leading "0" in each group can be omitted, that is, the above address can be written as 2001:0:130f: 0:0:9c0:876a:130b.

2) If the address contains two or more consecutive groups with 0, it can be replaced by double colon "::" that is, the above address can be written as 2001:0:130f:: 9c0:876a:130b。

Note:

The double colon '::' can only be used once in an IPv6 address. Otherwise, when

the device converts': 'to 0 to recover the 128 bit address, the number of zeros represented by':: 'cannot be determined。

IPv6 address consists of two parts: address prefix and interface identification. Among them, the address prefix is equivalent to the network number field part in the IPv4 address, and the interface ID is equivalent to the host number part in the IPv4 address.

The address prefix is expressed as IPv6 address / prefix length. The IPv6 address is any of the forms listed above, and the prefix length is a decimal number, indicating how many digits on the left of the IPv6 address are the address prefix。

2 IPv6 address classification

IPv6 mainly has three types of addresses: unicast address, multicast address and anycast address

1) Unicast address: used to uniquely identify an interface, similar to IPv4 unicast address. The data message sent to the unicast address will be transmitted to the interface identified by this address.

2) Multicast address: used to identify a group of interfaces (usually belonging to different nodes), which is similar to the IPv4 multicast address. The data message sent to the multicast address is transmitted to all interfaces identified by this address.

3) Anycast address: used to identify a group of interfaces (usually these interfaces belong to different nodes). The data message sent to the anycast address is transmitted to the interface closest to the source node (measured according to the routing protocol used) in the set of interfaces identified by this address.

There is no broadcast address in IPv6. The function of broadcast address is realized through multicast address.

IPv6 address type is specified by the first few digits of the address (called format prefix). The corresponding relationship between the main address type and format prefix is shown in Table 1-1。

地址类型		格式前缀（二进制）	IPv6 前缀标识
单播地址	未指定地址	00...0 (128 bits)	::/128
	环回地址	00...1 (128 bits)	::1/128
	链路本地地址	1111111010	FE80::/10
	站点本地地址	1111111011	FEC0::/10
	全球单播地址	其他形式	-
组播地址		11111111	FF00::/8
任播地址		从单播地址空间中进行分配，使用单播地址的格式	

Table 1-1 correspondence between address type and format prefix

3 Type of unicast address

There are many types of IPv6 unicast addresses, including global unicast address, link local address and site local address.

1) The global unicast address is equivalent to the IPv4 public network address and is provided to the network service provider. This type of address allows aggregation of routing prefixes, which limits the number of global routing table entries.

2) Link local address is used for communication between nodes on the link in neighbor discovery protocol and stateless automatic configuration. Data messages using the link local address as the source or destination address will not be forwarded to other links.

3) The site local address is similar to the private address in IPv4. The data message using the local address of the site as the source or destination address will not be forwarded to other sites outside the site (equivalent to a private network).

4) Loopback address: unicast address 0:0:0:0:0:0:1 (simplified as:: 1) is called loopback address and cannot be assigned to any physical interface. Its function is the same as the loopback address in IPv4, that is, the node is used to send IPv6 messages to itself.

5) Unspecified address: the address':: 'is called an unspecified address and cannot be assigned to any node. Before the node obtains a valid IPv6 address, the address can be filled in the source address field of the sent IPv6 message, but it cannot be used as the destination address in the IPv6 message。

4 Multicast address

The multicast addresses shown in table 1-2 are reserved multicast addresses for special purposes。

地址	应用
FF01::1	节点本地范围所有节点组播地址
FF02::1	链路本地范围所有节点组播地址
FF01::2	节点本地范围所有路由器组播地址
FF02::2	链路本地范围所有路由器组播地址
FF05::2	站点本地范围所有路由器组播地址

Table 1-2 list of reserved IPv6 multicast addresses

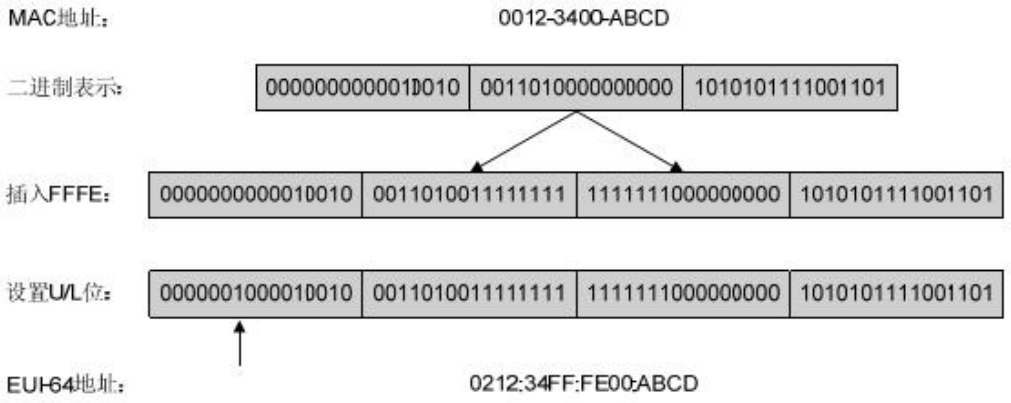
In addition, there is another kind of multicast address: the address of the solicited node. This address is mainly used to obtain the link layer address of neighbor nodes on the same link and realize duplicate address detection. Each unicast or anycast IPv6 address has a corresponding requested node address. The format is:

