Industrial Managed Switch
IMS52 series

Configuration Guide

The corresponding software version: release/1.6.0

Document version：V1.0

Release Date：2021.11.1

Content

1. LOG IN TO THE SWITCH CONFIGURATION 5

1.1. CLI 5
1.2. WEB NETWORK MANAGEMENT 8

2. SYSTEM MANAGEMENT 10

2.1. CONFIGURATION SAVE/CLEAR OPERATION 10
2.2. DEVICE HOT RESTART OPERATION 10
2.3. USER LOGIN MANAGEMENT 10
2.4. CONFIGURE SYSTEM NAME 11
2.5. CONFIGURE SYSTEM UPGRADE 12
2.6. CONFIGURE SYSTEM TIME 14

3. CONFIGURE THE INTERFACE 15

3.1. OVERVIEW OF INTERFACE TYPES 15
3.2. CONFIGURATION COMMAND 15
3.3. CONFIGURATION CASE 17
3.4. SHOW COMMAND 18

4. MAC ADDRESS MANAGEMENT 23

4.1. MAC ADDRESS OVERVIEW 23
4.2. CONFIGURATION COMMAND 24
4.3. CONFIGURATION CASE 25
4.4. SHOW COMMAND 25

5. CONFIGURE VLAN 26

5.1. OVERVIEW OF VLAN FUNCTION 26
5.2. CONFIGURATION COMMAND 26
5.3. SHOW COMMAND 28

6. CONFIGURE ERPS 29

6.1. ERPS FUNCTION OVERVIEW 29
6.2. INTRODUCTION TO ERPS PRINCIPLES 30
6.3. CONFIGURATION COMMAND 32
6.4. CONFIGURATION CASE 34
6.5. SHOW COMMAND 47

7. CONFIGURE PORT AGGREGATION 50

7.1. OVERVIEW OF THE AGGREGATION PORT 50
7.2. LACP OVERVIEW 50
7.3. CONFIGURATION COMMAND 51
7.4. CONFIGURATION CASE 52
7.5. SHOW COMMAND 52

8. CONFIGURE SPAN 56

8.1. SPAN OVERVIEW 56
8.2. CONFIGURATION COMMAND 57
8.3. CONFIGURATION CASE 57

8.4. SHOW COMMAND 57

9. CONFIGURE STORM CONTROL 59

9.1. STORM CONTROL OVERVIEW 59
9.2. CONFIGURATION COMMAND 59
9.3. CONFIGURATION CASE 59
9.4. SHOW COMMAND 59

10. CONFIGURE SNMP NETWORK MANAGEMENT 61

10.1. SNMP OVERVIEW 61
10.2. CONFIGURATION COMMAND 63
10.3. CONFIGURATION CASE 66
10.4. SHOW COMMAND 67

11. CONFIGURE RMON 69

11.1. RMON OVERVIEW 69
11.2. RMON RELATED CONCEPTS 70
11.3. CONFIGURATION COMMAND 71
11.4. CONFIGURATION CASE 72
11.5. SHOW COMMAND 73

12. CONFIGURE IGMP SNOOPING 74

12.1. OVERVIEW OF IGMP SNOOPING 74
12.2. CONFIGURATION COMMAND 75
12.3. CONFIGURATION CASE 75
12.4. SHOW COMMAND 76

13. CONFIGURE STP SPANNING TREE PROTOCOL 78

13.1. STP OVERVIEW 78
13.2. CONFIGURATION COMMAND 78
13.3. CONFIGURATION CASE 81
13.4. SHOW COMMAND 85

14. CONFIGURE ACL 86

14.1. ACL OVERVIEW 86
14.2. CONFIGURATION COMMAND 86
14.3. CONFIGURATION CASE 88
14.4. SHOW COMMAND 88

15. CONFIGURE DHCP SNOOPING 89

15.1. OVERVIEW OF DHCP SNOOPING 89
15.2. CONFIGURATION COMMAND 89
15.3. CONFIGURATION CASE 89
15.4. SHOW COMMAND 90

16. CONFIGURE QOS 92

16.1. QOS OVERVIEW 92
16.2. CONFIGURATION COMMAND 92
16.3. CONFIGURATION CASE 95
16.4. SHOW COMMAND 95

17. CONFIGURE QINQ 101

17.1. QINQ OVERVIEW 101
17.2. CONFIGURATION INSTRUCTIONS 101
17.3. CONFIGURATION COMMAND 103
17.4. CONFIGURATION CASE 103
17.5. SHOW COMMAND 106

18. CONFIGURE POE 108

18.1. POE OVERVIEW 108
18.2. CONFIGURATION COMMAND 109
18.3. CONFIGURATION CASE 109
18.4. SHOW COMMAND 109

19. CONFIGURE IP 111

19.1. IP OVERVIEW 111
19.2. DETAILED FUNCTION 111
19.3. CONFIGURATION COMMAND 115
19.4. CONFIGURATION CASE 116
19.5. SHOW COMMAND 120

20. CONFIGURE IPV6 121

20.1. IPV6 OVERVIEW 121
20.2. DETAILED FUNCTION 121
20.3. CONFIGURATION COMMAND 122
20.4. SHOW COMMAND 122

21. CONFIGURE DHCP CLIENT 124

21.1. DHCP CLIENT OVERVIEW 124
21.2. DETAILED FUNCTION 124
21.3. 2.84 CONFIGURATION COMMANDS 126
21.4. CONFIGURATION CASE 127
21.5. SHOW COMMAND 127

22. CONFIGURE DHCP SERVER 129

22.1. DHCP SERVER OVERVIEW 129
22.2. DETAILED FUNCTION 129
22.3. CONFIGURATION COMMAND 133
22.4. CONFIGURATION CASE 137
22.5. SHOW COMMAND 139

23. CONFIGURE 802.1X AUTHENTICATION 143

23.1. PROTOCOL OVERVIEW 143
23.2. CONFIGURATION COMMAND 145
23.3. CONFIGURATION CASE 146
23.4. SHOW COMMAND 148

24. CONFIGURE OUTLET FILTERING 150

24.1. OVERVIEW OF OUTLET FILTRATION 150
24.2. CONFIGURATION COMMAND 150

1. LOG IN TO THE SWITCH CONFIGURATION

1.1. CLI

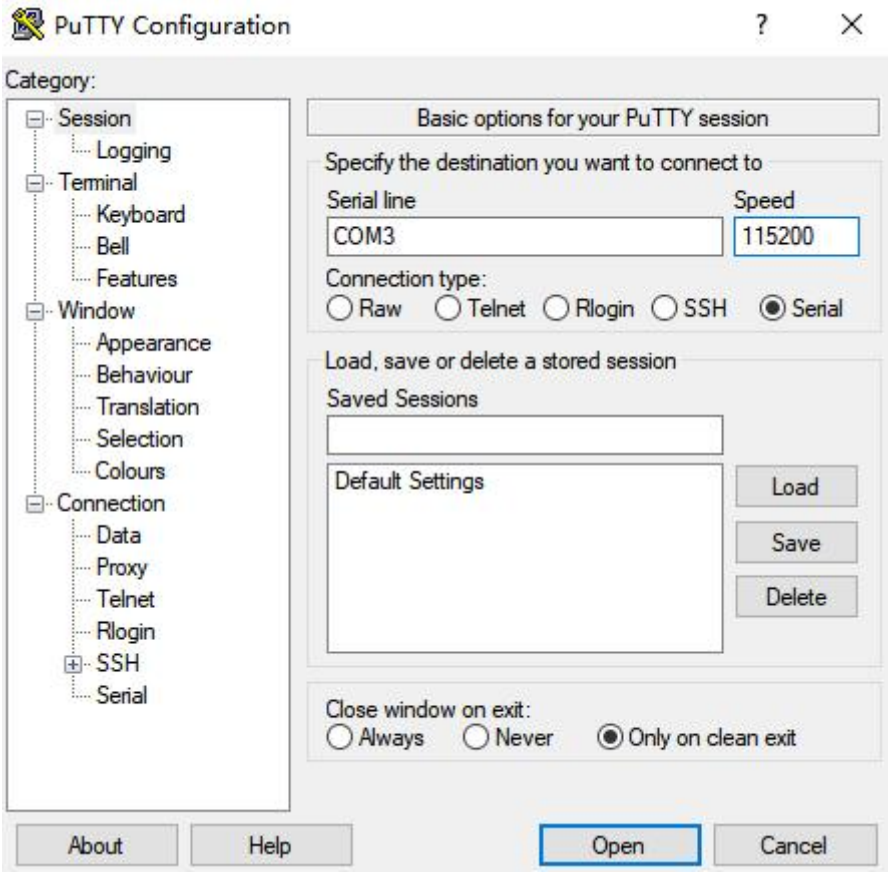
The CLI(command line interface) is a text-type command interactive interface between the user and the device. The user types in a text-type command and submits the device to execute the relevant command by entering the Enter key. Through the command line interface, the user can input commands to configure the device, and can confirm the configuration result by viewing the output information, which is convenient for the user to configure and manage the device.

Administrators can enter the command line interface in a variety of ways:

- Enter the command line interface interface through the Console port
- Enter the command line interface interface through Telnet

1.1.1. Enter the command line interface through the Console port

1. Connect the switch to the PC through the console port cable
2. Open the software that supports serial connection, here is PuTTY as an example.

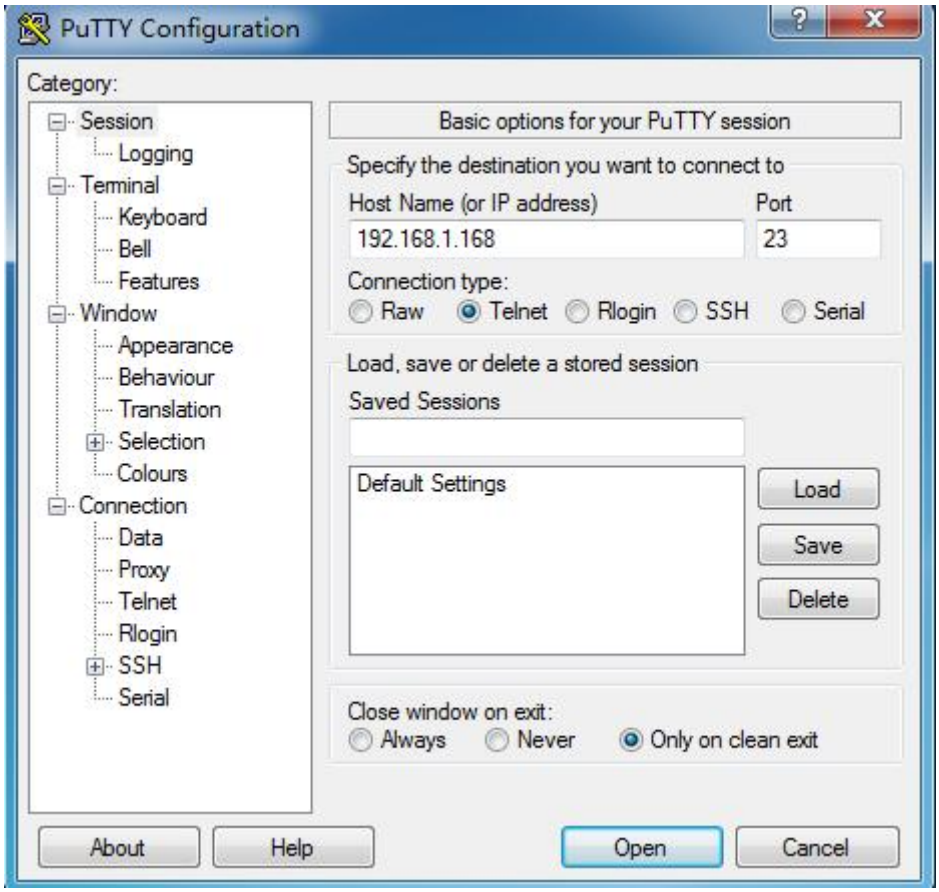


- Choose Serial
- Serial line input the serial device used by the PC
- Speed is modified to 115200 (Console port baud rate)

- Press Enter to enter the login interface. If you cannot log in, please check whether the serial port parameter settings are correct, set the baud rate to 115200, the data bit to 8, the parity check to none, the stop bit to 1, and the flow control to none.
- Log in to the device and enter the user name and password to enter the CLI mode
    - The default user name is admin
    - The default password is admin

1.1.2. Enter the command line interface through Telnet

1. Connect the switch to the PC through a network cable
2. Open the client software that supports telnet, here is PuTTY as an example.



- Choose Telnet
- Host Name Enter the switch management IP address
    - The default management IP is 192.168.1.168
- Press Enter to enter the login interface, enter the user name and password to enter the CLI mode.
    - he default user name is admin
    - The default password is admin

It is recommended that the administrator configure the Telnet service as soon as possible after logging in to the switch for the first time, so that the device can be configured and managed through the remote terminal later.

Enter configuration mode

SWITCH# **configure terminal**

Open the telnet server service

SWITCH(config)# **telnet-server enable**

1.1.3. CLI command line mode

The CLI management interface is divided into several different modes. The current command mode of the user determines the commands that can be used. Enter the question mark key (?) at the command prompt to list the commands supported by each command mode. When a user logs on to the device, it is first in user mode.

Pattern name	Prompt symbol	Switch mode	Mode description
User mode	SWITCH>	Configure enable to switch to privileged mode	Support device information display, debugging command line, etc.
Privileged Mode	SWITCH#	Configure "configure terminal" to switch to global mode; configure "diasble" to switch to user mode	Support network testing; Support function module information viewing; Support configuration save, empty and other operations
Global mode	SWITCH(config)#	Configure "exit" to switch to privileged mode; configure "interface" to switch to interface mode	Support global configuration commands
Interface mode	SWITCH(config-if)#	Configure "exit" to switch to global mode; configure "end" to switch to privileged mode	Support configuration commands in interface mode, interfaces include physical interfaces, aggregation ports, and SVI ports

1.1.4. CLI command line NO command

CLI configuration commands feel that most of the corresponding commands beginning with NO exist, which means that the configuration is deleted or the default operation is restored. After the NO command is input, the question mark key (?) can be input for command reference.

For example: add VLAN 100, delete VLAN 100

```
SWITCH(config)#vlan 100
```

```
SWITCH(config)#no vlan 100
```

1.1.5. Command format description

For the configuration commands in this document, the keywords use bold fonts. Non-keyword parameters are indicated in italics.

In addition, regarding the special symbols in the configuration command, the description is as follows:

Angle brackets, < >: Represents the configurable range of values.

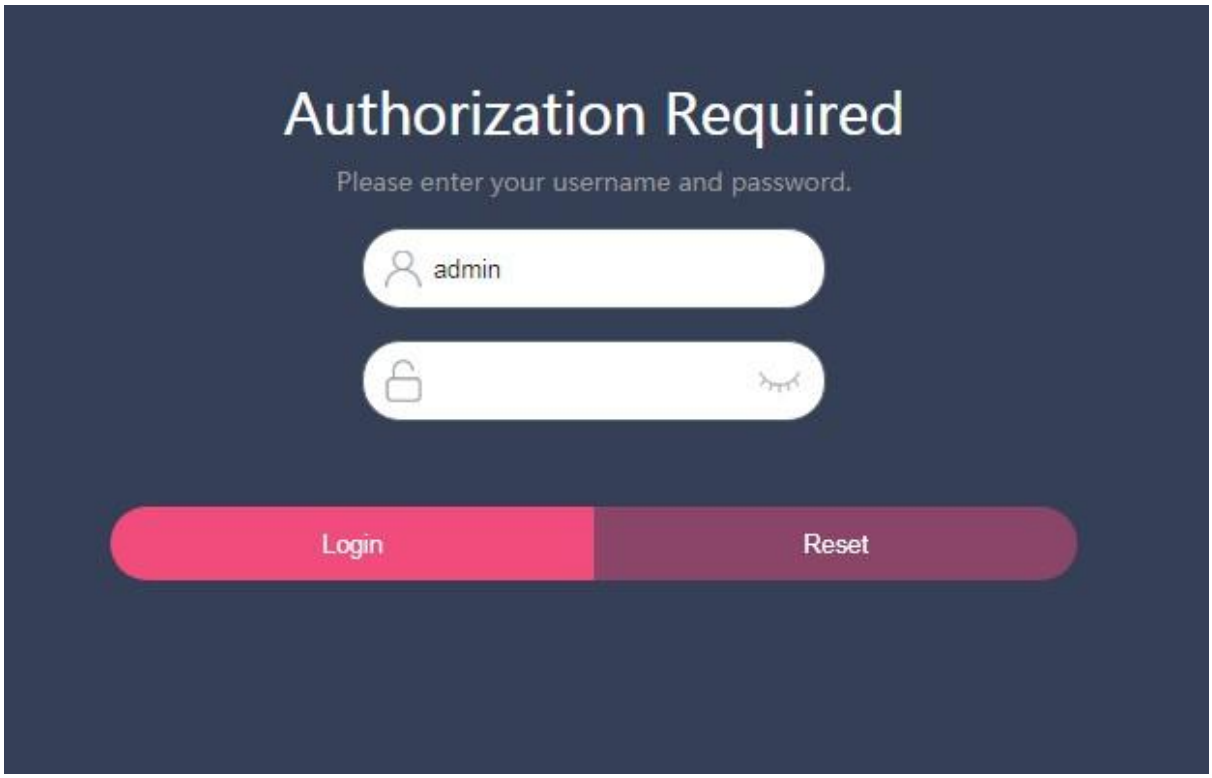
Brackets [ ]: Indicates that the commands in parentheses are optional.

Parentheses (|) : Among them, "|" is used to separate multiple commands, the last position can be empty, and empty means optional, which has the same meaning as square brackets.

Big parantheses {|}: The "|" is used to separate multiple commands. The brackets cannot end with "|". Generally speaking, there must be at least two commands in the braces, which means that at least one command is selected from the two commands, and the order of the commands is irrelevant.

1.2. Web network management

The web server service is enabled by default when the device leaves the factory, and the IP address of the server is 192.168.1.168. The user needs to log in with the default account "admin" when logging in to the web management system for the first time, and the password is also "admin".



All configurations of the web network management operation need to be saved manually (upper right corner of the web network management page), otherwise the configuration will be lost after restarting.

The CLI command to configure the web service is as follows.