FF02:0:0:0:0:1:FFXX:XXX

Ff02:0:0:0:0:1: FF is a 104 bit fixed format; 20: XXXX is the last 24 bits of unicast or anycast IPv6 address。

5 IEEE EUI-64 Interface identifier in format

The interface identifier in the IPv6 unicast address is used to identify a unique interface on the link. At present, IPv6 unicast addresses basically require the interface identifier to be 64 bits. The interface identifier in IEEE eui-64 format is changed from the link layer address (MAC address) of the interface. The interface identifier in the IPv6 address is 64 bits, while the MAC address is 48 bits. Therefore, it is necessary to insert the hexadecimal number fffe (1110) in the middle of the MAC address (after the 24th bit from the high bit). In order to ensure that the interface identifier obtained from the MAC address is unique, set the universal / local (U / L) bit (the 7th bit from the high bit) to "1". The final set of numbers is used as the interface identifier in eui-64 format。



conversion process from MAC address to eui-64 format interface identifier

1.148.3 IPv6 Introduction to neighbor discovery protocol

IPv6 neighbor discovery protocol uses five types of ICMPv6 messages to realize the

following functions: address resolution, verifying whether neighbors can reach, duplicate address detection, router discovery / prefix discovery, automatic address configuration and redirection.

The types and functions of ICMPv6 messages used by neighbor discovery protocol are shown in table 1-3。

ICMPv6 消息	类型号	作用
邻居请求消息 NS（Neighbor Solicitation）	135	获取邻居的链路层地址
		验证邻居是否可达
		进行重复地址检测
邻居通告消息 NA（Neighbor Advertisement）	136	对 NS 消息进行响应
		节点在链路层变化时主动发送 NA 消息，向邻居节点通告本节点的变化信息
路由器请求消息 RS（Router Solicitation）	133	节点启动后，通过 RS 消息向路由器发出请求，请求前缀和其他配置信息，用于节点的自动配置
路由器通告消息 RA（Router Advertisement）	134	对 RS 消息进行响应
		在没有抑制 RA 消息发布的条件下，路由器会周期性地发布 RA 消息，其中包括前缀信息选项和一些标志位的信息
重定向消息（Redirect）	137	当满足一定的条件时，缺省网关通过向源主机发送重定向消息，使主机重新选择正确的下一跳地址进行后续报文的发送

Table 1-3 ICMPv6 message types and functions used by neighbor discovery protocol

The main functions provided by neighbor discovery protocol are as follows：

1 Address resolution

Obtain the link layer address of the neighbor node on the same link (the same function as the ARP of IPv4) through the neighbor request message ns and neighbor notification message Na. As shown in Figure 1-3, node a needs to obtain the link layer address of node B。

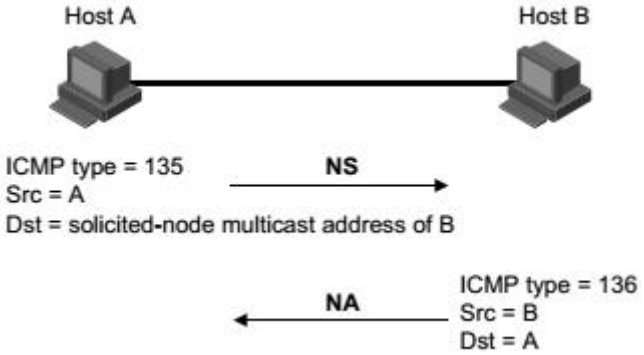


Figure 1-3 schematic diagram of address resolution

(1) Node a sends ns messages by multicast. The source address of NS message is the interface IPv6 address of node a, and the destination address is the multicast address of the requested node of node B. the message content includes the link layer address of node a.

(2) After receiving the NS message, node B determines whether the destination address of the message is the multicast address of the requested node corresponding to its IPv6 address. If yes, node B can learn the link layer address of node A and return Na messages in unicast mode, including its own link layer address.

(3) Node a can obtain the link layer address of node B from the received Na message。

2 Verify neighbor reachability

After obtaining the link layer address of the neighbor node, it can verify whether the neighbor node is reachable through the neighbor request message ns and neighbor notification message Na.

(1) The node sends ns message, where the destination address is the IPv6 address of the neighbor node.

(2) If the confirmation message of the neighbor node is received, it is considered that the neighbor is reachable; Otherwise, the neighbors are considered unreachable。

3 Duplicate address detection

When a node obtains an IPv6 address, it needs to use the duplicate address detection function to determine whether the address has been used by other nodes (similar to the free ARP function of IPv4). Duplicate address detection can be realized through NS and Na, as shown in Figure 1-4。

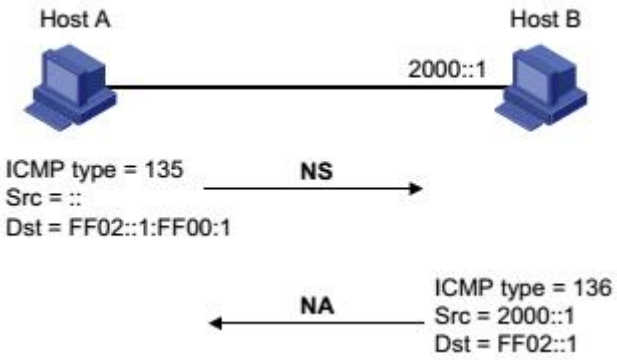


Figure 1-4 schematic diagram of duplicate address detection

(1) Node a sends ns message. The source address of NS message is unspecified address::, and the destination address is the multicast address of the requested node corresponding to the IPv6 address to be detected. The message content contains the IPv6 address to be detected

(2) If node B already uses this IPv6 address, Na message will be returned. It contains its own IPv6 address

(3) When node a receives the Na message from node B, it knows that the IPv6 address has been used. Otherwise, it means that the address is not used, and node a can use this IPv6 address。

4 Router discovery / prefix discovery and automatic address configuration

Router discovery / prefix discovery refers to that the node obtains the prefix of the neighbor router and the network from the received RA message, as well as other configuration parameters.

Address stateless automatic configuration refers to that the node automatically configures the IPv6 address according to the information obtained by router discovery / prefix discovery. Router discovery / prefix discovery is realized through router request message RS and router notification message RA. The specific process is as follows:

1) When the node starts, it sends a request to the router through RS message to request prefix and other configuration information for node configuration.

(2) The router returns RA messages, including prefix information options (the router will also publish RA messages periodically).

(3) The node uses the address prefix and other configuration parameters in the RA message returned by the router to automatically configure the IPv6 address and other information of the interface.

- The prefix information option includes not only the information of the address prefix, but also the preferred lifetime and valid lifetime of the address prefix. After receiving the RA message sent periodically, the node will update the preferred life and effective life of the prefix according to the message.
- Within the valid life, the automatically generated address can be used normally; When the validity period expires, the automatically generated address will be deleted。

5 Redirection function

When the host starts, there may be only one default route to the default gateway in its routing table. When certain conditions are met, the default gateway will send ICMPv6 redirection message to the source host, notifying the host to select a better next hop to send subsequent messages (the same function as the ICMP redirection message of IPv4).

- When the device meets the following conditions, it will send ICMPv6 redirection message for host redirection:
- The interface for receiving and forwarding data messages is the same interface;
- The selected route itself has not been created or modified by ICMPv6 redirection message;
- The selected route is not the default route;
- The forwarded IPv6 data message does not contain the routing extension header。

1.148.4 IPv6 PMTU discovery

The links in the transmission path of the message from the source end to the destination end may have different MTUs. In IPv6, when the length of the message is greater than the MTU of the link, the fragmentation of the message will be carried out at the source end, so as to reduce the processing pressure of the intermediate forwarding equipment and make rational use of network resources.
The purpose of pmtu (path MTU) discovery mechanism is to find the smallest MTU on the path from source to destination. The working process of pmtu is shown in Figure 1-5。

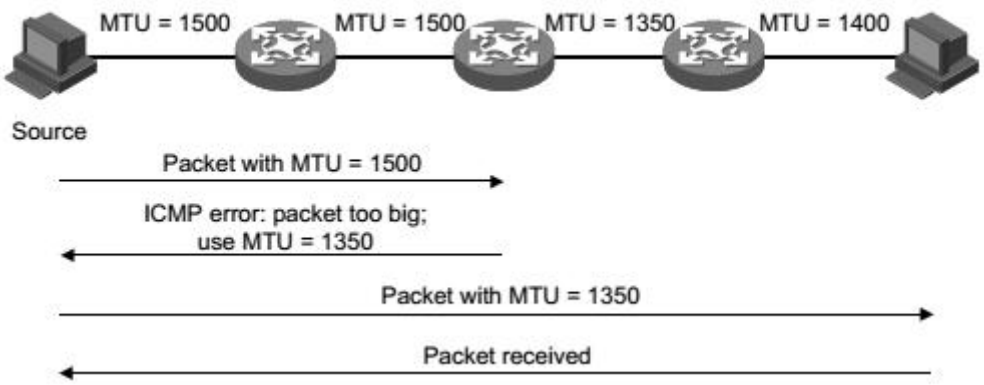


Figure 1-5 pmtu discovery process

(1) The source host uses its own MTU to fragment the message, and then sends the message to the destination host.

(2) When the intermediate forwarding device receives the message for forwarding, if it finds that the MTU value supported by the interface forwarding the message is less than the message length, it will discard the message and return an ICMPv6 error message to the source end, including the MTU of the interface failed to forward.

(3) After receiving the error message, the source host will use the MTU carried in the message to fragment and send the message again.