Enter configuration mode

SWITCH# configure terminal

Start the Web server service

SWITCH(config)# web-server enable

2. SYSTEM MANAGEMENT

2.1. Configuration save/clear operation

The corresponding web network management configuration path is: Homepage -> Upper right corner -> Save, Homepage -> System -> Configuration file management

Configuration save command
SWITCH#**write**

Save configuration

Restore default configuration command
SWITCH#**copy default-config startup-config**

Restore the system default configuration (to take effect after the device restarts)

2.2. Device hot restart operation

The corresponding web network management configuration path is: Home -> System -> Restart

Configure hot restart commands
SWITCH#**reload**

Device hot restart

2.3. User login management

The corresponding web network management configuration path is: Homepage -> System -> User Management, Telnet Server

Add user, modify user password
SWITCH(config)#**username** NAME **password** LINE

If the user NAME does not exist, add a new user, if it exists, modify the user's password;

The device has its own user "admin" and password "admin" by default, and supports password modification and deletion operations;

The device supports up to 8 users, and the length of the user and password is 0-32 bytes;

Password display adopts encryption method;

Password characters are case sensitive;

The delete operation does not support deleting the user himself;

To delete an online user, you need to kick the user offline before deleting;

Kick online users offline

SWITCH# **clear line (vty | console)** LINE

vty represents the remote login user;

console represents the serial port login user;

LINE information can be viewed in the show users command;

Does not support kicking users themselves;

Does not support operation on the Web network management;

Configure and enable web network management

SWITCH(config)# **web-server enable**

The default "enable" state of the web network management;

Does not support configuration on the Web network management;

Configure and enable Telnet management

SWITCH(config)# **telnet-server enable**

Telnet management default enable state

Show all online users

SWITCH#**show users**

SWITCH#show users

Type	Line	User	Host(s)	Idle	PID
con	0	admin	idle	00:00:03	1932

2.4. Configure system name

The corresponding web network management configuration path is: Homepage -> Basic Information -> Host Name

Configure system name

SWITCH(config)# **hostname** WORD

Set the system name. The name must consist of printable characters and the length cannot exceed 63 bytes;

Configuration takes effect immediately;

2.5. Configure system upgrade

The corresponding web network management configuration path is: Home -> System -> System Upgrade

Configure system upgrade

SWITCH# **upgrade tftp tftp://**SERVER/FILENAME

For firmware upgrade commands, you need to build a TFTP server on the terminal and ensure the two-way interconnection between the terminal and the device network;

SERVER: TFTP server IP and the relative address of the server window and the firmware upgrade file;

FILENAME: firmware upgrade file;

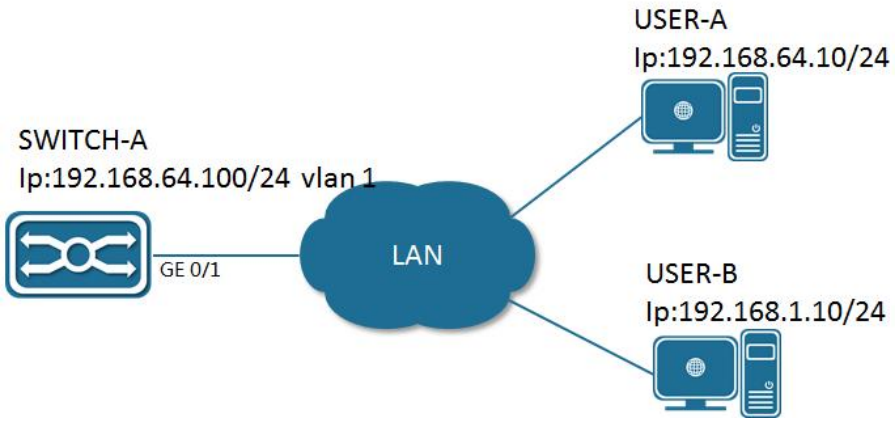
The firmware upgrade process will take 5-6 minutes, restart the device to complete the firmware upgrade;

Do not power off the device during the upgrade process;

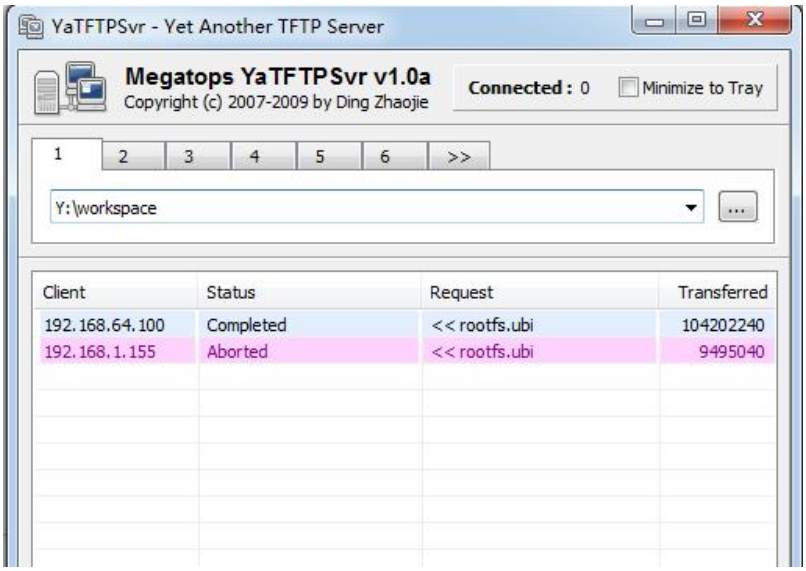
Configuration case

Remote telnet to complete the firmware upgrade operation

- As shown in the figure below, SWITCH-A is the device to be upgraded, and the telnet function is turned on; USER-A is the host in the same network segment in the LAN, and USER-B is the management device in the LAN. Both can Telent to SWITCH-A.



- Select USER-B for version upgrade operation. Open the TFTP server software on USER-B, and put the upgrade file firmware-release-5.1.0.bin in the Y:/workspace directory.



- USER-B telnet to log in to SWITCH-A and execute the upgrade command in privileged mode.

```
SWITCH#upgrade tftp tftp://192.168.5.101/firmware-release-5.1.0.bin
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 68.7M    0 68.7M    0     0   275k      0 --:--:--  0:04:15 --:--:-- 12324
100 68.7M    0 68.7M    0     0   275k      0 --:--:--  0:04:15 --:--:--  275k
Un-packet install file, this will last about 60 seconds.
Check upgrade file success.
Start erase and write bin to flash, this will last about 120 seconds.
Erasing 128 Kibyte @ 43e0000 -- 27 % complete flash_erase: Skipping bad block at 04400000
Erasing 128 Kibyte @ f5e0000 -- 100 % complete
Bad block at 4400000, 1 block(s) from 4400000 will be skipped
Reboot system to finish upgrade? (y/n):
```

- After the upgrade command is executed, select "y" to restart the device to complete the upgrade, and select "n" to continue the operation. The upgrade operation will be completed after the next device restart.

2.6. Configure system time

The corresponding web network management configuration path is: Homepage -> System -> Time and Date

Manually configure the system time

SWITCH# **clock set** HH:MM:SS DAY MON YEAR

Set the system time;

Configuration case

Configured at 15:30: 0 on October 1, 2017

```
SWITCH# clock set 15:30:00 1 october 2017
```

Configure ntp server

SWITCH(config)# **ntp server** A.B.C.D

Configure the IP address of the NTP server (domain name configuration is not supported). After the configuration is complete, if the device maintains network connectivity with the server, the device will automatically synchronize time information from the server. It takes about 4-8 minutes to complete the time synchronization for the first time.

Configure the system time zone

SWITCH(config)# **clock timezone** ZONE

Configure the system time zone, the default is UTC, and support standard time zone configuration, such as Shanghai time zone keyword "Shanghai", Hong Kong time zone keyword "Hong_Kong", etc.

View system time

SWITCH# **show clock**

3. CONFIGURE THE INTERFACE

The corresponding web network management configuration path is: Home -> Interface -> Port Management, Port Statistics, Port Isolation

3.1. Overview of interface types

The interface of the switching equipment can be divided into the following two categories according to the business level: Layer 2 interface and Layer 3 interface.

Layer 2 interface (L2 interface), here includes ordinary physical port (Switch Port) and aggregation port (Port Channel).

The Switch Port is composed of a single physical port on the device and only has the Layer 2 switching function. The port can be an Access Port, Hybrid Port or Trunk Port. You can configure a port as an Access Port, Hybrid Port or Trunk Port through the Switch Port interface configuration command.

Port Channel is abbreviated as PO, which is formed by the aggregation of multiple physical member ports. We can bundle multiple physical links together to form a simple logical link, which we call an aggregation port. For Layer 2 switching, the aggregation port is like a high-bandwidth Switch port, which can superimpose the bandwidth of multiple ports and expand the link bandwidth.

Layer 3 interface (L3 interface), here mainly refers to the SVI (Switch virtual interface) port.

SVI is a switching virtual interface, a logical interface used to implement three-layer switching. SVI can be used as the management interface of this machine, and the administrator can manage the device through the management interface. For details, see the chapter "Configuring IP".

3.2. Configuration command

Configure port range

SWITCH(config)# **interface** GigabitEthernet0/1-4,GigabitEthernet0/9-12

When there are multiple range combinations, separate with ‘,’ in the middle, without spaces;

Support up to 5 range combinations;

When the configuration of a certain port in the middle fails, the configuration is returned, and the subsequent port configuration is not continued;

Configure port descriptor

SWITCH(config-if)# **description** DESCRIPTION

onfigure interface descriptor, up to 80 characters

Configure port closure

SWITCH(config-if)# **shutdown**

Close the port, enabled by default;

Only supports configuration on the physical port;

Configure port rate

SWITCH(config-if)# **speed** (**10 | 100 | 1000| 10000 | auto**)

Configure the port speed. When it is configured as auto or no speed, the port speed enters the auto-negotiation mode;

Default port rate auto-negotiation;

Does not support configuration on aggregate member ports; does not support configuration on SVI ports;

Configure port duplex

SWITCH(config-if)# **duplex** (**auto | full | half**)

Configure the port duplex, when configured to auto or no duplex, the port duplex enters the auto-negotiation mode;

Default port duplex auto-negotiation;

Does not support configuration on aggregate member ports; does not support configuration on SVI ports;

When both the speed and duplex exit the auto-negotiation mode, the port auto-negotiation is closed

Configure port flow control

When the flow control function is enabled on the local switch and the opposite switch, if the local switch is congested:

The local switch will send a message to the opposite switch to notify the opposite switch to temporarily stop sending packets or slow down the speed of sending packets.

After receiving the message, the opposite switch will suspend sending messages to the local end or slow down the speed of sending messages, thus avoiding the occurrence of message loss and ensuring the normal operation of network services.

SWITCH(config-if)# **flowcontrol** (**on | off | auto**)

Configure port flow control, default port flow control auto-negotiation;

Does not support configuration on aggregate member ports; does not support configuration on SVI ports;

Configure port MTU

When a port performs high-throughput data exchange, it may encounter a frame larger than the length of the Ethernet standard frame. This kind of frame is called a jumbo frame. The user can control the maximum frame length allowed to be sent and received by the port by setting the MTU of the port. MTU refers to the length of the valid data segment in the frame, excluding the overhead of Ethernet encapsulation. Frames received or forwarded by the port will be discarded if their length exceeds the set MTU.

SWITCH(config-if)# **mtu** LENGTH

onfigure the port MTU, the allowed range is 64~10240 bytes, the default is 1526 bytes

Does not support configuration on aggregate member ports; does not support configuration on SVI ports;

Configure SFP port mode

By default, the SFP port is in 1000BASE-X mode and can support SFP modules that comply with 1000BASE-X. Some optical modules (some 1000BASE-T SFP modules and some 100BASE-FX SFP modules) use the SGMII protocol, and the ports can be switched to SGMII mode to provide support. The port bandwidth can be increased to 2.5G by configuring the port mode 2500BASE-X, but it only supports specific types of SFP modules provided by our company.

SWITCH(config-if)# **port mode (sgmii | 10gbase-x| 2500base-x| 1000base-x| 100base-fx)**

The default is in 1000base-x mode

sgmii: Configure the port mode as SGMII mode (only supported on optical ports)

10gbase-x: configure port 10g base-x mode, support 10G bandwidth

2500base-x: Configure port 2500 base-x mode, support 2.5G bandwidth

1000base-x: configure port 1000 base-x mode, support 1G bandwidth

100base-fx: configure port 100 base-fx mode, support 100M bandwidth

Only supports configuration on the physical port;

Configure port isolation

In some application environments, it is required that some ports of the device cannot communicate with each other, which can be achieved by setting these ports as isolated ports. When the port is set as an isolated port, the isolated ports cannot communicate with each other, the isolated port and the non-isolated port can communicate normally, and the non-isolated port and the non-isolated port can communicate normally.

SWITCH(config-if)#**switchport isolate**

The default port is a non-isolated port;

The isolation function is not supported on the aggregation port and vlan port;

3.3. Configuration case

The port description information of interface GigabitEthernet0/1 is "TEST_A"

```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#description TEST_A
```

The interface GigabitEthernet0/1 port is closed

```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#shutdown
```

Interface GigabitEthernet0/1 forced port rate 100M, full duplex, open flow control function

```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#speed 100
SWITCH(config-if)#duplex full
SWITCH(config-if)#flowcontrol on
```

Configure interface GigabitEthernet0/1 with a port MTU value of 1024

```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#mtu 1024
```

3.4. Show command

Display brief information of all ports

SWITCH#**show interface brief**

```
SWITCH#show interface brief
Codes: ETH - Ethernet, LB - Loopback , AGG - Aggregate , MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down , NA - Not Applicab
le
       NOM - No operational members , PVID - Port Vlan-id
--------------------------------------------------------------------------------
Ethernet                  Type Status Reason Speed Duplex Flowcontrol Autoneg Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
GigabitEthernet0/1        ETH  up     none   1000M FULL   OFF             ON
--
GigabitEthernet0/2        ETH  down   PD     --    --     --              --   --
GigabitEthernet0/3        ETH  down   PD     --    --     --              --   --
GigabitEthernet0/4        ETH  down   PD     --    --     --              --   --
GigabitEthernet0/5        ETH  down   PD     --    --     --              --   --
GigabitEthernet0/6        ETH  down   PD     --    --     --              --   --
GigabitEthernet0/7        ETH  down   PD     --    --     --              --   --
GigabitEthernet0/8        ETH  down   PD     --    --     --              --   --
GigabitEthernet0/9        ETH  down   PD     --    --     --              --   --
GigabitEthernet0/10       ETH  down   PD     --    --     --              --   --
GigabitEthernet0/11       ETH  down   PD     --    --     --              --   --
GigabitEthernet0/12       ETH  down   PD     --    --     --              --   --
GigabitEthernet0/13       ETH  down   PD     --    --     --              --   --
GigabitEthernet0/14       ETH  down   PD     --    --     --              --   --
```

GigabitEthernet0/15	ETH	down	PD	--	--	--	--	--
GigabitEthernet0/16	ETH	down	PD	--	--	--	--	--
GigabitEthernet0/17	ETH	down	PD	--	--	--	--	--
GigabitEthernet0/18	ETH	down	PD	--	--	--	--	--
GigabitEthernet0/19	ETH	down	PD	--	--	--	--	--
GigabitEthernet0/20	ETH	down	PD	--	--	--	--	--
GigabitEthernet0/21	ETH	down	PD	--	--	--	--	--
GigabitEthernet0/22	ETH	down	PD	--	--	--	--	--
GigabitEthernet0/23	ETH	down	PD	--	--	--	--	--
GigabitEthernet0/24	ETH	down	PD	--	--	--	--	--
TenGigabitEthernet0/25	ETH	down	PD	--	--	--	--	--
TenGigabitEthernet0/26	ETH	down	PD	--	--	--	--	--
TenGigabitEthernet0/27	ETH	down	PD	--	--	--	--	--
TenGigabitEthernet0/28	ETH	down	PD	--	--	--	--	--

Display single port configuration and status information

SWITCH#**show interface** IFNAME

```
SWITCH#show interface GigabitEthernet0/1
Interface GigabitEthernet0/1
  Hardware is ETH  Current HW addr: 0022.3300.0a0a
  Logical:(not set)
  Port Mode is access
  Index 1 metric 0 mtu 1500
  Interface configure:
    Media type: RJ45 mtu: 1500 admin status: no shutdown
    Speed: auto Duplex: auto Flowcontrol: off
  Interface status:
    Link status: UP Bandwidth: 1g
    Speed: 1000M Duplex: full Flowcontrol: off
  input packets:
    Good Octets Rx              : 228042
```

```
    Good Packets Rx          : 1480
    Broadcast Packets Rx     : 109
    Multicast Packets Rx     : 979
  ouput packets:
    Good Octets Tx           : 243972
    Good Packets Tx          : 3811
    Broadcast Packet Tx      : 3419
    Multicast Packet Tx      : 1
  un-normal packets:
    Drop Events              : 0
    Undersized Pkts Recvd    : 0
    Oversized Pkts Recvd     : 0
    Bad CRC                  : 0
```

Display port packet statistics

SWITCH#**show counters interface** IFNAME

```
SWITCH#show counters interface GigabitEthernet0/1
Interface GigabitEthernet0/1
 5 seconds input rate     : 192 bits/sec, 0 packets/sec
 5 seconds output rate    : 200 bits/sec, 0 packets/sec
 Rxload                   : 0.00%
 Txload                   : 0.00%
 Good Octets Tx           : 245572
 Good Octets Rx           : 230000
 Bad Octets Rx            : 0
 Mac Tx Err Pkts          : 0
 Good Packets Tx          : 3836
 Good Packets Rx          : 1491
 Bad Packets Rx           : 0
 Broadcast Packet Tx      : 3443
 Broadcast Packets Rx     : 110
```

```
Multicast Packet Tx          : 1
Multicast Packets Rx         : 988
pkts_64_octets Rx            : 0
pkts_65_127_octets Rx        : 0
pkts_128_255_octets Rx       : 0
pkts_256_511_octets Rx       : 0
pkts_512_1023_octets Rx      : 0
pkts_1024_max_octets Rx      : 0
pkts_64_octets               : 4258
pkts_65_127_octets           : 253
pkts_128_255_octets          : 786
pkts_256_511_octets          : 0
pkts_512_1023_octets         : 30
pkts_1024_max_octets         : 0
Excessive Collisions         : 0
UnRecg MAC Cntl Pkts Rx      : 0
Flow Ctrl Pkts Sent          : 0
Flow Ctrl Pkts Recvd         : 0
Drop Events                  : 0
Undersized Pkts Recvd        : 0
Fragments Recvd              : 0
Oversized Pkts Recvd         : 0
Jabber Pkts Recvd            : 0
mac_rcv_error                : 0
Bad CRC                      : 0
Collisions                   : 0
Late Collisions              : 0
Bad Flow Ctrl Recv           : 0
```

Display port isolation configuration information

SWITCH#**show switchport isolate**

```
SWITCH#show switchport isolate
```

interface	config
GigabitEthernet0/1	normal
GigabitEthernet0/2	normal
GigabitEthernet0/3	normal
GigabitEthernet0/4	normal
GigabitEthernet0/5	normal
GigabitEthernet0/6	normal
GigabitEthernet0/7	normal
GigabitEthernet0/8	normal
GigabitEthernet0/9	normal
GigabitEthernet0/10	normal
GigabitEthernet0/11	normal
GigabitEthernet0/12	normal
GigabitEthernet0/13	normal
GigabitEthernet0/14	normal
GigabitEthernet0/15	normal
GigabitEthernet0/16	normal
GigabitEthernet0/17	normal
GigabitEthernet0/18	normal
GigabitEthernet0/19	normal
GigabitEthernet0/20	normal
GigabitEthernet0/21	normal
GigabitEthernet0/22	normal
GigabitEthernet0/23	normal
GigabitEthernet0/24	normal
TenGigabitEthernet0/25	normal
TenGigabitEthernet0/26	normal
TenGigabitEthernet0/27	normal
TenGigabitEthernet0/28	normal
Port-Channel1	normal

4. MAC ADDRESS MANAGEMENT

The corresponding web network management configuration path is: Home -> Exchange -> MAC Management

4.1. MAC address overview

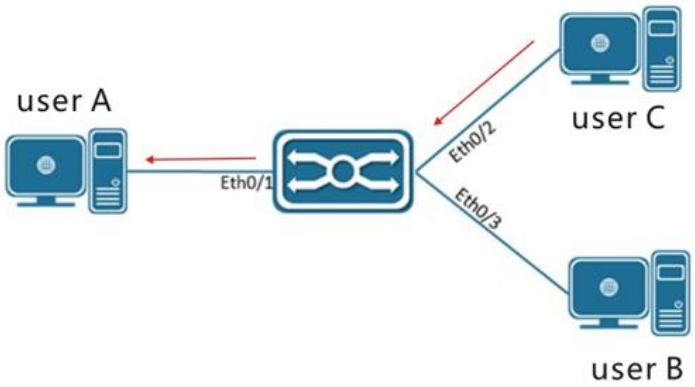
The Ethernet switch queries the MAC address table by analyzing the destination MAC address carried in the message, and sends the message to the corresponding port. The MAC address table records the MAC address, interface, and VLAN ID information of the device connected to the device. The Ethernet switch decides to use the well-known unicast or unknown-name broadcast forwarding method according to the results of the MAC address table search.