(4) This is repeated until the destination host receives the message, so as to determine the minimum MTU in the path from the source to the destination。

1.148.5 Protocol specification

The protocol specifications related to IPv6 foundation are：

- RFC 1881：IPv6 Address Allocation Management
- RFC 1887：An Architecture for IPv6 Unicast Address Allocation
- RFC 1981：Path MTU Discovery for IP version 6
- RFC 2375：IPv6 Multicast Address Assignments
- RFC 2460：Internet Protocol, Version 6 (IPv6) Specification.
- RFC 2461：Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2462：IPv6 Stateless Address Autoconfiguration
- RFC 2463： Internet Control Message Protocol (ICMPv6)for the Internet Protocol Version 6
- (IPv6) Specification
- RFC 2464：Transmission of IPv6 Packets over Ethernet Networks
- RFC 2526：Reserved IPv6 Subnet Anycast Addresses
- RFC 3307：Allocation Guidelines for IPv6 Multicast Addresses
- RFC 3513：Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3596：DNS Extensions to Support IP Version 6

1.149 IPv6 Introduction to basic configuration tasks

Configure IPv6 basic function
Configure IPv6 Neighbor Discovery Protocol
Configure pmtu discovery
Configure ICMPv6 message sending Configure IPv6 basic functions

1.149.1 Configure IPv6 unicast address

The IPv6 global unicast address is obtained by manually specifying.
The IPv6 link local address can be obtained in the following two ways:

- Automatic generation: when the VLAN port is up, the device automatically generates the link local address for the interface according to the link local address prefix (fe80:: / 10) and the link layer address of the interface;
- Link: manual IPv6 user configuration。

Command	Description	CLI mode
ipv6 address <ipv6-address>/<prefix-length>	Specify IPv6 address manually. By default, the local address of the link will be automatically generated according to the MAC address of the VLAN interface under the layer 3 interface。	配置模式

1.150 Configure IPv6 Neighbor Discovery Protocol

1.150.1 Configure relevant parameters of RA message

The user can configure whether the interface sends RA message and the time interval of sending RA message according to the actual situation. At the same time, the user can configure the relevant parameters in RA message to notify the host. When the host receives the RA message, it can use these parameters for corresponding operations. The parameters and meanings in configurable RA messages are shown in table 1-4。

Table 1-4 parameters and description in RA message

parameter	describe
（Cur Hop Limit）	When sending IPv6 messages, the host will use this parameter value to fill the hop limit field in the IPv6 message header. At the same time, the parameter value is also used as the hop limit field value in the equipment response message。
（Prefix Information）	After the host on the same link receives the prefix information published by the device, it can perform stateless automatic configuration and other operations.
Managed address configuration flag bit（M flag）	Used to determine whether the host uses stateful automatic configuration to obtain IPv6 address If the flag bit is set to 1, the host will obtain the IPv6 address through stateful automatic configuration (such as DHCP server); Otherwise, the IPv6 address will be obtained through stateless automatic configuration, that is, the IPv6 address will be generated according to its own link layer address and the prefix information published by the router.
Other configuration flag bits（O flag）	It is used to determine whether the host adopts stateful automatic configuration to obtain other information except IPv6 address. If the other configuration flag bit is set to 1, the host will obtain other information except IPv6 address through stateful automatic configuration (such as DHCP server); Otherwise, other information will be obtained through stateless automatic configuration.
Router lifetime （ Router Lifetime）	Used to set the time when the router that publishes RA messages is the default router of the host. According to the router lifetime parameter value in the received RA message, the host can determine whether to take the router that publishes the RA message as the default router.
Neighbor request message retransmission interval（Retrans Timer）	After the device sends the NS message, if it does not receive a response within the specified time interval, it will resend the NS message.
Time to keep neighbors reachable（Reachable Time）	When the neighbor reachability is confirmed through the neighbor reachability detection, the device considers the neighbor reachable within the set reachability time; After the set time is exceeded, if it is necessary to send a message to the neighbor, it will reconfirm whether the neighbor is reachable.
Link maximum transmission unit (Link MTU)	The MTU option is used in the RA message to ensure that all nodes on the link use the same MTU value. It is mainly used when the node may not know the link MTU. Other neighbor discovery messages must be silent. Ignore this option.

Configure hop limit

Command：**ipv6 nd cur-hop-limit** *value*

View mode: VLAN interface mode

Default configuration: by default, the number of hops published by the router is limited to 64 hops

Cancel the suppression of RA message publishing 制

Command：**ipv6 nd send-ra** View mode: VLAN interface mode

Default configuration: by default, RA messages are suppressed from being published

Configure the maximum and minimum time intervals for RA message publishing

Command：**ipv6 nd max-ra-interval** *value*

View mode: VLAN interface mode

Default configuration: by default, the maximum interval between RA messages is 600 secondsCommand：**ipv6 nd min-ra-interval** *value*

View mode: VLAN interface mode

Default configuration: by default, the minimum time interval for RA message publishing is 198 seconds

Note:

- When RA messages are published periodically, the time interval between two adjacent times is to randomly select a value between the maximum time interval and the minimum time interval as the time interval for periodic publication of RA messages。
- The configured minimum time interval should be less than or equal to 0.75 times the maximum time interval。

Configure prefix information in RA messages

Command： **ipv6 nd prefix** X:X::X:X/M (*valid-lifetime preferred-lifetime* (**off-link** | **no-autoconfig**))

View mode: VLAN interface mode

Default configuration: by default, the prefix information in the RA message is not configured. At this time, the IPv6 address of the interface sending the RA message will be used as the prefix information in the RA message。

Set the managed address configuration flag bit

Command：**ipv6 nd managed-config-flag**

View mode: VLAN interface mode

Default configuration: by default, the flag bit of the managed address is 0, that is, the host obtains the IPv6 address through stateless automatic configuration.

Set other configuration flag bits

Command：**ipv6 nd other-config-flag**

View mode: VLAN interface mode

Default configuration: by default, other configuration flag bits are 0, that is, the host obtains other information through stateless automatic configuration

Configure the lifetime of the router in the RA message

Command：**ipv6 nd ra-lifetime** *value*

Figure: VLAN interface mode

Default configuration: by default, the lifetime of the router in the RA message is 1800 seconds.

Configure the retransmission interval of neighbor request message

Command：**ipv6 nd base retrans-timer** *value*

View mode: configuration mode

Default configuration: by default, the interface sends ns messages at an interval of 1000 milliseconds.
Configure the retransmission interval of the router in the RA message
Command：**ipv6 nd retrans-timer** *value*
View mode: VLAN interface mode

Default configuration: by default, the value of the retrans timer field in the RA message published by the interface is 0
Configure the time to keep neighbors reachable
Command：**ipv6 nd base reachable-time** *value*
View mode: configuration mode

Default configuration: by default, the interface keeps the neighbor reachable state for 30000 milliseconds.
Configure the time to keep neighbors reachable
Command：**ipv6 nd reachable-time** *value*
View mode: VLAN interface mode

Default configuration: by default, the value of the reachable timer field in the RA message published by the interface is 0.
Configure link MTU size
Command：**ipv6 nd link-mtu** *value*
View mode: VLAN interface configuration mode

Default configuration: by default, the value of the link MTU field in the RA message published by the interface is 0.

When the source host sends a message from the interface, it will compare the MTU of the interface with the link MTU. If the message length is greater than the minimum of the two, the minimum value will be used to segment the message。

1.150.2 Configure the number of neighbor request messages sent during duplicate address detection

After the interface obtains the IPv6 address, it will send the neighbor request message for duplicate address detection. If no response is received within the specified time (configured through IPv6 nd retrans timer command), it will continue to send the neighbor request message. When the number of times sent reaches the set number, and no response is received, it is considered that the address is available。

Command	Description	CLI mode
ipv6 nd dad attempts <value>	By default, the number of neighbor request messages sent during duplicate address detection is 1. When value is 0, duplicate address detection is prohibited.	Configuration mode

1.151 IPv6 Static routing configuration

Command	Description	CLI mode
ipv6 route <X:X::X:X/M> (<X:X::X:X> | <ifName>) <distance>	Configure IPv6 static routing。	Configuration mode

1.152 IPv6 Display and maintenance

After completing the above configuration, execute the show command in the privileged view to display the operation of IPv6 after configuration, and verify the effect of configuration by viewing the display information.

Command	Description	CLI mode
show ipv6 ndp nc	Display neighbor information。	Privileged mode
show ipv6 interface (<ifName>) brief	Displays the IPv6 information of the interface that can be configured with IPv6 address	Privileged mode
show ipv6 route (database)	Show IPv6 routes	Privileged mode

MLD SNOOPING configuration

In man / Internet, when unicast is used to send the same data packets to multiple rather than all recipients in the network, because it is necessary to copy packets to each receiving endpoint, the number of packets to be sent will increase linearly with the increase of the number of recipients, which will increase the overall burden of hosts, switching routing equipment and network bandwidth resources, Efficiency is greatly affected. With the increasing demand of multi-point video conference, video on demand and group communication applications, multicast has increasingly become a widely used transmission mode in multi-point communication in order to improve resource utilization

The switch implements the MLD snooping function to serve multicast applications. MLD snooping monitors MLD packets on the network and realizes the dynamic learning of IPv6 Multicast MAC address.

This chapter describes the concept and configuration of MLD snooping, mainly including the following contents

MLD snooping introduction

MLD snooping configuration

MLD snooping configuration example

1.153 MLD SNOOPING introduction

In traditional networks, multicast packets are treated as broadcast packets in a subnet, which is easy to cause large network traffic and network congestion. When MLD snooping is implemented on the switch, MLD snooping can dynamically learn IPv6 Multicast MAC address, maintain the output port list of IPv6 Multicast MAC address, and make multicast data flow only sent to the output port, which can reduce network traffic.

This section mainly includes the following contents:

- MLD snooping process
- Layer 2 Dynamic Multicast
- Join a group
- Leave a group

1.153.1 MLD snooping process

MLD snooping is a layer-2 network protocol, which monitors the MLD protocol packets passing through the switch, maintains a multicast group according to the receiving port, VLAN ID and multicast address of these MLD protocol packets, and then forwards these MLD protocol packets. Only the ports that join the multicast group can receive the multicast data stream; This reduces the network traffic and saves the network bandwidth.

Multicast group includes multicast group address, member port, VLAN ID and age time.

The formation of MLD snooping multicast group is a learning process. When a port of the switch receives MLD report packet, MLD snooping will generate a new multicast group, and the port receiving MLD report packet will be added to the multicast group. When the switch receives an MLD query packet, if the multicast group already exists in the switch, the port receiving the MLD query will also join the multicast group, otherwise it will only forward the MLD query packet. MLD snooping also supports the done mechanism of MLD V2; If MLD snooping is configured with fast leave as enable, its receiving port can leave the multicast group immediately when receiving the done packet of MLD V2; If the fast leave timeout is configured, the multicast group will leave the multicast group after the time expires.