Well-known unicast: The Ethernet switch finds the entry corresponding to the destination MAC address and VLAN ID of the message in the MAC address table, and the output port in the entry is unique, and the message is output directly from the port corresponding to the entry .

Unknown broadcast: The Ethernet switch does not find the entry corresponding to the target MAC address in the address table, and the message is sent to all ports except the message input port in the VLAN to which it belongs.

The MAC address of the Ethernet switch can be obtained dynamically or configured statically, and in general, it can be obtained dynamically. Next, by analyzing the interaction process between user A and user C, the working principle of MAC address dynamic learning is given.

User A sends a message to the switch port GigabitEthernet0/1, and the Ethernet switch learns the MAC address of user A into the MAC address table. Since there is no source MAC address of user C in the address table, the Ethernet switch broadcasts the message to all ports belonging to VLAN1 except GigabitEthernet0/1 connected to user A, including the ports of user B and user C. At this time, user B can receive the message sent by user A that does not belong to it.



Current dynamic MAC address table information:

User	VLAN	MAC address	Port
User A	1	000E.C6C1.C8AB	GigabitEthernet0/1

After receiving the message, user B sends the response message to user A through port GigabitEthernet0/2 of the Ethernet switch. At this time, the MAC address of user A already exists in the MAC address table of the Ethernet switch, and the message is unicast The Ethernet switch will learn the MAC address of user C. The difference is that user B cannot receive the message sent by user C to user A at this time.

Current dynamic MAC address table information:

User	VLAN	MAC address	Port
User A	1	000E.C6C1.C8AB	GigabitEthernet0/1
User C	1	000E.C6C1.C8AD	GigabitEthernet0/2

After an interaction process between user A and user C, the device learns the source MAC addresses of user A and user C, and then the message interaction between user A and user C is forwarded in unicast mode. After that, user B will No more interaction messages between user A and user C are received.

4.2. Configuration command

Configure the dynamic MAC address aging time

SWITCH(config)#**mac-address-table aging-time** <0-600>

Configure the MAC address aging time, the range is 0-600 seconds;

The default MAC address aging time is 300 seconds;

When configured as 0, it means that the MAC address aging function is disabled;

Configure static MAC address

SWITCH(config)#**mac-address-table static** MAC_ADDR **vlan** VLANID **interface** IFNAME

When the device receives a packet with MAC_ADDR as the destination address on the VLAN specified by VLANID, the packet will be forwarded to the interface specified by IFNAME;

IFNAME supports physical port and aggregation port;

Configure MAC address filtering

SWITCH(config)#**mac-address-table filter** MAC_ADDR **vlan** VLANID

When the device receives a packet with the address specified by MAC_ADDR as the source or destination address on the VLAN specified by the VLANID, it will be discarded;

Clear dynamic MAC address

SWITCH#**clear mac-address-table dynamic**

SWITCH#**clear mac-address-table dynamic vlan** VLANID

SWITCH#**clear mac-address-table dynamic interface** IFNAME

Support all, VLAN-based, port-based MAC address clearing operations;

4.3. Configuration case

Configure the dynamic MAC address aging time to 60 seconds

```
SWITCH(config)#mac-address-table aging-time 60
```

Configure a static MAC address, all destination MAC addresses are 000E.C6C1.C8AB, and VLAN 1 packets are forwarded from port GigabitEthernet0/1

```
SWITCH(config)#mac-address-table static 000E.C6C1.C8AB vlan 1 interface GigabitEthernet0/1
```

Configure MAC address filtering to discard the packets with the source or destination MAC address of VLAN 1 being 000E.C6C1.C8AB

```
SWITCH(config)#mac-address-table filter 000E.C6C1.C8AB vlan 1
```

Clear the dynamic MAC address under port GigabitEthernet0/1

```
SWITCH#clear mac-address-table dynamic interface GigabitEthernet0/1
```

4.4. Show command

Show MAC address

SWITCH#**show mac-address-table**

```
SWITCH#show mac-address-table
 VLAN       MAC Address       Type        Ports
  -----+---------------+---------+----------------------+
  20       0000.0000.0009    filter      drop
  20       0000.0000.000a    filter      drop
```

Display statistics on the number of MAC addresses

SWITCH#**show mac-address-table count**

```
SWITCH#show mac-address-table count
Static Address Count: 0
Filter Address Count: 2
Dynamic Address Count: 0
```

5. CONFIGURE VLAN

The corresponding web network management configuration path is: Homepage -> Switching -> VLAN

5.1. Overview of VLAN function

VLAN is the abbreviation of Virtual Local Area Network, which is a logical network divided on a physical network. This network corresponds to the second layer of the ISO model. The division of VLAN is not restricted by the actual physical location of the network port. VLAN has the same attributes as a normal physical network, except that it has no physical location restrictions, it is the same as a normal LAN. The unicast, broadcast, and multicast frames of the second layer are forwarded and diffused in a VLAN without directly entering other VLANs.

Port-based VLAN is the simplest method of VLAN division. The user can divide the ports on the device into different VLANs, and then the packets received from a certain port can only be transmitted in the corresponding VLAN, so as to realize the isolation of the broadcast domain and the division of virtual working groups.

The port link types of Ethernet switches can be divided into three types: Access, Trunk, and Hybrid. These three types of ports will process differently when they join a VLAN and when forwarding packets.

Access type: The port can only belong to one VLAN; it is generally used for the connection between the switch and the end user;

Trunk type: A port can belong to multiple VLANs, and can receive and send packets from multiple VLANs, but only Native VLANs can be untagged; generally used for connections between switches;

Hybrid type: The port can belong to multiple VLANs, can receive and send packets of multiple VLANs, and can configure whether the relevant VLAN is tagged with VLAN according to the needs of the user; it can be used for the connection between switches, and it can also be used for connecting users. computer.

5.2. Configuration command

Create VLAN
SWITCH(config)#**vlan** VLAN_RANGE
Configure Access Port
SWITCH(config)#**interface** GigabitEthernet0/1
SWITCH(config-if)#**switchport mode access**
Configure the port type as Access port (by default, the port is Access type).

Configure the VLAN to which the Access port belongs
SWITCH(config-if)#**switchport access vlan** VLANID
Add the current port to the specified VLAN (by default, all Access ports belong to and only belong to VLAN1), and the no command restores the default;

The above command can be used only after the interface has been configured as an access port, and the specified VLAN must have been created;

When configured as non-VLAN 1, if the corresponding VLAN is deleted, it will automatically revert to VLAN 1;

Configure Trunk Port

SWITCH(config)#**interface** GigabitEthernet0/1
SWITCH(config-if)#**switchport mode trunk**
Configure the port type as Trunk port.

Configure Trunk Port Allowed VLAN List

SWITCH(config-if)#**switchport trunk allowed vlan** (**all** | VLAN_LIST | **none**)
Only when the interface has been configured as a trunk port, the above command can be used;
All means automatic mode, which automatically joins all created VLANs (even if it is created later, it will automatically join);
None means clear the Allowed VLAN list, that is, the port does not belong to any VLAN (including Native vlan);
VLAN_LIST means to manually set the Allowed VLAN list. If it was ALL (automatic mode) before, the Allowed VLAN list will be cleared first, and then the VLAN list will be added. VLAN_LIST supports standard multi-vlan representation methods ("-" and "," and a combination of the two);
When the no keyword is added in front, it means to delete the VLAN indicated by VLAN_LIST from the Allowed VLAN list;
When setting all, the maintenance of the Allowed VLAN list is changed to automatic mode, and other commands are changed to manual mode. (By default, it is automatic mode. When switching from other port mode to Trunk port, it is automatic mode).

Only created VLANs can be added to the Allowed VLAN list; when a VLAN is deleted, the corresponding VLAN in the Allowed VLAN list will be deleted automatically.

Configure Trunk Port Native VLAN

SWITCH(config-if)#**switchport trunk native vlan** VLANID

Set the Native VLAN of the Trunk port. (By default, the Native VLAN of the Trunk port is VLAN1), restore the default with the no command;

Only when the interface has been configured as a trunk port, the above command can be used;

The setting of Native VLAN has nothing to do with whether the Allowed VLAN contains this VLAN, or even whether the VLAN is created, that is, the Native VLAN can be set to an uncreated VLAN;

The Native VLAN ID of the trunk port connecting the device and the device must be the same, otherwise the packets of the Native VLAN will not be transmitted correctly

Configure Hybrid port

SWITCH(config-if)#**switchport mode hybrid**
Configure the port type Hybrid to port.

Configure the Allowed VLAN list of the Hybrid port

SWITCH(config-if)#**switchport hybrid allowed vlan** (**all** | VLAN_LIST | **none**)
Only when the interface has been configured as a Hybrid port, the above command can be used;

All means automatic mode, which automatically joins all created VLANs (even if it is created later, it will automatically join);

None means clear the Allowed VLAN list, that is, the port does not belong to any VLAN (including Native vlan);

VLAN_LIST means to manually set the Allowed VLAN list. If it was ALL (automatic mode) before, the Allowed VLAN list will be cleared first, and then the VLAN list will be added. VLAN_LIST supports standard multiple VLAN representation methods ("-" and "," and a combination of the two);

When the no keyword is added in front, it means to delete the VLAN indicated by VLAN_LIST from the Allowed VLAN list;

When setting all, the maintenance of the Allowed VLAN list is changed to automatic mode, and other commands are changed to manual mode. (By default, it is automatic mode. When switching from other port mode to Hybrid port, it is automatic mode);

Only VLANs that have been created can be added to the Allowed VLAN list; when a VLAN is deleted, the corresponding VLAN in the Allowed VLAN list will be automatically deleted;

Configure the default VLAN of the Hybrid port

SWITCH(config-if)#**switchport hybrid vlan** VLANID

Set the default VLAN of the Hybrid port (when the port receives an untagged packet, it defaults to the specified VLAN; when outputting the packet with the default VLAN, it outputs Untag), (by default, the port's default VLAN is VLAN1), the no command is restored to the default condition;

Only when the interface has been configured as a Hybrid port, the above command can be used;

The setting of the default VLAN has nothing to do with whether the Allowed VLAN contains this VLAN, or even whether the VLAN is created, that is, the default VLAN can be set to an uncreated VLAN.

Configure the untagged VLAN list of the Hybrid port

SWITCH(config-if)#**switchport hybrid untagged vlan** VLAN_LIST

Since the default VLAN must be untagged output, it is not maintained by the untagged VLAN list;

By default, the untagged VLAN list is empty (that is, except for the default VLAN, all VLANs are tagged output);

The VLAN maintained by the Untagged VLAN list must be in the Allowed VLAN list of the Hybird port. Therefore, when a VLAN is deleted from the Allowed VLAN, it will also be deleted from the Untagged VLAN list.

Since the untagged VLAN list does not maintain the default VLAN, if a VLAN in the previous list is set as the default VLAN, it will be deleted from the untagged VLAN list, and the process is irreversible.

The default VLAN ID of the Hybrid port connecting the device and the device must be the same, otherwise the packets of the default VLAN will not be transmitted correctly

5.3. Show command

Only in privileged mode can you view VLAN information. The displayed information includes VLAN ID, VLAN status, VLAN member ports, and VLAN configuration information.

Show VLAN

SWITCH#**show vlan** VLANID

```
SWITCH#show vlan 2

Bridge   VLAN ID   Name       State H/W Status Member ports
```

```
                                                    (u)-Untagged, (t)-Tagged

======= ======= ============ ======= ====================

1                          2                    VLAN0002    ACTIVE          Up
GigabitEthernet0/1(u)GigabitEthernet0/2(t)
```

6. CONFIGURE ERPS

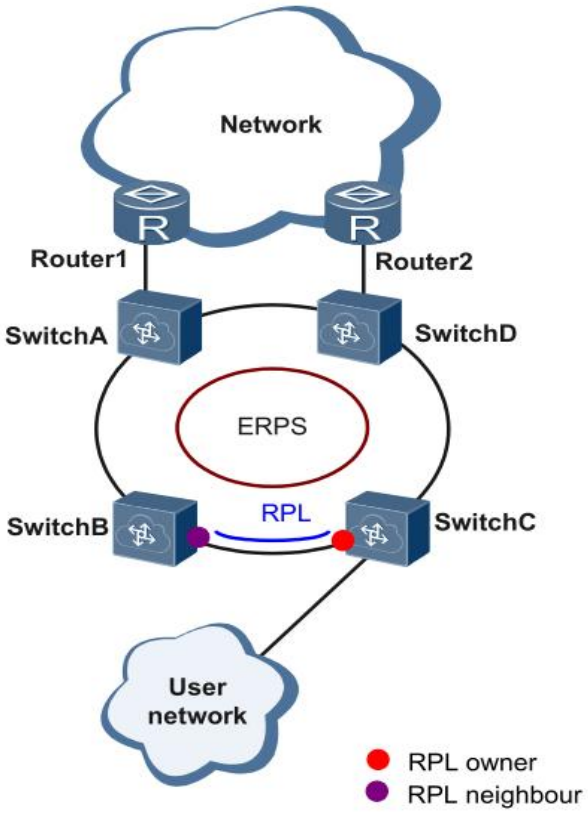
The corresponding web network management configuration path is: Home -> Exchange -> ERPS

6.1. ERPS function overview

ERPS (Ethernet Ring Protection Switching, Ethernet Ring Protection Switching Protocol) is a ring protection protocol developed by the ITU, also known as G.8032. It is a link layer protocol specially applied to the Ethernet ring network. When the Ethernet ring network is complete, it can prevent broadcast storms 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.

At present, STP is another technology that solves the loop problem of the Layer 2 network. STP application is relatively mature, but its convergence time is relatively long (second level). ERPS is a link layer protocol specially applied to the Ethernet ring network. The layer 2 convergence performance is within 50ms, and it has a faster convergence speed than STP.

Typical ERPS networking:



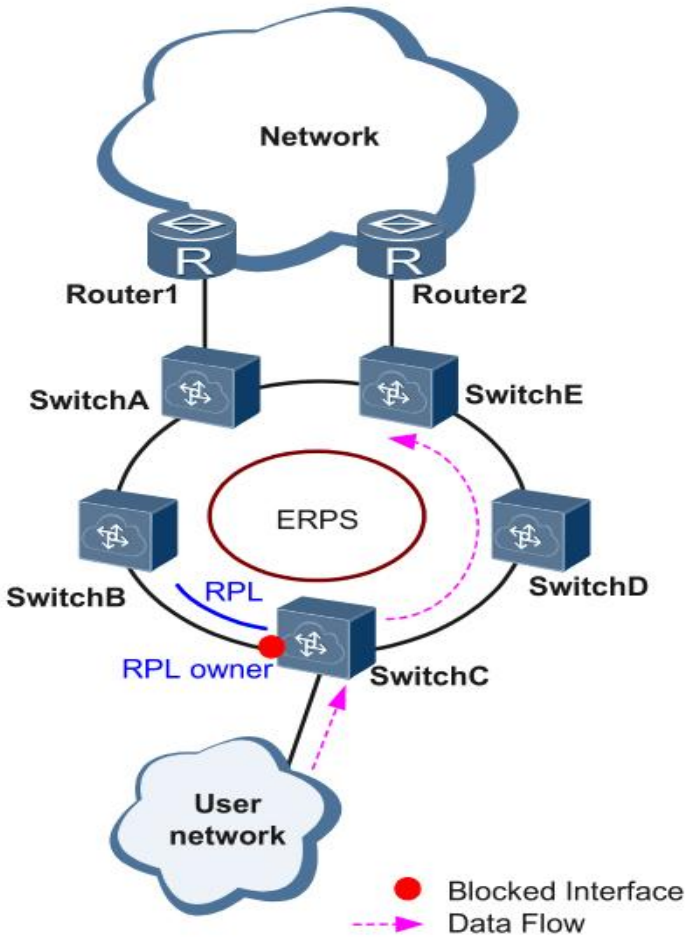
6.2. Introduction to ERPS Principles

ERPS is a standard ring network protocol dedicated to the Ethernet link layer, with the ERPS ring as the basic unit. Only two ports on each layer 2 switching device can join the same ERPS ring. In an ERPS ring, in order to prevent loops, a loop-breaking mechanism can be activated to block the RPL owner port and eliminate loops. When a link failure occurs in the ring network, the equipment running the ERPS protocol can quickly release the blocked port, perform link protection switching, and restore the link communication between nodes on the ring network. This section mainly introduces the implementation principle of ERPS under the basic single-ring network according to the process of link normal -> link failure -> link recovery (including protection switching operation) in the form of examples.