MLD snooping has two update mechanisms. One is the done mechanism introduced above. In most cases, MLD snooping deletes expired multicast groups through age time. When the multicast group joins MLD snooping, the joining time is recorded. When the multicast group remains in the switch for more than a configured age time, the exchange opportunity deletes the multicast group.

When a port receives the done protocol packet, the port will be immediately deleted from its multicast group, which may affect the continuity of network data flow; Because a hub or a network device without MLD snooping function may be connected under this port. Many devices receiving multicast data streams are connected under this device. If one device sends done, it may affect other devices and cannot receive multicast data stream. The fast leave timeout mechanism can prevent this from happening. Configure a departure waiting time through fast leave timeout. After receiving the leave packet, the port waits for a long time for fast leave timeout and then deletes it from the multicast group it belongs to, which may ensure the continuity of network multicast flow。

1.153.2 Layer 2 Dynamic Multicast

The multicast MAC address entries in the layer 2 hardware multicast forwarding table

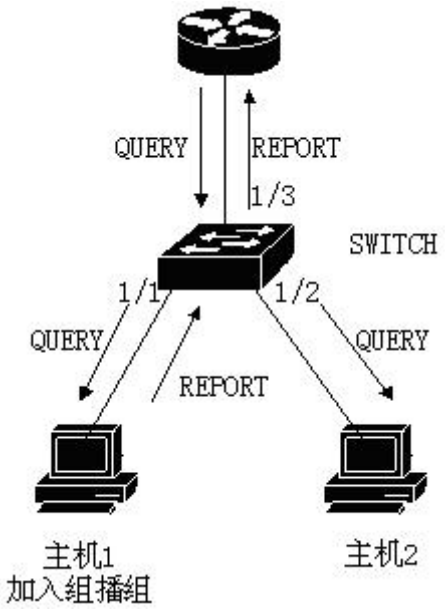
can be obtained through MLD snooping dynamic learning. The IPv6 Multicast MAC address is dynamically learned through MLD snooping.

When the switch turns off MLD snooping, the layer-2 hardware multicast forwarding table is in the unregistered forwarding mode, and the multicast MAC address cannot be dynamically learned. There are no entries in the layer-2 hardware multicast forwarding table, and all layer-2 multicast data streams are treated as broadcast.

When the network has a multicast environment, in order to effectively control the multicast traffic of the network, the switch can turn on MLD snooping. At this time, the layer-2 hardware multicast forwarding table is in the registered forwarding mode. The switch can learn the multicast MAC address by listening to the MLD protocol packet on the network. Only the layer-2 multicast flow matching the entries in the layer-2 hardware multicast forwarding table can be forwarded。

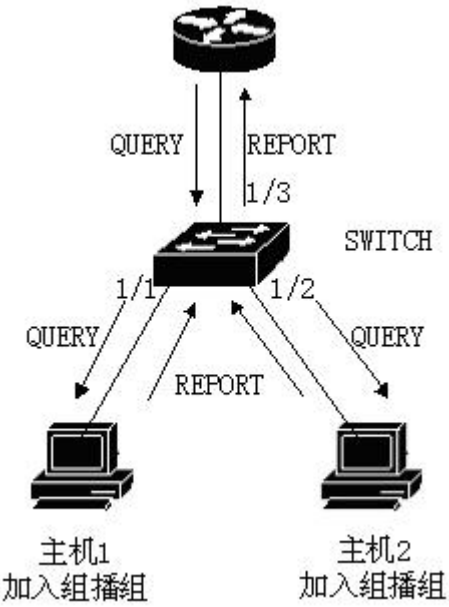
1.153.3 Join a group

When a host wants to join a multicast group, the host will send an MLD report packet, which specifies the multicast group that the host wants to join. When the switch receives an MLD query packet, the switch will forward the packet to all other ports of the same VLAN. When the host under the port wants to join the multicast group receives the MLD query packet, it will return an MLD report packet. When the switch receives an MLD report packet, it will establish a layer-2 multicast entry. The port receiving the MLD query packet and the port of the MLD report packet will be added to the layer-2 multicast entry and become its output port。



As shown in the figure above, all devices are in a subnet, assuming that the VLAN of the subnet is 2. The router runs MLDv2 protocol and sends MLD query packets regularly. Host 1 wants to join the multicast group ff15:: 1. After receiving the MLD query packet from port 1 / 3, the switch will record this port and forward the packet to Ports 1 / 1 and 1 / 2. Host 1 sends back an MLD report packet after receiving the MLD query packet. Host 2 does not send the MLD report packet because it does not want to join the multicast group. After receiving the MLD report packet from port 1 / 1, the switch will forward the packet from query port 1 / 3 and create a layer-2 multicast entry (assuming that the entry does not exist). The layer-2 multicast entry includes the following items:：

Layer 2 multicast address	VLAN ID	Output port list
33:33:00:00:00:01	2	1/1，1/3



As shown in the above figure, the conditions are the same as those in Figure 1. Host 1 has joined the multicast group ff15:: 1, and now host 2 wants to join the multicast group ff15:: 1. When the host 2 receives the MLD query packet and sends back an MLD report packet, the switch will forward the packet from the query port 1 / 3 after receiving the MLD report from port 1 / 2, and the packet port 1 / 2 will be added to the layer 2 multicast entry, and the layer 2 multicast entry becomes：

Layer 2 multicast address	VLAN ID	Output port list
33:33:5e:00:00:01	2	1/1，1/2，1/3

1.153.4 Leave a group

In order to form a stable multicast environment, devices running MLD (such as routers) will send an MLD query packet to all hosts at regular intervals. Hosts that have joined the multicast group or want to join the multicast group will send back an MLD report after receiving the MLD query.