Link is normal

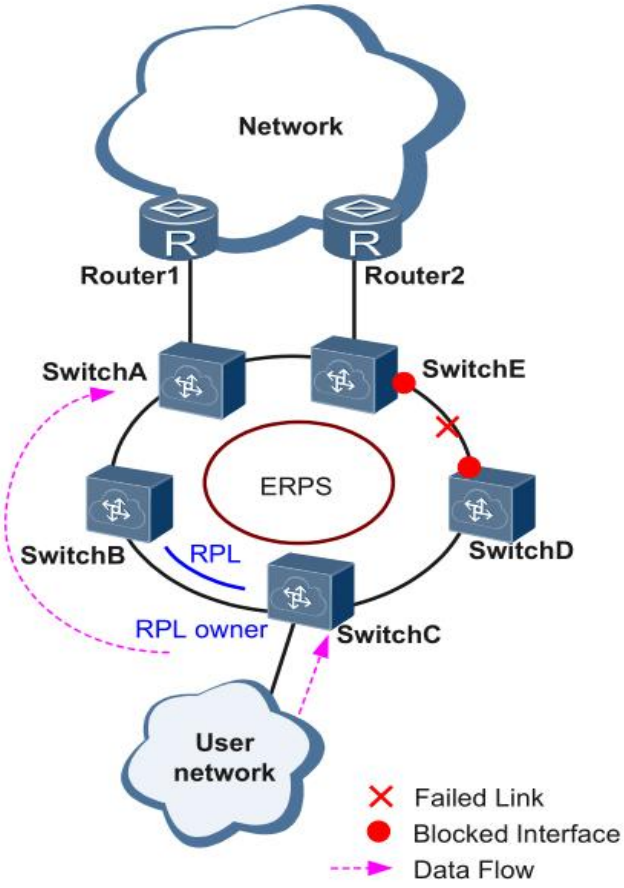
As shown in the figure below, the devices on the loop composed of SwitchA to SwitchE communicate normally.

To prevent loops, ERPS will first block the RPL owner port. If the RPL neighbour port is configured, this port will also be blocked, and other ports can forward business traffic normally.



Link failure

As shown in the figure, when the link between SwitchD and SwitchE fails, the ERPS protocol starts the protection switching mechanism to block the ports at both ends of the failed link, and then releases the RPL owner port. These two ports resume user traffic. Receiving and sending, thus ensuring uninterrupted traffic.



Link recovery

After the link returns to normal, if the ERPS ring is configured in the failback mode, the device where the RPL owner port is located will block the traffic on the RPL link again, and the failed link will be used again to complete the transmission of user traffic.

6.3. Configuration command

Create an ERPS ring

SWITCH(config)#**erps ring** <1-255> **east-interface** IFNAME **west-interface** IFNAME

The ERPS ring is composed of a group of interconnected Layer 2 switching devices configured with the same control VLAN. It is the basic unit of the ERPS protocol and needs to be configured on each device in the ring;

The ring number is the unique identifier of the ERPS ring;

Create an ERPS instance

SWITCH(config)#**erps instance** NAME

It will enter the instance configuration mode when it is created;

For Layer 2 devices running the ERPS protocol, the VLAN that transmits ERPS protocol packets and data packets must be mapped to the protection instance, so that the ERPS protocol can forward or block these packets according to its blocking principle. Otherwise, VLAN packets may generate broadcast storms in the looped network and cause the network to be unavailable;

Associate ERPS instances and rings

SWITCH(config-erps-inst)#**ring** <1-255>

Configure the correspondence between ERPS instances and rings;

Configure ERPS instance level

SWITCH(config-erps-inst)#**level** <0-7>

Configure the ERPS instance level;

Configure the configuration template used by the ERPS instance

SWITCH(config-erps-inst)#**profile** NAME

Configure the ERPS configuration template name;

Configure the RPL role in the ERPS instance

SWITCH(config-erps-inst)#**rpl-role** XXX

An ERPS ring has only one RPL owner port, which is determined by user configuration. By blocking the RPL owner port to forward user traffic to prevent loops in the ERPS ring;

Configure the management VLAN of the ERPS instance

SWITCH(config-erps-inst)#**vlan** <2-4094> **raps-channel**

Configure/delete the management VLAN of the ERPS instance;

Each ERPS ring must be configured with a management VLAN, and different ERPS rings must use different management VLANs;

Configure the intersecting sub-ring blocking port

SWITCH(config-erps-inst)#**sub-ring block** (**east-interface | west-interface**)

Configure the ERPS instance as a sub-ring instance, and specify the sub-ring blocking port;

Configure the MST instance associated with the ERPS instance

SWITCH(config-erps-inst)#**id** <0-255>

The default MST instance ID is 0;

Indirectly associate the VLAN by associating the MST Instance ID (see the "Configure the MST VLAN and Instance Correspondence" configuration of Configuring STP Spanning Tree Protocol for details);

It is currently not supported to change the MST instance in the intersecting ring

Configure sub-ring virtual channels and non-virtual channels

SWITCH(config-erps-inst)#**virtual-channel attached-to-instance** NAME

SWITCH(config-erps-inst)# **non-virtual-channel**

Configure sub-ring virtual channels and non-virtual channels

The position displayed by this command in show running-config must be after the display position of the associated instance. Usually, you only need to ensure that the sub-ring ID and instance name are larger than those of the main ring.

Create ERPS configuration template

SWITCH(config)#**erps profile** NAME

Create an ERPS configuration template; enter the ERPS template configuration mode after the creation is successful;

Configure the failback mode of the ERPS template

SWITCH(config-erps-prof)#**revertive**

Configure ERPS automatic switchback;

Configure the timer parameters of the ERPS template

SWITCH(config-erps-prof)#**timer** (**wait-to-restore** (<1-12> | **default**) | **hold-off** (<0-100> | **default)** | **guard-timer (**<1-200> | **default**))

wait-to-restore: The unit is minute; the switchback time after fault recovery, the default is 5 minutes;

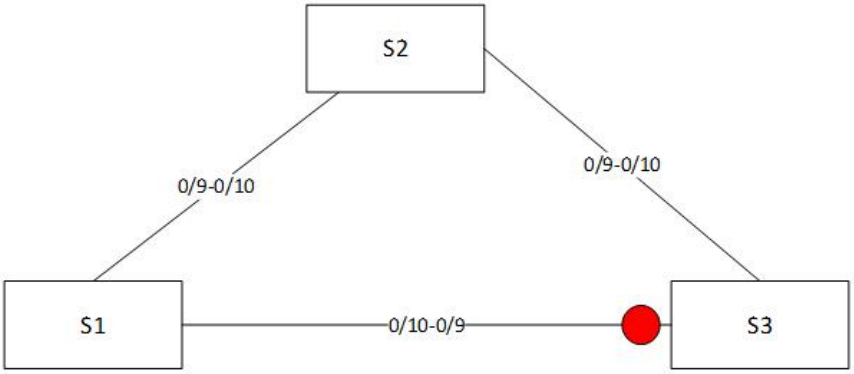
hold-off: The unit is 100 milliseconds; the hold time before the port forward, the default is 0, and the direct forward is not delayed;

guard-timer: The unit is 10 milliseconds; the protection window when the state changes, to avoid receiving a message in the previous state from causing a misjudgment of the protocol, the default value is 50: 500 milliseconds;
The guard-timer parameter will limit the network scale to a certain extent. It is conservatively recommended that when there are more than 300 nodes in the ring network, this parameter should be directly configured to the maximum value to avoid the failure of old packets to be discarded normally due to the excessive network scale; 300 No special configuration is required for nodes within.

6.4. Configuration case

Case 1: Single-loop case requirements

As shown in the topology in the figure below, the configuration blocks the direct links of S1 and S2 by default, and restores the links in time to ensure that the network is available in the event of a failure. The data VLAN is 1, 2, 3.



Switch S1, S2 configuration

- CLI reference configuration

```
SWITCH(config)#vlan 2,3,1000
SWITCH(config)#interface GigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 1 east-interface GigabitEthernet0/9 west-interface
      GigabitEthernet0/10
SWITCH(config)#erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role non-owner
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

- Web network management reference configuration

1) Add VLAN 2, 3, 1000

Add VLAN in Homepage->Switch->VLAN, and then click Apply.

2) Configure GigabitEthernet0/9-10 as a trunk port

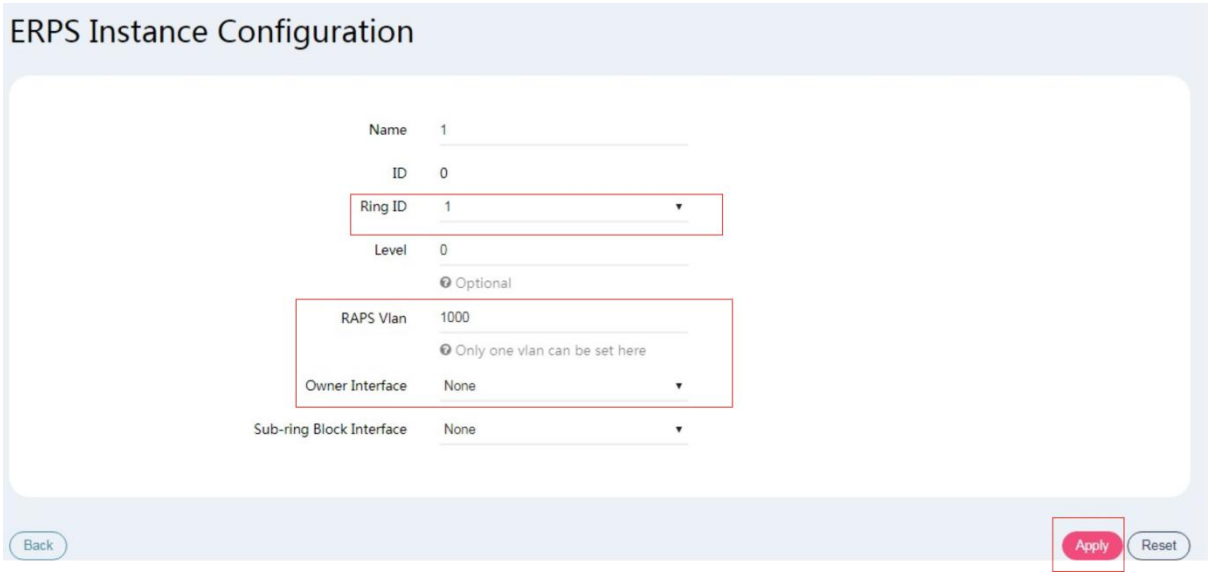
Select the port to be configured in the home page -> switching -> VLAN, click Edit, modify the port VLAN mode, and then click Apply.

3) Add ERPS ring 1

Add the ERPS ring configuration in the home page->Exchange->ERPS->Configuration, select the corresponding port, and then click Apply.

4) Add ERPS instance 1

Add the ERPS instance configuration in the home page -> exchange -> ERPS -> configuration, select the corresponding ring number, management VLAN, and whether it is the Owner interface, and then click Apply.



Switch S3 reference configuration

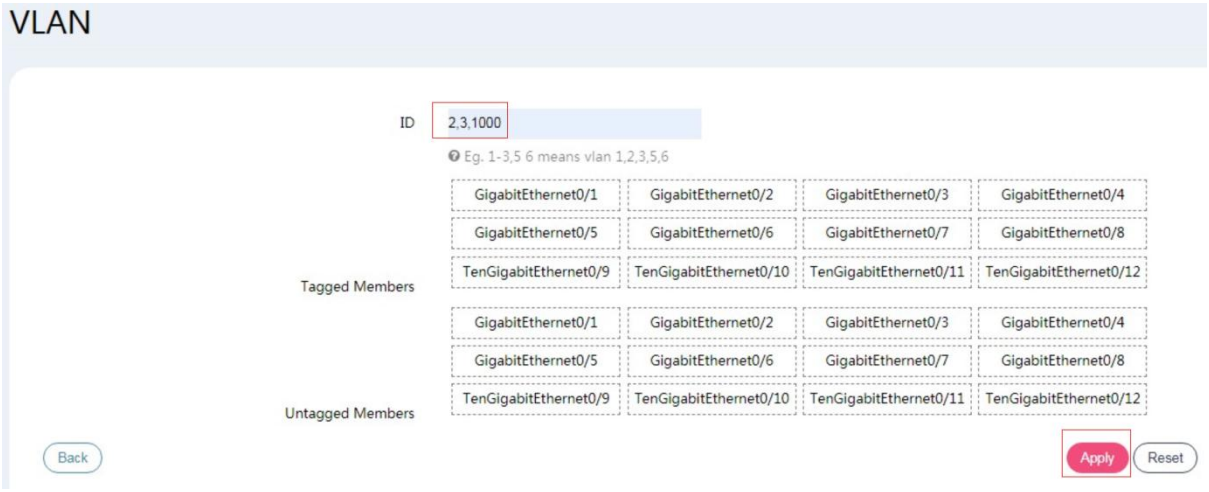
- CLI reference configuration

```
SWITCH(config)#vlan 2,3,1000
SWITCH(config)#interface GigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 1 east-interface GigabitEthernet0/9 west-interface GigabitEthernet0/10
SWITCH(config)#erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role owner east-interface
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

- Web network management reference configuration

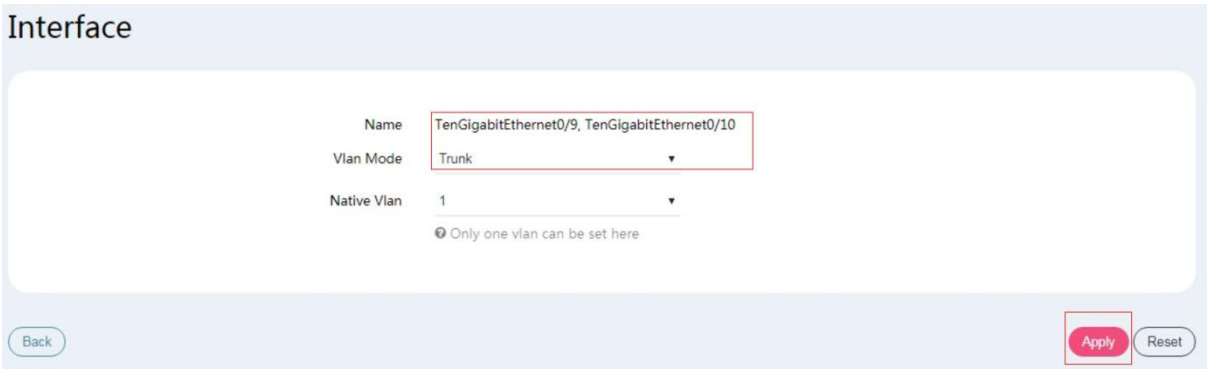
1) Add VLAN 2, 3, 1000

Add VLAN in Homepage->Switch->VLAN, and then click Apply.



2) Configure GigabitEthernet0/9-10 as a trunk port

Select the port to be configured in the home page -> switching -> VLAN, click Edit, modify the port VLAN mode, and then click Apply.

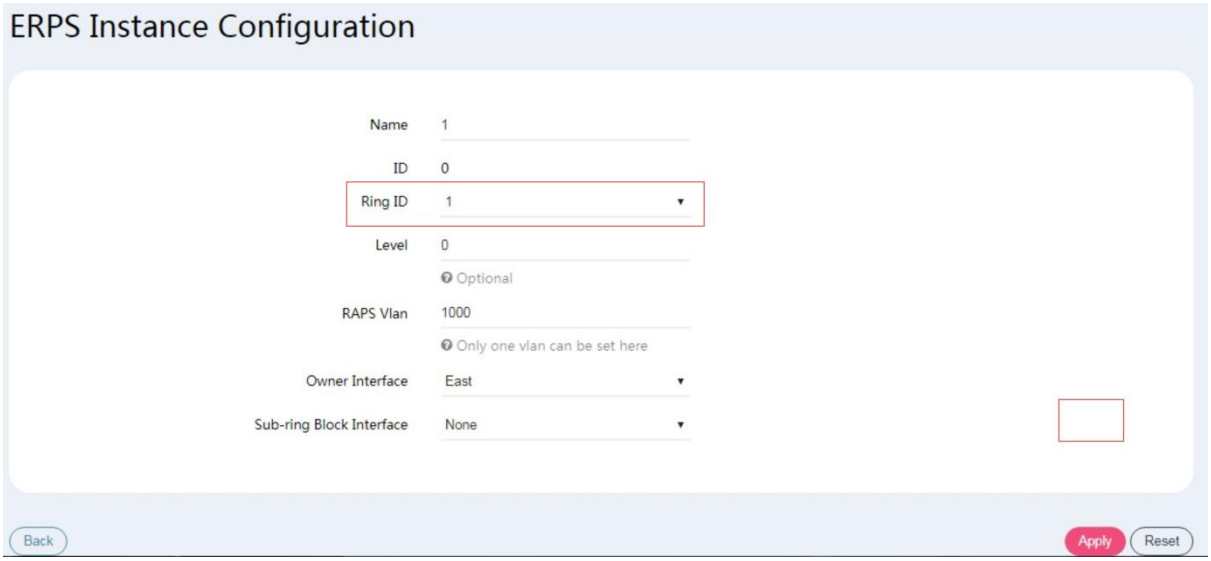


3) Add ERPS ring 1

Add the ERPS ring configuration in the home page->Exchange->ERPS->Configuration, select the corresponding port, and then click Apply.

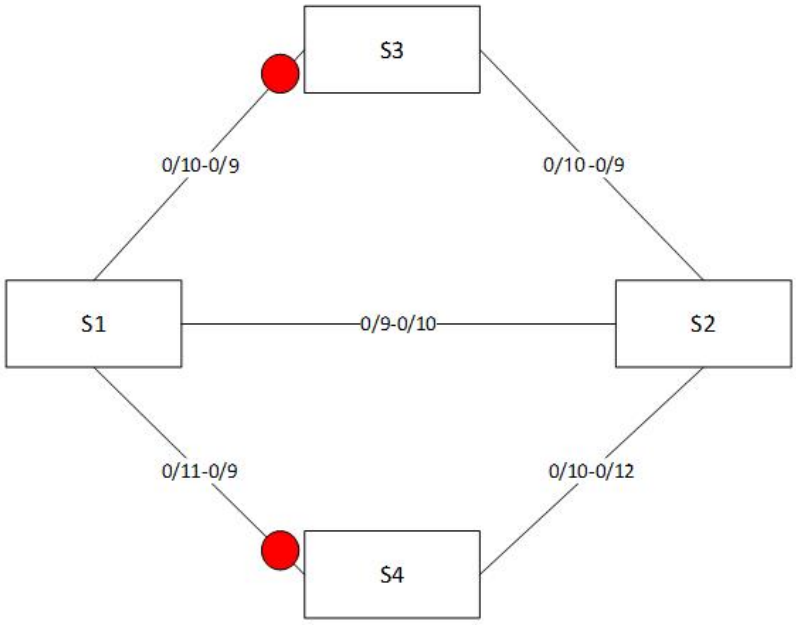
4) Add ERPS instance 1

Add the ERPS instance configuration in the home page -> exchange -> ERPS -> configuration, select the corresponding ring number, management VLAN, and whether it is the Owner interface, and then click Apply.