If the host wants to leave a multicast group, there are two ways: active leaving and passive leaving. Active leave means that the host sends an MLD leave packet to the router. Passive leave means that the host does not send back the MLD report after receiving the MLD query sent by the router.

Corresponding to the way the host leaves the multicast group, there are also two ways to leave the layer-2 multicast entry at the port on the switch: timeout leaving and receiving MLD done packet leaving.

When the switch does not receive the MLD report packet of a multicast group from a port for more than a certain time, the port shall be cleared from the corresponding layer-2 multicast entry. If the layer-2 multicast entry has no port, the layer-2 multicast entry shall be deleted.

When the fast leave of the switch is configured as enable, if a port receives the MLD leave packet of a multicast group, the port will be cleared from the corresponding layer 2 multicast entry. If the layer 2 multicast entry has no port, the layer 2 multicast entry will be deleted.

Fast leave is generally used when one port is connected to another host; If there are more than one host under a port, the fast leave timeout waiting time can be configured to ensure the continuity and reliability of multicast streams in the network。

1.154 MLD SNOOPING Configuration

1.154.1 MLD **SNOOPING** default configuration

MLD snooping is off by default, and the layer 2 hardware multicast forwarding table is in unregistered forwarding mode

Fast leave is off by default.

The fast leave timeout time is 300 seconds

The age time of the multicast group report port defaults to 400 seconds.

The age time of multicast group query port is 300 seconds by default。

1.154.2 On and off **MLD SNOOPING**

Open MLD snooping protocol, which can be opened globally or separately; MLD snooping of a VLAN can only be turned on or off when MLD snooping is turned on globally

Open global MLD snooping

Switch#configure terminal

Switch(config)#ipv6 mld snooping

Open MLD snooping of a VLAN

Switch#configure terminal

Switch(config)#ipv6 mld snooping vlan <vlan-id>

Turn off global MLD snooping

Switch#configure terminal

Switch(config)#no ipv6 mld snooping

Turn off MLD snooping of a VLAN

Switch#configure terminal

Switch(config)#no ipv6 mld snooping vlan <vlan-id>

1.154.3 Configure lifetime

Configure multicast group lifetime

Switch#configure terminal

Switch(config)#ipv6 mld snooping group-membership-timeout <interval> vlan <vlan-id>

Interval is in milliseconds.

Configure query group lifetime

Switch#configure terminal

Switch(config)#ipv6 mld snooping query-membership-timeout <interval> vlan <vlan-id>

Interval is in milliseconds。

1.154.4 Configure fast-leave

Start fast leave of a VLAN

Switch#configure terminal

Switch(config)#ipv6 mld snooping fast-leave vlan <vlan-id>

Close fast leave

Switch#configure terminal

Switch(config)#no ipv6 mld snooping fast-leave vlan <vlan-id>

Configure fast leave wait time

Switch#configure terminal

Switch(config)# ipv6 mld snooping fast-leave-timeout <interval> vlan <vlan-id>

Restore the default fast leave wait time

Switch#configure terminal

Switch(config)#no ipv6 mld snooping fast-leave-timeout vlan <vlan-id>

1.154.5 Configure **MROUTER**

Configure static query port

Switch#configure terminal

Switch#interface ge1/6

Switch(config-ge1/6)#ipv6 mld snooping mrouter vlan [vlan-id]

1.154.6 Configure and startup **VLAN querier**

Configure and start the query function of VLAN 1

Switch#configure terminal

Switch(config)#ipv6 mld snooping querier vlan 1

1.154.7 display information

Display MLD snooping configuration information

Switch#show ipv6 mld snooping

Displays the configuration information of a VLAN

Switch#show ipv6 mld snooping vlan <vlan-id>

Display aging information of report multicast group

Switch#show ipv6 mld snooping age-table group-membership

Display aging information of query

Switch#show ipv6 mld snooping age-table query-membership

Display forwarding information of multicast group

Switch#show ipv6 mld snooping forwarding-table

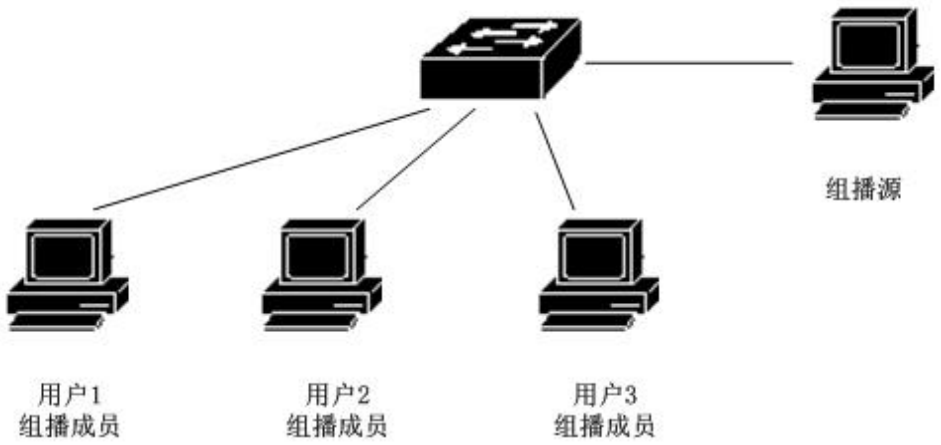
Display mrouter information

Switch#show ipv6 mld snooping mrouter

Displays the current configuration of the system, including the configuration of MLD snoopingSwitch#show running-config