Case 2: Intersecting Ring Case Requirements

In the topology shown in the figure below, S1, S2, S3, and S4 form an intersecting ring, and the data vlan is 1, 2, 3, and 4. It is required to achieve rapid convergence when a single point of failure occurs in each ring; at most two failures can occur in the network Point (different ring) without user disconnection, to achieve optimal reliability.



Switch S1 reference configuration

- CLI reference configuration

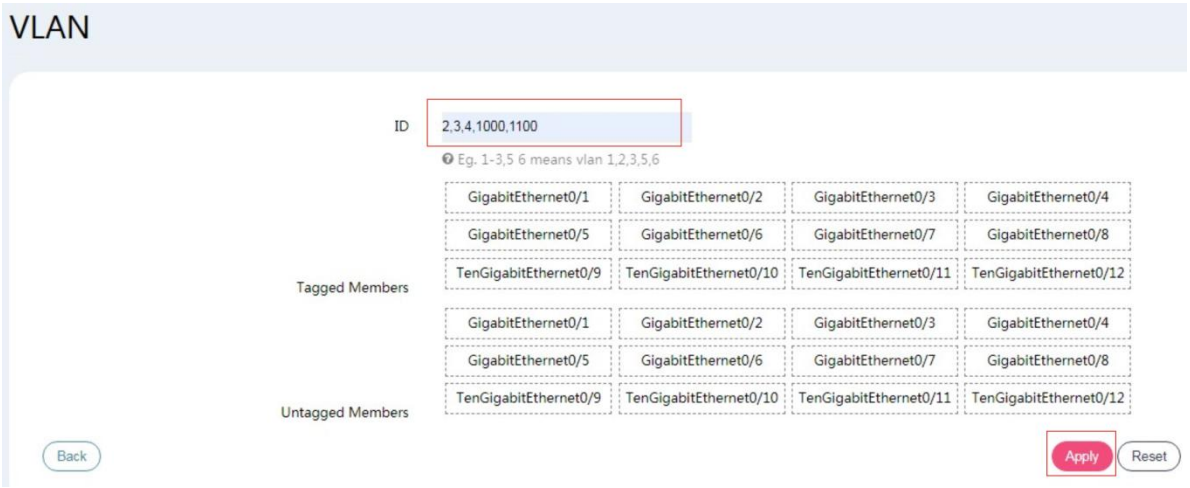
```
SWITCH(config)#vlan 2,3,4,1000,1100
SWITCH(config)#interface GigabitEthernet0/9-11
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 1 east-interface GigabitEthernet0/9 west-interface
```

```
GigabitEthernet0/10
SWITCH(config)#erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role non-owner
SWITCH(config-erps-inst)#vlan 1000 raps-channel

SWITCH(config)#erps ring 2 east-interface GigabitEthernet0/9 west-interface
GigabitEthernet0/11
SWITCH(config)#erps instance 2
SWITCH(config-erps-inst)#ring 2
SWITCH(config-erps-inst)#sub-ring block east-interface
SWITCH(config-erps-inst)#vlan 1100 raps-channel
SWITCH(config-erps-inst)#virtual-channel attached-to-instance 1
```

- Web network management reference configuration

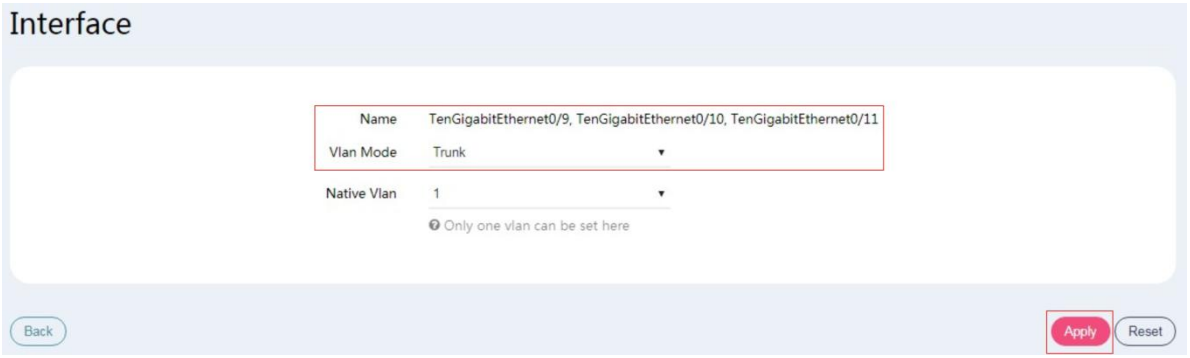
1) Add VLAN 2, 3, 4, 1000, 1100

Add VLAN in Homepage->Switch->VLAN, and then click Apply.



2) Configure GigabitEthernet0/9-11 as a trunk port

Select the port to be configured in the home page -> switching -> VLAN, click Edit, modify the port VLAN mode, and then click Apply.

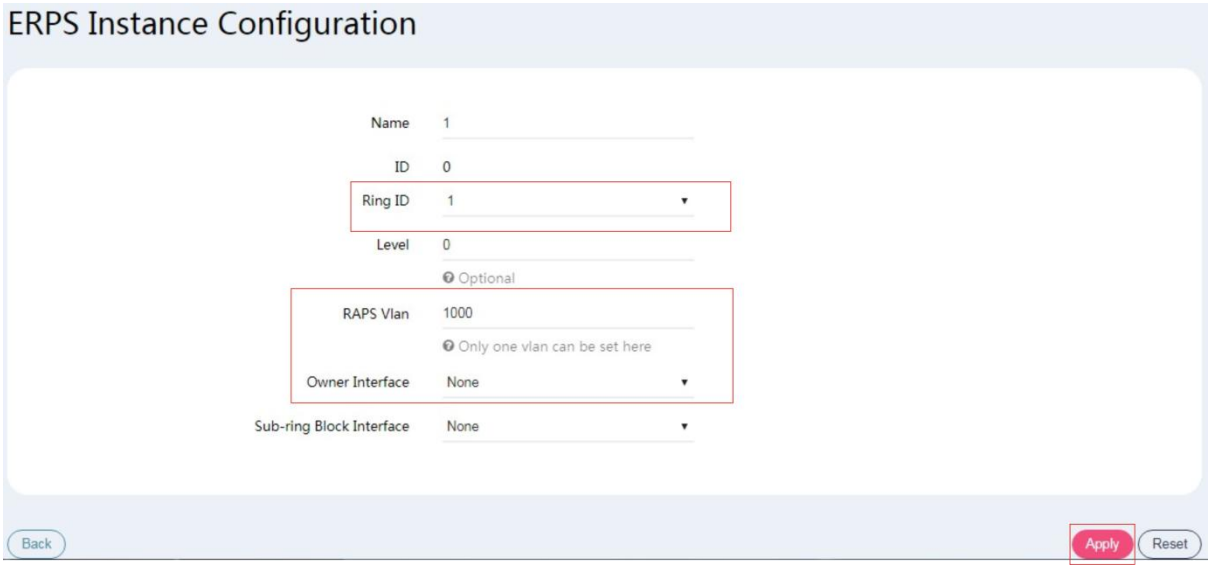


3) Add ERPS ring 1

Add the ERPS ring configuration in the home page->Exchange->ERPS->Configuration, select the corresponding port, and then click Apply.

4) Add ERPS instance 1

Add the ERPS instance configuration in the home page -> exchange -> ERPS -> configuration, select the corresponding ring number, management VLAN, and whether it is the Owner interface, and then click Apply.

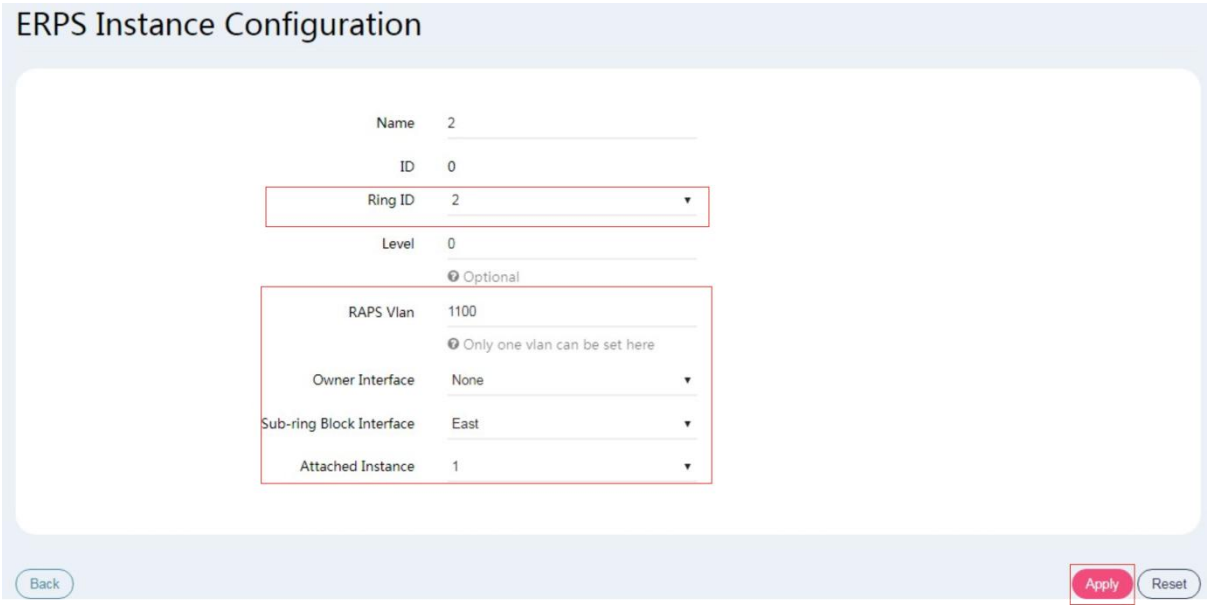


5) Add ERPS ring 2

Add the ERPS ring configuration in the home page->Exchange->ERPS->Configuration, select the corresponding port, and then click Apply.

6) Add ERPS instance 2

Add ERPS instance configuration in Home->Switch->ERPS->Configuration, select the corresponding ring number, management VLAN, Owner interface, sub-ring blocking port, primary ring instance ID, and then click Apply.



Switch S2 reference configuration

- CLI reference configuration

```
SWITCH(config)#vlan 2,3,4,1000,1100
SWITCH(config)# interface GigabitEthernet0/9-10,GigabitEthernet0/12
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 1 east-interface GigabitEthernet0/9 west-interface
      GigabitEthernet0/10
SWITCH(config)#erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#vlan 1000 raps-channel


SWITCH(config)#erps ring 2 east-interface GigabitEthernet0/12 west-interface
```

```
GigabitEthernet0/10
SWITCH(config)#erps instance 2
SWITCH(config-erps-inst)#ring 2
SWITCH(config-erps-inst)#sub-ring block west-interface
SWITCH(config-erps-inst)#vlan 1100 raps-channel
SWITCH(config-erps-inst)#virtual-channel attached-to-instance 1
```

- The reference configuration of the web network management is similar to the reference configuration of the switch S1 in the same case, and will not be repeated here.

Switch S3 reference configuration

- CLI reference configuration

```
SWITCH(config)#vlan 2,3,4,1000
SWITCH(config)#interface GigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 1 east-interface GigabitEthernet0/9 west-interface
GigabitEthernet0/10
SWITCH(config)#erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role owner east-interface
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

- The reference configuration of the Web network management is similar to the reference configuration of the switch S3 in the single-ring case, and will not be repeated here.

Switch S4 reference configuration

- CLI reference configuration

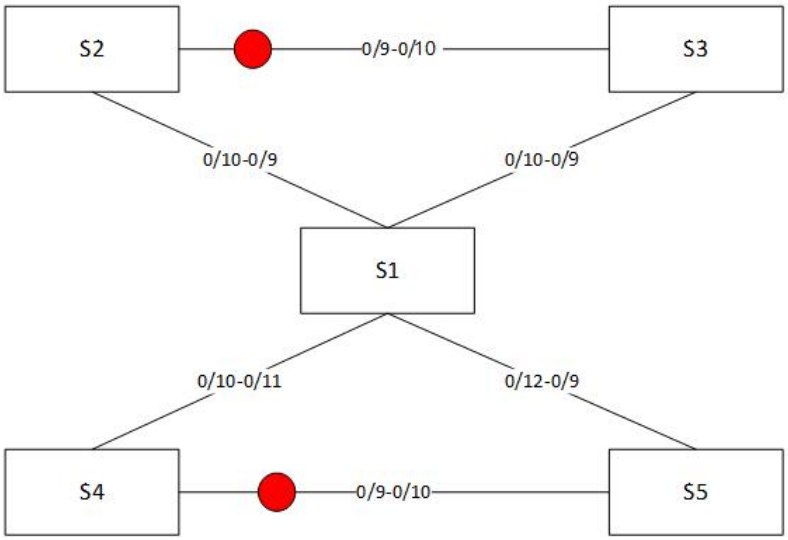
```
SWITCH(config)#vlan 2,3,4,1100
SWITCH(config)#interface GigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 2 east-interface GigabitEthernet0/9 west-interface
GigabitEthernet0/10
SWITCH(config)#erps instance 2
SWITCH(config-erps-inst)#ring 2
SWITCH(config-erps-inst)#rpl-role owner east-interface
SWITCH(config-erps-inst)#vlan 1100 raps-channel
```

- The reference configuration of the Web network management is similar to the reference configuration of the switch S3 in the single-ring case, and will not be repeated here.

Case 3: Tangent Ring Case Requirements

The topology diagram is shown below. S1 is located in the central computer room and can be supervised and maintained by the administrator in real time. It has high reliability; S2-S5 are distributed in various deployment points. In order to improve the reliability of the network, avoid single-link external connections. At the same time, it avoids the risk of single-machine failure that may occur when a dual-link external single-machine is connected, and the dual-link external connection forms a ring network.

The data vlan is 1, 2, 3, and 4, and each ring network is required to converge quickly when a single point of failure occurs to avoid user network interruption.



Switch S1 reference configuration

- CLI reference configuration

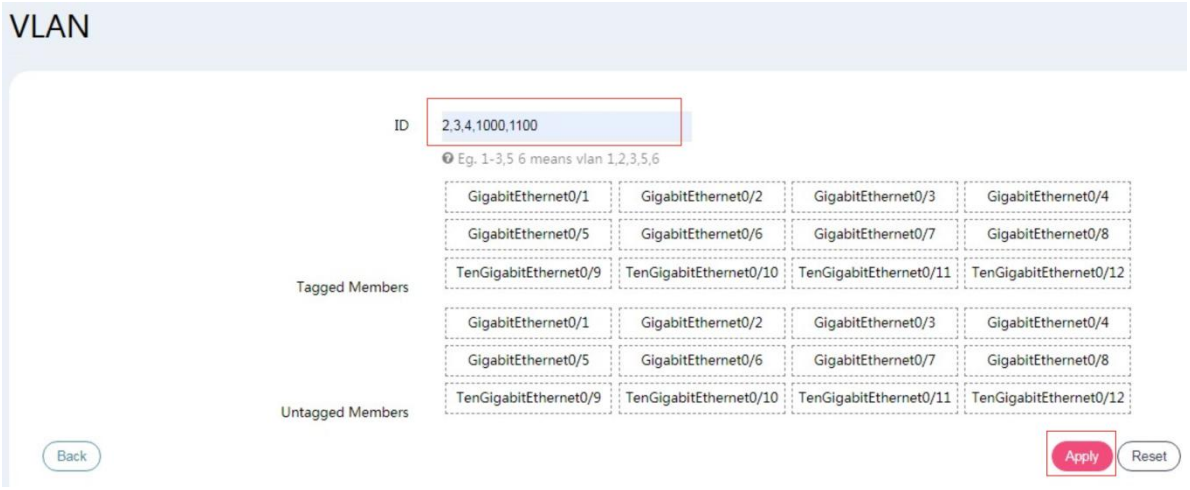
```
SWITCH(config)#vlan 2,3,4,1000,1100
SWITCH(config)#interface GigabitEthernet0/9-12
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 1 east-interface GigabitEthernet0/9 west-interface
      GigabitEthernet0/10
SWITCH(config)#erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role non-owner
SWITCH(config-erps-inst)#vlan 1000 raps-channel

SWITCH(config)#erps ring 2 east-interface GigabitEthernet0/11 west-interface
```

```
        GigabitEthernet0/12
SWITCH(config)#erps instance 2
SWITCH(config-erps-inst)#ring 2
SWITCH(config-erps-inst)#rpl-role non-owner
SWITCH(config-erps-inst)#vlan 1100 raps-channel
```

- Web network management reference configuration

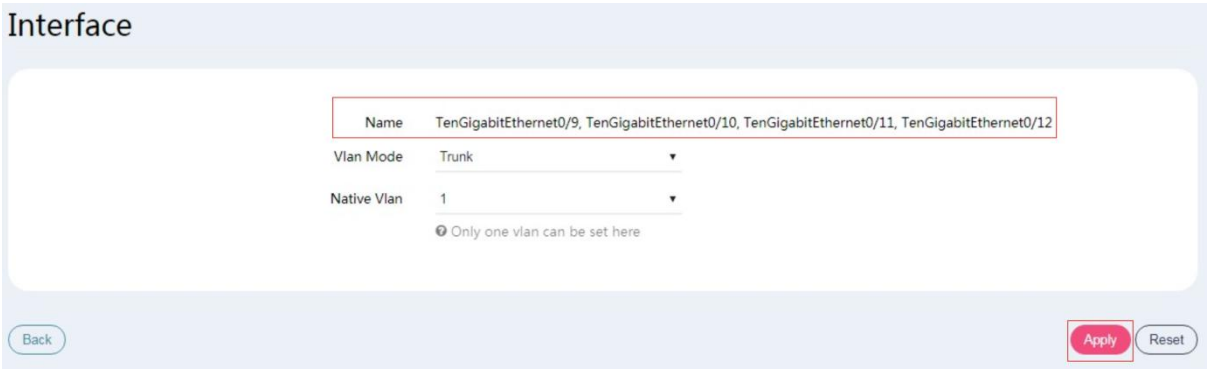
1) Add VLAN 2, 3, 4, 1000, 1100

Add VLAN in Homepage->Switch->VLAN, and then click Apply.



2) Configure GigabitEthernet0/9-12 as a trunk port

Select the port to be configured in the home page -> switching -> VLAN, click Edit, modify the port VLAN mode, and then click Apply.

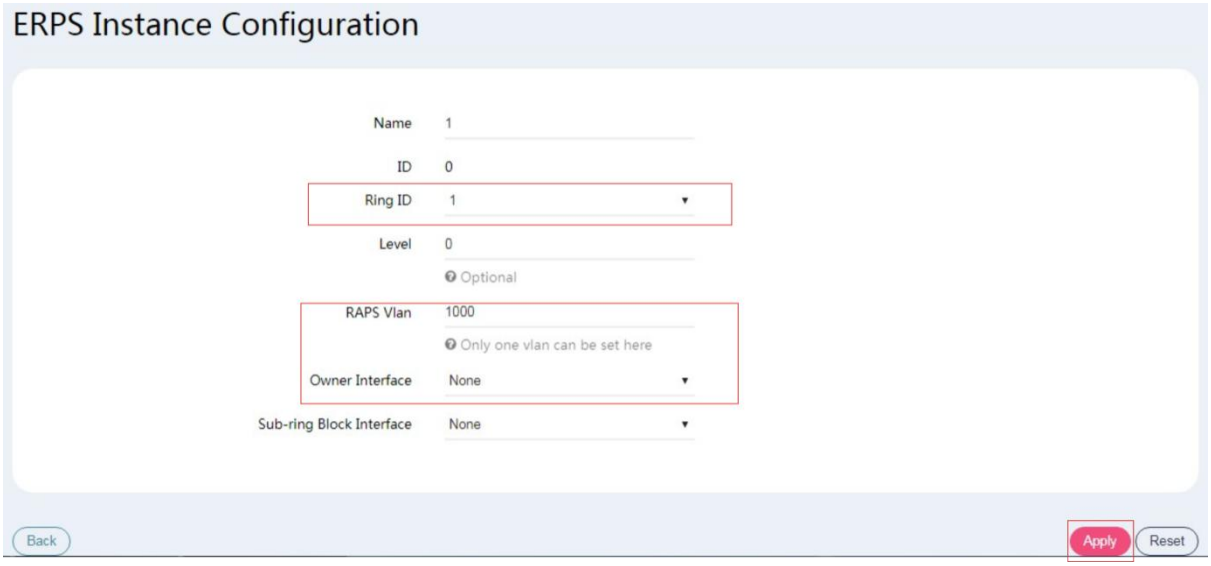


3) Add ERPS ring 1

Add the ERPS ring configuration in the home page->Exchange->ERPS->Configuration, select the corresponding port, and then click Apply.

4) Add ERPS instance 1

Add the ERPS instance configuration in the home page -> exchange -> ERPS -> configuration, select the corresponding ring number, management VLAN, and whether it is the Owner interface, and then click Apply.

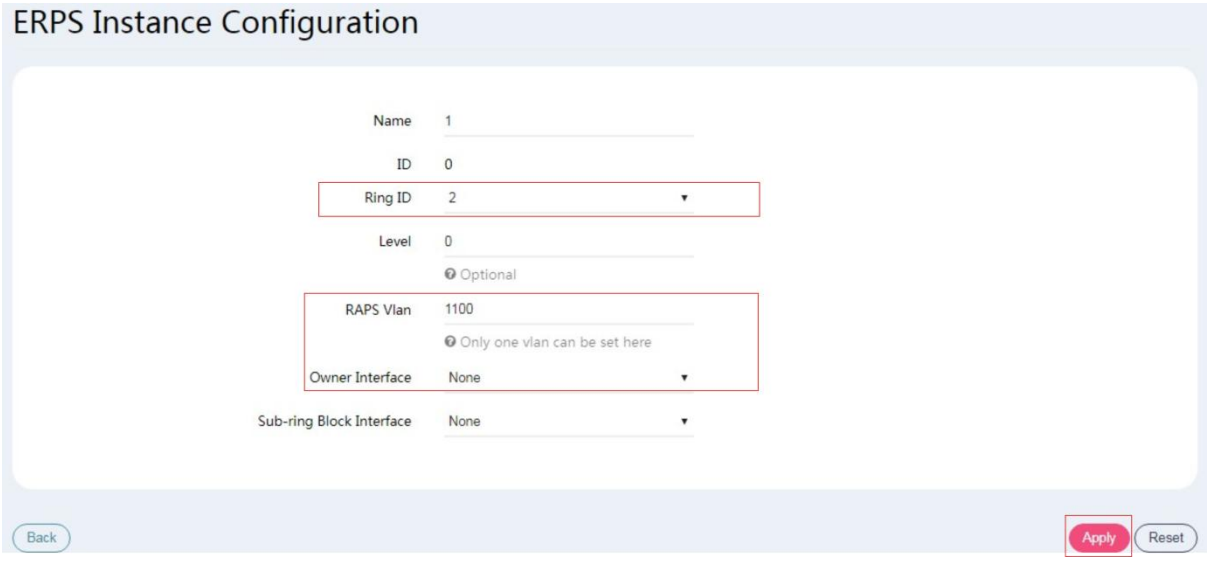


5) Add ERPS ring 2

Add the ERPS ring configuration in the home page->Exchange->ERPS->Configuration, select the corresponding port, and then click Apply.

6) Add ERPS instance 2

Add the ERPS instance configuration in the home page -> exchange -> ERPS -> configuration, select the corresponding ring number, management VLAN, and whether it is the Owner interface, and then click Apply.



Switch S2 reference configuration

- CLI reference configuration

```
SWITCH(config)#vlan 2,3,4,1000
SWITCH(config)#interface GigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 1 east-interface GigabitEthernet0/9 west-interface GigabitEthernet0/10
SWITCH(config)#erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role owner east-interface
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

- The reference configuration of the Web network management is similar to the reference configuration of the switch S3 in the single-ring case, and will not be repeated here.

Switch S3 reference configuration

- CLI reference configuration

```
SWITCH(config)#vlan 2,3,4,1000
SWITCH(config)#interface GigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 1 east-interface GigabitEthernet0/9 west-interface GigabitEthernet0/10
SWITCH(config)#rps instance 1
SWITCH(config-erps-inst)#ring 1
```

```
SWITCH(config-erps-inst)#rpl-role non-owner
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

- The reference configuration of the web network management is similar to the reference configuration of the switch S1 in the single-ring case, and will not be repeated here.

Switch S4 reference configuration

- CLI reference configuration

```
SWITCH(config)#vlan 2,3,4,1100
SWITCH(config)#interface GigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 2 east-interface GigabitEthernet0/9 west-interface GigabitEthernet0/10
SWITCH(config)#erps instance 2
SWITCH(config-erps-inst)#ring 2
SWITCH(config-erps-inst)#rpl-role owner east-interface
SWITCH(config-erps-inst)#vlan 1100 raps-channel
```

- The reference configuration of the Web network management is similar to the reference configuration of the switch S3 in the single-ring case, and will not be repeated here.

Switch S5 reference configuration

- CLI reference configuration

```
SWITCH(config)#vlan 2,3,4,1100
SWITCH(config)#interface GigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#erps ring 2 east-interface GigabitEthernet0/9 west-interface GigabitEthernet0/10
SWITCH(config)#erps instance 2
SWITCH(config-erps-inst)#ring 2
SWITCH(config-erps-inst)#rpl-role non-owner
SWITCH(config-erps-inst)#vlan 1100 raps-channel
```

- The reference configuration of the web network management is similar to the reference configuration of the switch S1 in the single-ring case, and will not be repeated here.

6.5. Show command

Display ERPS ring information

SWITCH#**show erps ring** <1-255>

```
SWITCH#show erps ring 1


Ring        : 1
==========
Bridge      : 1
East        : GigabitEthernet0/9
West        : GigabitEthernet0/10
ERP Inst :1,
```

Show ERPS instance

SWITCH#**show erps instance** NAME

```
SWITCH#show erps instance 1
Inst Name           : 1
Inst Id             : 0
State               : ERPS_ST_IDLE
Last Priority       : RAPS-NR-RB
Phy Ring            : 1
Role                : NON-OWNER
East Link           : Link_Unblocked(up)(00-D0-FA-0A-10-06, 1)
West Link           : Link_Unblocked(up)(00-D0-FA-0A-10-06, 1)
TCN Propagation : Disabled
Attached            : -
Attached To         : -
Virtual ID          : -:-
------------------------------------------------------------
        Channel             |           Interface                       |    Profile
  (LEVL, VID, RID)     | (east,ver) ,    (west,ver)           |
============================================================
  (0, 1000,       1)       | (GigabitEthernet0/9, V=1), (GigabitEthernet0/10, V=1)        | Default
============================================================
```

Display ERPS configuration template

SWITCH#**show erps profile** NAME

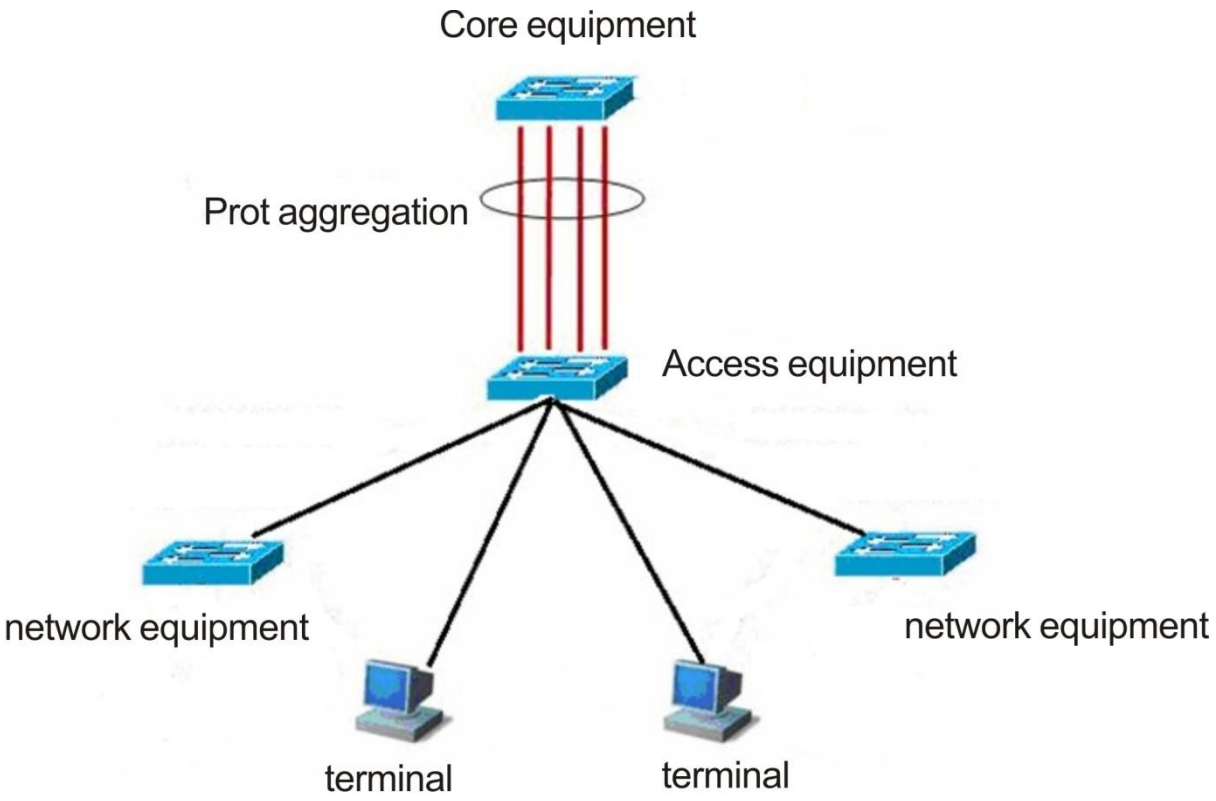
```
SWITCH#show erps profile 1


Profile : 1
=========
 Wait-To-Restore : 5 mins
 Hold Off Timer   : 0 secs
 Guard Timer       : 500 ms
 Wait-To-Block    : 5500 ms
 Protection Type : Revertive
```

7. CONFIGURE PORT AGGREGATION

The corresponding web network management configuration path is: Home -> Interface -> Port Aggregation

7.1. Overview of the aggregation port

Bundle multiple physical links together to establish a logical link. We call this logical link the aggregation port (Port-Channel port). This function is called the port aggregation function. The aggregation port function complies with the IEEE802.3ad standard. It can be used to expand link bandwidth and provide higher connection reliability. It is often used for port uplinks, as shown in the figure below.



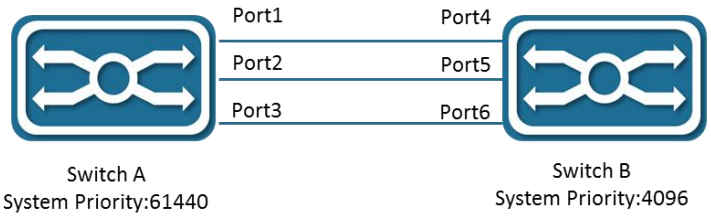
The aggregation port has the following characteristics: high bandwidth, the total bandwidth of the aggregation port is the sum of the bandwidth of the physical member ports; it supports a traffic balancing strategy, which can allocate traffic to each member link according to the strategy; supports link backup, when one of the aggregation ports When a member link is disconnected, the system will automatically distribute the traffic of the member link to other valid member links in the aggregation port.

7.2. LACP overview

LACP (Link Aggregation Control Protocol) based on the IEEE802.3ad standard is a protocol for dynamic link aggregation. If the port is enabled with LACP protocol, the port will send LACPDU to announce its own system priority, system MAC, port priority, port number, operation key, etc. After the connected device receives the LACP packet from the opposite end, it compares the system priorities of both ends according to the system ID in the packet. At the end with the higher system ID

priority, the ports in the aggregation group will be set to be in the aggregation state according to the priority of the port ID from high to low, and updated LACP packets will be sent. After the peer device receives the packets, The corresponding port will also be set to the aggregation state, so that the two parties can reach the same when the port exits or joins the aggregation group. Only after the ports of both parties complete the dynamic aggregation and binding operation, the physical link can forward data packets.

After LACP member port links are bound, periodic LACP message interaction will be performed. When the LACP message is not received for a period of time, the packet is considered to be timed out, the member port link is unbound, and the port is not forwardable again. state. There are two modes of timeout here: long timeout mode and short timeout mode. In long timeout mode, the port sends a message every 30 seconds. If the peer message is not received in 90 seconds, it is in packet receiving timeout; In the short timeout mode, the port sends a message every 1 second. If it does not receive a message from the opposite end in 3 seconds, it is in a packet receiving timeout.



As shown in the figure above, switch A and switch B are connected together through 3 ports. Set the system priority of switch A to 61440, and set the system priority of switch B to 4096. Open LACP link aggregation on the 3 directly connected ports of switches A and B, set the aggregation mode of the 3 ports to active mode, and set the port priority of the 3 ports to the default priority of 32768.

After receiving the LACP packet from the opposite end, switch B finds that its system ID priority is higher (the system priority of switch B is higher than that of switch A), so it follows the order of port ID priority (in the case of the same port priority) , According to the port number from small to large) set ports 4, 5, and 6 to be in aggregation state. After switch A receives the updated LACP packet from switch B, it finds that the system ID priority of the opposite end is higher, and the port is set to the aggregation state, and ports 1, 2, and 3 are also set to the aggregation state.

7.3. Configuration command

Add port to static aggregation port
SWITCH(config-if)#**channel-group** ID (**mode manual |**)
Add port to dynamic aggregation port
SWITCH(config-if)#**channel-group** ID **mode** (**active** | **passive**)
Support 12 aggregation ports <1-12>;

An aggregation port is either static or dynamic, which is determined by the joining method of the first member port to join;

Active aggregation mode means that the port will actively initiate LACP aggregation operations; Passive aggregation mode means that the port will not actively initiate LACP aggregation operations, but will passively participate in LACP calculations after receiving LACP packets from neighbors;

When the aggregate port (Port-Channel port) is not created, and the first port is added to the aggregate port, the Port-Channel port is actively created, and the default attribute of the Port-Channel port is the port attribute;

The premise of adding a port to the aggregation port is the same as the following basic properties of the aggregation port:

- Port VLAN attribute configuration
- Port isolation configuration

Configure the aggregation port load balancing mode
SWITCH(config)#**port-channel load-balance** (**dst-ip | dst-mac | dst-port | src-dst-ip | src-dst-mac | src-dst-port | src-ip | src-mac | src-port**)
Configure the load balancing mode, the default is src-dst-mac
Configure LACP system priority
SWITCH(config)#**lacp system-priority** system-priority
The system priority range is <1-65535>, the default is 32768;

All dynamic link groups of a device can only have one LACP system priority. Modifying this value will affect all aggregation groups on the switch;

Configure LACP port priority
SWITCH(config-if)#**lacp port-priority** port-priority
Port priority is configured in interface mode, and only supports physical port configuration;
The port priority range is <1-65535>, the default is 32768;
Configure LACP port timeout mode
SWITCH(config-if)#**lacp timeout** (**long | short**)
Port timeout mode is configured in interface mode, and only supports physical port configuration;
The default is long mode, LACP protocol message sending interval is 30S, 90S timeout; short mode, LACP protocol message sending interval is 1S, 3S timeout;

7.4. Configuration case

Add GigabitEthernet0/5 and GigabitEthernet0/6 to Port-Channel1; configure the load balancing mode to src-ip.