1.155 MLD SNOOPING Configuration example

Enable the MLD snooping function on the switch, and users 1, 2 and 3 can join a specific multicast group。



Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 200

Switch(config)#ipv6 mld snooping

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 200

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 200

Switch(config)#interface ge1/3

Switch(config-ge1/3)#switchport mode access

Switch(config-ge1/3)#switchport access vlan 200

Switch(config)#ipv6 mld snooping group-membership-timeout 60000 vlan 200

POE configuration

The switch supports Poe functions, mainly including the following contents::

- POE introduction
- Configure POE

1.156 POE introduction

POE (power over Ethernet, also known as remote power supply) refers to that the equipment uses twisted pair to connect PD (powered device) equipment (such as IP phone, wireless AP, webcam, etc.) through Ethernet interface for remote power supply。

1. Advantages of Poe

Reliable: centralized power supply, convenient backup

Simple connection: the network terminal does not need external power supply, but only one network cable

Standard: comply with IEEE 802.3af and 802.3at standards, and use the globally unified power interface

Wide application prospects: it can be used for IP phone, wireless AP (access point), portable device charger, card reader, webcam, data acquisition, etc

2. Composition of Poe system

Poe system includes Poe power supply, PSE and PD

Poe power supply

Poe power supply supplies power to the whole Poe system, which is divided into external power supply and built-in power supply

PSE

PSE (power sourcing equipment) is a single board (sub card). Each PSE manages the POE interface in the board (sub card) independently. PSE looks for and detects PD on the line of Poe interface, classifies PD and supplies power to it. When PD pull-out is detected, PSE stops power supply. The Ethernet interface with POE power supply capability is called Poe interface, including Fe and Ge.

PD

PD is a device powered by PSE. It is divided into standard PD and non-standard PD. Standard PD refers to PD equipment conforming to IEEE 802.3af and 802.3at standards. While receiving Poe power supply, PD equipment is allowed to connect other power supplies for power redundancy backup.

1.157 Configure POE

Poe configuration includes the following three parts:

- Manual Poe configuration
- Poe policy configuration
- PD query configuration

1.157.1 Configure POE by hand

The commands for manual Poe configuration are as follows:

- Turn on or off interface Poe power supply
- Display Poe information

Command	Description	CLI mode
[no] poe enable	Turn on or off the interface Poe power supply. The default interface power supply status is on.	Interface configuration mode
show poe	Displays Poe information for all interfaces.	User mode or privileged user mode

1.157.2 POE Policy configuration

The commands for POE policy configuration are as follows:

- Turns on or off the POE policy of the interface
- Set Poe policy entry for interface
- Display Poe policy information

Command	Description	CLI mode
[no] poe policy enable	Open or close the interface Poe policy. The POE policy of the default interface is closed.	Interface configuration mode
[no] poe policy shutdown clock <clock-value> week-day <day-value>	Set or cancel the POE policy entry of the interface. This command can be set multiple times. The POE policy entry is not set by default. Clock value is the time or time range in 24-hour system. If the value is 1, it means 1 point (i.e. between 1 and 2 points), and 20-23 means 20 to 23 points (i.e. between 20 and 0 points). Day value is the day of the week, which means a day or consecutive days. For example, 3 means Wednesday and 1-7 means Monday to Sunday. The POE policy can take effect only when the POE policy of the interface is on.	Interface configuration mode
show poe policy <if-name>	Displays Poe policy information for an interface	User mode or privileged user mode

1.157.3 PDQuery configuration

The commands for PD query configuration are as follows:

- Set the IP address of PD
- Set the time interval for querying PD
- Set the timeout times of PD query

- Set the start time of PD
- Display PD information

Command	Description	CLI mode
poe pd-ip-address <ip-address> no poe pd-ip-address	Set or clear the IP address of the PD connected to the interface. By default, the IP address of the PD is not configured. If the IP address of PD is configured, the system will query this IP address regularly. If PD does not respond for a given number of times, it will restart PD through Poe control.	Interface configuration mode
poe pd-query-interval <interval> no poe pd-query-interval	Set the time interval for querying PD. The default time interval for querying PD is 5 seconds.	Interface configuration mode
poe pd-timeout-number <number> no poe pd-timeout-number	Set the timeout times of querying PD. The default timeout times of querying PD is 3.	Interface configuration mode
poe pd-boot-time <time> no poe pd-boot-time	Set the startup time of PD. The default startup time of PD is 120 seconds.	Interface configuration mode
show poe pd-information	Displays information for all configured PD	User mode or privileged user mode