```
SWITCH(config)#interface GigabitEthernet0/5
SWITCH(config-if)#channel-group 1 mode manual
SWITCH(config-if)#exit
SWITCH(config)#interface GigabitEthernet0/6
SWITCH(config-if)#channel-group 1 mode manual
SWITCH(config-if)#exit
SWITCH(config)#port-channel load-balance src-ip
```

7.5. Show command

Show aggregation port configuration and status information
SWITCH#**show port-channel**

```
SWITCH#show port-channel
Load balance: Source and Destination Mac address

Interface Port-Channel3
   Type: static
   Member:
      GigabitEthernet0/18       link down       Disable

Interface Port-Channel8
   Type: LACP
   Member:
      GigabitEthernet0/19       link up         Enable
      GigabitEthernet0/17       link up         Enable
```

Show aggregate port load balancing mode

SWITCH#**show port-channel load-balance**

```
SWITCH#show port-channel load-balance
Source and Destination Mac address
```

Show brief LACP information

SWITCH#**show lacp summary**

```
SWITCH#show lacp summary
% Aggregator Port-Channel8 1008
% Aggregator Type: Layer2
% Admin Key: 0008 - Oper Key 0008
%     Link: GigabitEthernet0/17 (17) sync: 1 status: Bundled
%     Link: GigabitEthernet0/19 (19) sync: 1 status: Bundled
```

Show LACP details

SWITCH#**show lacp detail**

```
SWITCH#show lacp detail
% Aggregator Port-Channel 8 1008
% Aggregator Type: Layer2
%   Mac address: 00:02:04:ee:25:46
```

```
%  Admin Key: 0008 - Oper Key 0008
%  Actor LAG ID- 0x8000,00-02-04-ee-25-46,0x0008
%  Receive link count: 2 - Transmit link count: 2
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x8000,00-01-a0-00-10-10,0x0032
%    Link: GigabitEthernet0/17 (17) sync: 1 status: Bundled
%    Link: GigabitEthernet0/19 (19) sync: 1 status: Bundled
```

Show LACP packet statistics

SWITCH#**show lacp counter**

```
SWITCH#show lacp counter
% Traffic statistics
    Port          LACPDUs          Marker          Marker-Rsp          Pckt err
                  Sent      Recv      Sent      Recv      Sent      Recv      Sent
Recv
% Aggregator Port-Channel8 1008
GigabitEthernet0/17       23        13        0         0         0         0
0         0
GigabitEthernet0/19       25        15        0         0         0         0
0         0
```

Show LACP System ID

SWITCH#**show lacp sys-id**

```
SWITCH#show lacp sys-id
% System 8000,00-02-04-ee-25-46
```

Show LACP port information

SWITCH#**show lacp** ID

```
SWITCH#show lacp 8
% Aggregator Port-Channel8 1008 Admin Key: 0008 - Oper Key 0008
% Partner LAG ID: 0x8000,00-01-a0-00-10-10,0x0032
% Partner Oper Key 0050
```

Show LACP member port information

SWITCH#**show lacp port** IFNAME

```
SWITCH#show lacp port GigabitEthernet0/19
```

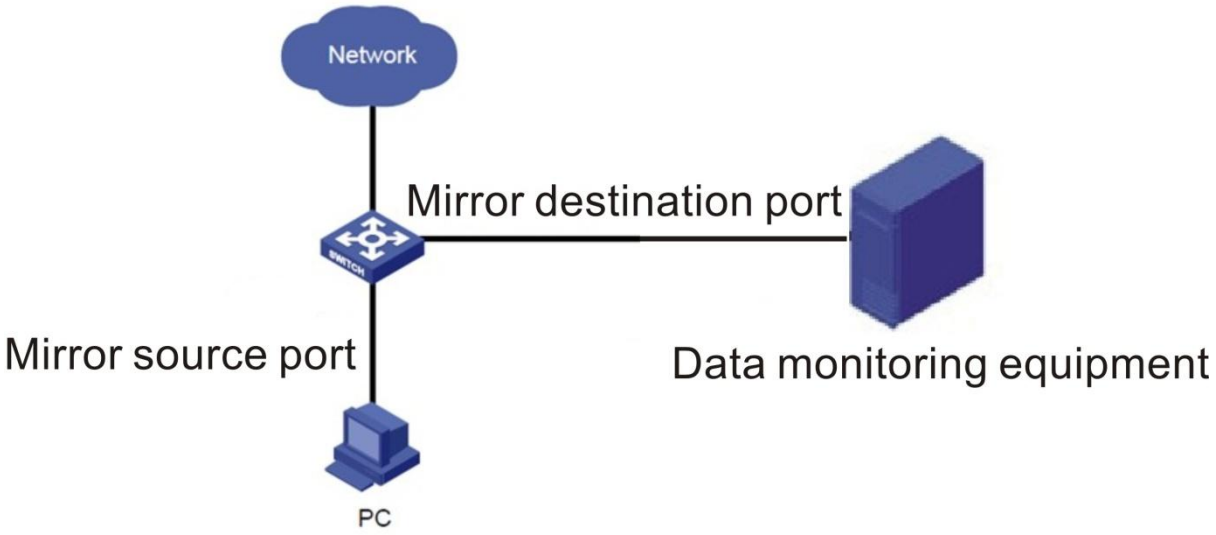
```
% LACP link info: GigabitEthernet0/19 - 19
% LAG ID: 0x8000,00-02-04-ee-25-46,0x0008
% Partner oper LAG ID: 0x8000,00-01-a0-00-10-10,0x0032
% Actor Port priority: 0x8000 (32768)
% Admin key: 0x0008 (8) Oper key: 0x0008 (8)
% Physical admin key:(1)
% Receive machine state : Current
% Periodic Transmission machine state : Slow periodic
% Mux machine state : Collecting/Distributing
% Oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Partner oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Partner link info: admin port 0
% Partner oper port: 20
% Partner admin LAG ID: 0x0000-00:00:00:00:00:0000
% Admin state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner admin state: ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner system priority - admin:0x0000 - oper:0x8000
% Partner port priority - admin:0x0000 - oper:0x8000
% Aggregator ID: 1008
```

8. CONFIGURE SPAN

The corresponding web network management configuration path is: Home -> Interface -> Port Mirroring

8.1. SPAN overview

SPAN (Local Switched Port Analyzer) is a local mirroring function. The SPAN function copies the packets of the designated port to the destination port. Generally, the SPAN destination port is connected to a data detection device. Users use these devices to analyze the packets received by the destination port for network monitoring and troubleshooting.



SPAN does not affect the message exchange between the source port and the destination port. It just copies all incoming and outgoing messages from the source port to the destination port. When the mirrored traffic of the source port exceeds the bandwidth of the destination port, for example, the 100Mbps destination port monitors the 1000Mbps source port traffic, which may cause packets to be discarded.

SPAN is based on session management and configures the source port and destination port of SPAN in the session. In a session, there can only be one destination port, but multiple source ports can be configured at the same time.

8.2. Configuration command

Create a session
SWITCH(config)#**monitor session** ID
Create a session, create a session and enter the session mode at the same time;
Support 7 sessions;
Configure session description
SWITCH(config-monitor)#**description** DESCRIPTION
Configure session source port
SWITCH(config-monitor)#**source interface** IFNAME (**both | rx | tx**)
Configure the session destination port
SWITCH(config-monitor)#**destination interface** IFNAME

8.3. Configuration case

Use port GigabitEthernet0/8 to monitor ingress packets of GigabitEthernet0/1 and GigabitEthernet0/2. The monitoring session is described as "TRAFFIC_MONITOR".

```
SWITCH#configure terminal
SWITCH(config)#monitor session 1
SWITCH(config-monitor)#
SWITCH(config-monitor)#description TRAFFIC_MONITOR
SWITCH(config-monitor)#source interface GigabitEthernet0/1 rx
SWITCH(config-monitor)#source interface GigabitEthernet0/2 both
SWITCH(config-monitor)#destination interface GigabitEthernet0/8
```

8.4. Show command

Show specific conversation
SWITCH#**show monitor session** ID

```
SWITCH#show  monitor session 1
session 1
---------------
description          : TRAFFIC_MONITOR
type                 : local
source intf          :
    tx               : GigabitEthernet0/2
    rx               : GigabitEthernet0/1  GigabitEthernet0/2
```

```
    both                : GigabitEthernet0/2
source VLANs            :
    rx                  :
destination ports : GigabitEthernet0/8


Legend: f = forwarding enabled, l = learning enabled
```

9. CONFIGURE STORM CONTROL

The corresponding web network management configuration path is: Home -> Interface -> Storm Control

9.1. Storm control overview

When there are excessive broadcast, multicast, or unknown unicast data streams in the LAN, it will cause network performance degradation and even network paralysis, which is called a broadcast storm. Storm control limits the rate of broadcast, multicast, and unknown unicast data streams. When the rate of broadcast, unknown-name multicast or unknown unicast data streams received by the switch port exceeds the set bandwidth, the device will only allow it to pass For the data flow of the set bandwidth, the data flow exceeding the bandwidth will be discarded, so as to avoid excessive flooding data flow into the LAN to form a storm.

9.2. Configuration command

Configure interface storm control policy

SWITCH(config-if)#**storm-control** (**broadcast | multicast | unicast | all | unicast-broadcast | multicast-broadcast**) **level** LEVEL

Support the selection of configuration in broadcast/multicast/unicast/all/unicast-broadcast/ multicast-broadcast, and the selected configuration cannot coexist;

Among them, multicast means unknown name multicast message, unicast means unknown name list broadcast message;

The level value is the port bandwidth percentage, which supports adaptive port rate changes;

9.3. Configuration case

Configure the port GigabitEthernet0/1 unknown name multicast rate limit to 10% of the total bandwidth.

```
SWITCH#configure terminal
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#storm-control multicast level 10
```

9.4. Show command

Show all port storm control configurations

SWITCH#**show storm-control**

```
SWITCH#show storm-control
Port                BcastLevel      McastLevel      Unicastlevel
GigabitEthernet0/1  100.00%         100.00%         100.00%
GigabitEthernet0/2  100.00%         100.00%          50.00%
```

GigabitEthernet0/3	80.00%	100.00%	100.00%
GigabitEthernet0/4	100.00%	100.00%	100.00%
GigabitEthernet0/5	100.00%	100.00%	100.00%
GigabitEthernet0/6	100.00%	100.00%	100.00%
GigabitEthernet0/7	100.00%	100.00%	100.00%
GigabitEthernet0/8	100.00%	100.00%	100.00%
GigabitEthernet0/9	100.00%	100.00%	100.00%
GigabitEthernet0/10	100.00%	100.00%	100.00%
GigabitEthernet0/11	100.00%	100.00%	100.00%
GigabitEthernet0/12	100.00%	100.00%	100.00%
GigabitEthernet0/13	100.00%	100.00%	100.00%
GigabitEthernet0/14	100.00%	100.00%	100.00%
GigabitEthernet0/15	100.00%	100.00%	100.00%
GigabitEthernet0/16	100.00%	100.00%	100.00%
GigabitEthernet0/17	100.00%	100.00%	100.00%
GigabitEthernet0/18	100.00%	100.00%	100.00%
GigabitEthernet0/19	100.00%	100.00%	100.00%
GigabitEthernet0/20	100.00%	100.00%	100.00%
GigabitEthernet0/21	100.00%	100.00%	100.00%
GigabitEthernet0/22	100.00%	100.00%	100.00%
GigabitEthernet0/23	100.00%	100.00%	100.00%
GigabitEthernet0/24	100.00%	100.00%	100.00%
TenGigabitEthernet0/25	100.00%	100.00%	100.00%
TenGigabitEthernet0/26	100.00%	100.00%	100.00%
TenGigabitEthernet0/27	100.00%	100.00%	100.00%
TenGigabitEthernet0/28	100.00%	100.00%	100.00%

10. CONFIGURE SNMP NETWORK MANAGEMENT

The current web network management only supports V2C, and the corresponding web network management configuration path is: Home -> System -> SNMP

10.1. SNMP overview

SNMP is the abbreviation of Simple Network Management Protocol, which became a network management standard RFC1157 in August 1988. So far, SNMP has become a de facto network management standard due to the support of this protocol by many manufacturers, which is suitable for use in the interconnection environment of multi-vendor systems.

Using the SNMP protocol, network administrators can perform information query, network configuration, fault location, and capacity planning on nodes on the network. Network monitoring and management are the basic functions of SNMP.

The following versions of SNMP currently exist:

SNMPv1: The first official version of the Simple Network Management Protocol, defined in RFC1157.

SNMPv2C: Community-Based SNMPv2 management architecture, defined in RFC1901.

SNMPv3: By authenticating and encrypting data, it provides the following security features:

1) Ensure that the data is not tampered with during transmission.

2) Ensure that the data is sent from a legitimate data source.

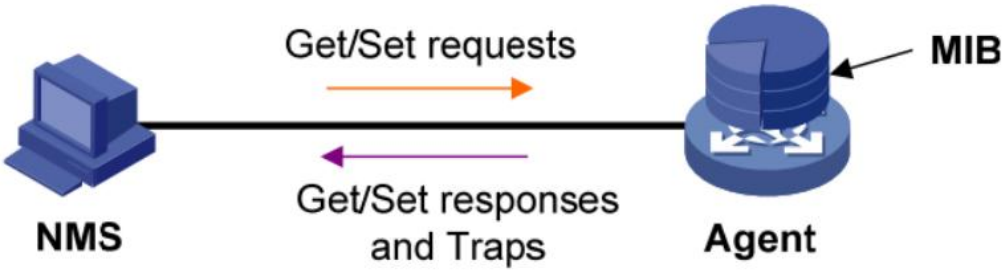
3) Encrypt messages to ensure data confidentiality.

The SNMP network includes two elements, NMS and Agent.

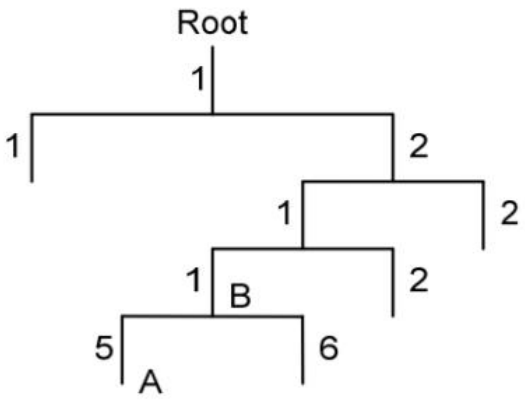
• NMS (Network Management System) is the administrator of SNMP networks and can provide a very friendly human-computer interaction interface to facilitate network administrators to complete most network management tasks.

• Agent is the managed person of the SNMP network, responsible for receiving and processing request messages from NMS. In some emergency situations, such as interface status changes, the Agent will actively send alarm information to the NMS.

When NMS manages devices, it usually pays more attention to some parameters, such as interface status, CPU utilization, etc. The collection of these parameters is called MIB (Management Information Base). These parameters are called nodes in the MIB. MIB defines the hierarchical relationship between nodes and a series of attributes of objects, such as the name, access rights, and data types of the objects. Each Agent has its own MIB. The managed device has its own MIB files. Compiling these MIB files on the NMS can generate the MIB of the device. The NMS reads/writes the MIB nodes according to the access rights, so as to realize the management of the Agent. The relationship between NMS, Agent and MIB is as follows:



MIB is organized according to a tree structure. It consists of many nodes. Each node represents a managed object. The managed object can be uniquely identified by a string of numbers from the root that represents the path. This string of numbers is called OID (Object Identifier). As shown below:



The managed object B can be uniquely identified by a string of numbers {.1.2.1.1}, which is the OID of the managed object B.

SNMP provides three basic operations to realize the interaction between NMS and Agent:

• GET operation: NMS uses this operation to query the value of one or more nodes in the Agent MIB.

• SET operation: NMS uses this operation to set the value of one or more nodes in the Agent MIB.

• Trap operation: The agent uses this operation to send trap information to the NMS. The Agent does not require the NMS to send a response message. NMS will not respond to Trap messages.

Currently, SNMP Agent supports three versions: SNMPv1, SNMPv2c and SNMPv3:

• SNMPv1 uses a community name (Community Name) authentication mechanism. The community name is similar to a password and is used to restrict the communication between the NMS and the Agent. If the community name set by the NMS is different from the community name set on the managed device, the NMS and the Agent cannot establish an SNMP connection, resulting in the NMS unable to access the Agent, and the alarm information sent by the Agent will also be discarded by the NMS.

• SNMPv2c also uses a community name authentication mechanism. SNMPv2c expands the functions of SNMPv1: provides more operation types; supports more data types; provides richer error codes, which can distinguish errors in more detail.

• SNMPv3 adopts the USM (User-Based Security Model, user-based security model) authentication mechanism. The network administrator can set up authentication and encryption functions. Authentication is used to verify the legitimacy of the message sender to avoid access by illegal users;

encryption is to encrypt the transmission message between the NMS and the Agent to avoid eavesdropping. The use of authentication and encryption functions can provide higher security for the communication between the NMS and the Agent.

The SNMPv1 and SNMPv2c versions use community names to identify whether they are authorized to use MIB objects. In order to be able to manage the device, the authentication name of the network management system (NMS) must be the same as a community name defined in the device. A community name can have the following attributes:

• Read-only: Provides authorized management workstations with read access to all MIB variables. The prerequisite for successfully establishing a connection between NMS and Agent is that the SNMP version used by NMS and Agent must be the same.

• Read-write: Provide authorized management workstations with read and write permissions for all MIB variables.

On the basis of SNMPv2, SNMPv3 uses a security model to determine which security mechanism is used to process data; currently available security models have three categories: noauth, auth, and priv.

• noauth: No security authentication is required. Both SNNMPv1 and SNMPv2c use this security model.

• auth: Security authentication is required, but the transmitted message PDU is not encrypted.

• priv: It is necessary to perform security authentication and also to encrypt the transmitted message PDU.

The details are shown in the following table:

Version	Security model	Identify	Encryption	Illustrate
v1	noauth	Group name	NA	Confirm the legality of the data through the authentication name
v2c	noauth	Group name	NA	Confirm the legality of the data through the authentication name
v3	noauth	Username	NA	Confirm the legality of the data through the user name
v3	auth	MD5/SHA	NA	Provide a user name and password authentication mechanism based on MD5 or SHA.
v3	priv	MD5/SHA	AES/DES	Provide a user name and password authentication mechanism based on MD5 or SHA, and provide a data encryption mechanism based on AES or DES.

10.2. Configuration command

Configure SNMP View

SWITCH(config)# **snmp-server view** WORD OID-TREE **(include | exclude)**

An SNMP view can define several Oid-trees. An Oid-tree consists of two parts: oid and containment relations. For example, ".1.3.6.1.2.1.1" include means that all MIB nodes under the "system" node

belong to this view; ".1.3.6.1.2.1.1" exclude means that except for MIB nodes under the "system" node, All other MIB nodes belong to this view.
The length of the view name ranges from 1-31. The length of the OID-TREE string ranges from 2-63. ".1" include means to match all MIB nodes. If the Group does not specify view, all MIB nodes will be matched by default.
When deleting a view, use the command "no snmp-server view WORD (OID-TREE (include | exclude) |)", you can delete only one Oid-tree, or delete the entire view.
The view defines the range of MIB nodes that can be accessed. But for the view to take effect, it must be associated with a valid group.

Configure SNMP Group

SWITCH(config)# **snmp-server group** WORD **(v3 (auth | noauth | priv) |) (read (null |** READ-VIEW**) |) (write (null |** WRITE-VIEW**) |)**
SNMP group distinguishes the version into v3 or non-v3 (that is, v1 and v2c). If it is the v3 version, define the security model corresponding to the group. The length of the group name ranges from 1-31.
Optional configuration of read view and write view corresponding to the group, that is, the range of MIB nodes that can be read and the range of MIB nodes that can be written by the group. If view is not specified, it means that the MIB node range is all. If the keyword null is specified, it means that the corresponding operation on all MIB nodes is prohibited. read null indicates that read operations are prohibited; write null indicates that write operations are prohibited.
The view associated with the group must exist, otherwise the group will not be created successfully. Similarly, if the view associated with the group is deleted, the group will also be deleted automatically.
Use the command "no snmp-server group WORD" when deleting a group.
For group to take effect, it must be associated by community (non-v3 version) or user (v3 version).

Configure SNMP community

SWITCH(config)# **snmp-server community** WORD (**group** WORD **| (ro |) |)**
The length range of community (community name) is 1-31. Community is used for SNMPv1 and SNMPv2c versions.
If the community is not associated with a group, the ro keyword can be used to specify that the community has read-only access to all MIB nodes, or no parameter specifies that the community can read and write access to all MIB nodes.
The community must be associated with an existing group with a version other than v3. If the group does not exist or the version does not match, the community will not be created successfully. Similarly, if the group associated with the community is deleted, the community will also be deleted automatically.
After the community is associated with the group, the read and write MIB node range will be determined by the range defined by the group (actually determined by the view associated with the group).
Use the command "no snmp-server community WORD" when deleting community.

Configure SNMP user

SWITCH(config)# **snmp-server user** WORD **(group** WORD **|) (((encrypted|) auth (md5 | sha)** AUTH-PASSWORD**) ((priv (des | aes)** PRIV-PASSWORD**) |) |)**
The length of user (user name) ranges from 1-31. user is used for the SNMPv3 version.
The user does not need to be associated with the group. At this time, the access scope is readable and writable to all MIB nodes.
The encrypted keyword is used when flashing the configuration, and this keyword is not used when configuring.
The auth parameter and the priv parameter are optional parameters. The auth parameter is used to configure the security authentication algorithm, MD5 or SHA, and the password for security authentication; the priv parameter is used to configure the packet encryption algorithm, AES and

DES, and encrypted password. The length range of the authentication password and encryption password is 8-31.
The security model of the user is determined according to the auth and priv parameters. If the auth and priv parameters are not configured, the security model is noauth. If the auth parameter is configured without the priv parameter, the security model is auth. If both auth and priv are configured Parameter, the security model is priv.
If the user configures the associated group, the user must be associated with a group that exists and the version is v3. If the group does not exist or the version does not match, the user will not be created successfully. Similarly, if the group associated with the user is deleted, the user will be automatically deleted.
After the user associates with the group, the read and write MIB node range will be determined by the range defined by the group (actually determined by the view associated with the group).
Since both users and their associated groups have defined security models, the security models that can be used when accessing SNMP agents are shown in the following table:

User security model	Group security model	Available access security models
noauth	noauth	noauth
noauth	auth	无
noauth	priv	无
auth	noauth	noauth，auth
auth	auth	auth
auth	priv	无
priv	noauth	noauth，auth, priv
priv	auth	auth,priv
priv	priv	priv

The security model of user cannot be configured lower than that of group. For example, the security model of the group is auth and the security model of the user is noauth, and the security model actually required is auth, but at this time the user has not configured the auth parameter, therefore, the user cannot access any MIB nodes.
Use the command "no snmp-server user WORD" when deleting user.

Configure SNMP host

SWITCH(config)#**snmp-server host (**A.B.C.D **| **X:X::X:X**) (traps | informs) (v1 | v2c | v3 (auth | noauth | priv))** WORD **(udp-port** <1-1024> **|)**

Host refers to the server that receives SNMP traps. It can be represented by an ipv4 address or an ipv6 address.
The message sent can be trap or inform.
The parameter (v1 | v2c | v3 (auth | noauth | priv)) is used to determine the SNMP version and security model corresponding to the sent message.
The WORD parameter represents the community name (community) or user name (user) that sends the message. The corresponding v1 and v2c versions use community, and the corresponding v3 version uses user.
The optional parameter udp-port indicates that a non-default udp port number is used to send messages. The default udp port number is 162.
Support for configuring multiple hosts at the same time. The key of the host is the ip address, the message type (traps or information) and the corresponding SNMP version. That is, if the same ip address, message type or corresponding SNMP version is different, multiple hosts can be configured at the same time.

Only one community or user can be configured on a host. Indicates which community or user is used to send the message.

To delete the host, use the command "no snmp-server host (A.B.C.D | X:X::X:X) (traps | informs) (v1 | v2c | v3)".

Configure the use of TCP sessions

SWITCH(config)#**snmp-server tcp-session**

SNMP is based on UDP protocol by default, but it can be configured based on TCP protocol.

To restore based on UDP protocol, use the command "no snmp-server tcp-session".

Configure to close the trap

SWITCH(config)#**no snmp-server trap enable**

SNMP turns on the trap by default, but you can turn off the trap (including inform) of the corresponding agent through the above command.

To restore the enable trap, use the command "snmp-server trap enable".

Configure the contact information of SNMP agent

SWITCH(config)#**snmp-server contact** EMAIL

This attribute corresponds to the MIB node ".1.3.6.1.2.1.1.4.0".

Configure the address of the SNMP agent

SWITCH(config)#**snmp-server location** LOCATION

This attribute corresponds to the MIB node ".1.3.6.1.2.1.1.5.0".

10.3. Configuration case

Configure SNMP Agent:

- For SNMPv2c, configure the read-only community as ro-com; configure the OID-Tree as .1.3.6.1.2.1 and the read-write community as com-mib.
- SNMPv3, configure user-root (noauth) that can read and write all MIBs; configure user-ro (noauth) that can read all MIBs; configure OID-Tree as the readable and writable user user-of .1.3.6.1.2. 1 (noauth); the configuration can read all MIBs, and can write user-2 (auth) and user-3 (priv) of all MIBs except OID-Tree which is .1.3.6.1.2.1.2.

Configure SNMP Trap host:

- Configure IPv4 host 192.168.1.100 traps, corresponding to user-2; host 192.168.2.100 informs, corresponding to community com-mib.
- Configure IPv6 host [2060::5] informs, corresponding to user-3.

The configuration corresponding to the above configuration requirements is as follows:

```
SWITCH#configure terminal
SWITCH(config)# snmp-server view mib2 .1.3.6.1.2.1 include
SWITCH(config)# snmp-server view except-if .1.3.6.1.2.1.2 exclude
SWITCH(config)# snmp-server group v2c-g-mibs read mib2 write mib2
SWITCH(config)# snmp-server group v3-ro-g v3 noauth write null
SWITCH(config)# snmp-server group v3-g-mibs v3 noauth read mib2 write mib2
SWITCH(config)# snmp-server group v3-g-w-except-if v3 noauth write except-if
```

```
SWITCH(config)# snmp-server community ro-com ro
SWITCH(config)# snmp-server community com-mib group v2c-g-mibs
SWITCH(config)# snmp-server user user-root
SWITCH(config)# snmp-server user user-ro group v3-ro-g
SWITCH(config)# snmp-server user user-1 group v3-g-mibs
SWITCH(config)# snmp-server user user-2 group v3-g-w-except-if auth sha test-passwd
SWITCH(config)# snmp-server user user-3 group v3-g-w-except-if auth md5 test-passwd
priv des test-passwd
SWITCH(config)# snmp-server host 192.168.1.100 traps v3 auth user-2
SWITCH(config)# snmp-server host 192.168.2.100 informs v2c com-mib
SWITCH(config)# snmp-server host 2060::5 informs v3 priv user-3
```

10.4. Show command

show snmp-server (user | community | group | view | host |) If you carry user, or community, or group, or view, or host, only the configuration information of the corresponding item will be viewed. If it does not carry any parameters, then all configurations will be viewed information.

```
SWITCH#show snmp-server
SNMP TCP Session: Disable
SNMP Trap: Enable
SNMP server view configuration
------------------------------------------------------------------
View                    OID                                 Type
------------------+------------------------------+---------
mib2                    .1.3.6.1.2.1                      include
except-if             .1.3.6.1.2.1.2                    exclude

SNMP server group configuration
------------------------------------------------------------------
Group                   Ver    Sec mod RView                WView
------------------+-----+-------+------------------+------------------
v2c-g-mibs            v2c    noauth   mib2                  mib2
v3-ro-g               v3     noauth                         null
v3-g-mibs             v3     noauth   mib2                  mib2
v3-g-w-except-if      v3     noauth                         except-if
```

SNMP server community configuration

```
------------------------------------------------------------------------
Community                Group
------------------+-----------------
ro-com                   [def]:ro
com-mib                  v2c-g-mibs
```

SNMP server user configuration

```
------------------------------------------------------------------------
User                     Auth     Priv     Group
------------------+-------+-------+-----------------
user-root                                 [def]:noauth
user-ro                                   v3-ro-g
user-1                                    v3-g-mibs
user-2                   sha              v3-g-w-except-if
user-3                   md5      des     v3-g-w-except-if
```

SNMP trap/inform host configuration

```
------------------------------------------------------------------------
Host Ipaddr                              Type     Ver + Secm   User/Community
---------------------------------+-------+----------+-----------------
192.168.1.100                            trap     v3 auth      user-2
192.168.2.100                            inform   v2c          com-mib
2060::5                                  inform   v3 priv      user-3
```

11. CONFIGURE RMON

11.1. RMON overview

SNMP is the most widely used network management protocol in the Internet. It realizes the collection and statistics of network communication information through the agent software embedded in the device. The management software sends a query signal to the MIB of the agent through polling to obtain this information, and realizes the management of the network through the obtained information. Although the MIB counter records the sum of statistical data, it cannot perform historical analysis of daily communications. In order to be able to comprehensively view the flow of the day and the changes in the flow, the network management software needs to continuously poll to analyze the status of the network through the information obtained.

There are two obvious disadvantages of polling with SNMP:

- Occupies a lot of network resources. In a large network, a large number of network communication messages will be generated through polling, which will cause network congestion or even network congestion, so SNMP is not suitable for managing large networks , Not suitable for recycling large amounts of data, such as routing table information.

- It increases the burden on the administrator. The task of collecting data in SNMP polling is completed by the network administrator through the network management software. If the network administrator monitors more than 3 network segments, it may happen that the network is overloaded. The situation where the manager cannot complete the task.

In order to improve the availability of management information, reduce the burden of the management station, and meet the needs of network administrators to monitor the performance of multiple network segments, IETF developed RMON to solve the limitations of SNMP in the ever-expanding distributed interconnection. The monitoring function of the data flow of the network segment and even the entire network. The following are the characteristics of RMON:

- SNMP is the basis for the realization of RMON, and RMON is an enhancement of the SNMP function.

  RMON is implemented based on the SNMP architecture and is compatible with the existing SNMP framework. It is still composed of two parts: the network management workstation NMS and the agent running on each network device. Because RMON does not use another set of mechanisms, the network management workstation NMS and SNMP are shared, and network administrators do not need to perform additional learning, so the implementation is relatively simple.

- RMON enables SNMP to monitor remote network equipment more effectively and proactively, and provides an efficient means for monitoring the operation of the network.

  The RMON protocol stipulates that the managed device can automatically send Trap information when the alarm threshold is reached, so the management device does not need to poll multiple times to obtain the value of the MIB variable for comparison, which can reduce the communication traffic between the management device and the managed device, and achieve simple and convenient The purpose of effectively managing large-scale interconnection networks.

RMON allows multiple monitors, and the monitors can collect data in the following two ways:

- Through a dedicated RMON Probe (detector), NMS directly obtains management information from RMON Probe and controls network resources. In this way, all information of RMON MIB can be obtained.

- Embed RMON Agent directly into network devices, making them become network devices with RMON Probe function. NMS uses SNMP to exchange data and information with it and collect network management information. This method is limited by device resources. Generally, it is

impossible to obtain all the data of RMON MIB, and basically only collects the information of four groups (alarms, events, history, and statistics).

Our equipment adopts the second method to realize the RMON Agent function on the equipment. Through this function, the management device can obtain the overall traffic, error statistics, performance statistics and other information on the network segment connected to the managed network device interface, thereby realizing network monitoring.

11.2. RMON related concepts

Before configuring RMON, you need to understand the basic concepts of the four groups of statistics, history, alarms, and events defined by the RMON specification.

RMON features

RMON mainly implements statistics and alarm functions, which are used for remote monitoring and management of managed devices by management devices in the network.

The statistics function of RMON can be realized through RMON statistics group or RMON history group, which is divided into Ethernet statistics function and historical statistics function.

- Ethernet statistics function (corresponding to the statistics group in the RMON MIB): The system collects basic statistics of each network being monitored. The system will continuously count the traffic of a certain network segment and the distribution of various types of packets, or the number of various types of error frames, the number of collisions, etc. The statistical objects include the number of network collisions, the number of CRC error packets, and the number of packets that are too small ((Or very large) data packets, broadcast, multicast packets, received bytes, received packets, etc.

- Historical statistics function (corresponding to the historical group in the RMON MIB): The system regularly collects network status statistics and stores them for subsequent processing. The system will perform statistics on various traffic information periodically and periodically. The statistics include bandwidth utilization, number of error packets, and total packets, etc.

The RMON alarm function includes event definition function and alarm threshold setting function. The combination of these two sub-functions realizes the RMON alarm function.

- Event definition function (corresponding to the event group in the RMON MIB): The event group controls the events and prompts from the device, and provides all events generated by the RMON Agent. When an event occurs, you can record a log or send a trap to the network management station.

- Set alarm threshold function (corresponding to the alarm group in the RMON MIB): The system monitors the specified alarm variable (the OID corresponding to any alarm object). After the user predefines a set of thresholds and sampling time for the specified alarm, the system will obtain the value of the specified alarm variable according to the defined time period. When the value of the alarm variable is greater than or equal to the upper threshold, an upper alarm event is triggered; when an alarm If the value of the variable is less than or equal to the lower threshold, a lower alarm event is triggered. The RMON Agent will record the above monitored status as a log or send a trap to the network management station.

Multiple RMON groups are defined in the RMON specification (RFC2819), and the device implements the four groups of statistics, history, alarms, and events supported in the public MIB. These groups are introduced separately below.

- Statistics Group

The statistics group stipulates that the system will continuously perform statistics on various traffic information of the Ethernet interface, and store the statistical results in the Ethernet statistics table

(etherStatsTable) so that the management device can view it at any time. The statistical information includes the number of network conflicts, the number of CRC check error packets, the number of too small (or very large) data packets, the number of broadcast and multicast packets, the number of received bytes, and the number of received packets.

After the statistics entry is successfully created under the specified interface, the statistics group will count the number of packets on the current interface. The result of the statistics is a continuous cumulative value.

- History group

The history group regularly collects and stores network status statistics for subsequent processing.

The history group contains two tables:

- History Control Table: Mainly used to set control information such as sampling interval time.
- Ethernet History Table: It is mainly used to store the historical group periodically collecting network status statistics, and provide network administrators with historical data about network segment traffic, error packets, broadcast packets, utilization, and collision times and other statistical information.

- Event group

The events defined by the event group are used in the configuration items of the alarm group and the configuration items of the extended alarm group. When the monitored object reaches the alarm condition, the event will be triggered. RMON event management is to add events in the specified row of the event table and define the processing methods of the events:

- log: Only send logs
- trap: Only send Trap messages to NMS
- log-trap: Send both logs and Trap messages to NMS
- none: do nothing

- Alarm group

The alarm group allows a set of thresholds to be pre-defined for monitoring of alarm variables (which can be any object of the local MIB). After the user defines the alarm table item (alarmTable), the system will obtain the value of the monitored alarm variable according to the defined time period. When the value of the alarm variable is greater than or equal to the upper threshold, an upper limit alarm event is triggered; If the value is less than or equal to the lower limit threshold, a lower limit alarm event is triggered, and the alarm management will deal with it according to the definition of the event.

11.3. Configuration command

Configure RMON statistics group

SWITCH(config)#**rmon statistics** <1-65535> **interface** IFNAME (**owner** OWNERNAME |)

statistics <1-65535>: Statistics group index;

owner OWNERNAME: owner information;

Configure RMON history group

SWITCH(config)# **rmon history** <1-65535> **interface** IFNAME **buckets** <1-65535> **interval** <1-3600> (**owner** OWNERNAME |)

history <1-65535>: history group index;

buckets <1-65535>: historical bucket size;

interval <1-3600>: recording period; the unit is seconds;
owner OWNERNAME: owner information;
Configure RMON event group
SWITCH(config)# **rmon event** <1-65535> **(description** DESCRIPTION**|) (log | trap** COMMUNITY **| log-trap** COMMUNITY **| none)** (**owner** OWNERNAME **|**)
event <1-65535>: Event group index
description DESCRIPTION: event description;
trap COMMUNITY: Trap communication community word, only Trap;
log-trap COMMUNITY: Trap communication community word, Log and Trap are generated at the same time;
owner OWNERNAME: owner information;
Configure alarm group
SWITCH(config)# **rmon alarm** <1-65535> **object** STRING <1-65535> (**absolute | delta) rising-threshold** <1-2147483645> <1-65535> **falling-threshold** <1-2147483645> <1-65535> **(owner** OWNERNAME **|**)
alarm <1-65535>: alarm group index;
object STRING: OID of alarm monitoring, for example, 1.3.6.1.2.1.2.2.1.10.1 represents the number of bytes received by monitoring interface 1;
<1-65535>: monitoring period, in seconds;
absolute | delta: sampling type, absolute value or difference value;

rising-threshold <1-2147483645>: rising threshold;
<1-65535>: rising event index; corresponding to the index in the event group;
falling-threshold <1-2147483645>: falling threshold;
<1-65535>: the index of the falling event; the index in the corresponding event group;
owner OWNERNAME: owner information;
Configure the upper limit of log entries
SWITCH(config)# **rmon max-log** <1-65535>
max-log <1-65535>: the upper limit of the number of log entries;
The log here refers to the log generated by the event group, not the system log;
The default upper limit is 100; when the number of generated logs exceeds the limited number of entries, the old logs will be deleted according to the generation time to maintain the upper limit;

11.4. Configuration case

The IP address of the SNMP network management server is 2.2.2.2, and the read-write communication community is unified as public.

The network management server needs to query the traffic of device port 1 through rmon.

The network management server needs to monitor the input traffic of device port 1 through rmon, with a period of 10 seconds. Once the number of input traffic bytes changes more than 1MB (1000000B), an alarm is triggered and the log is recorded.

```
SWITCH#configure terminal
SWITCH(config)#snmp-server community public
SWITCH(config)#snmp-server 2.2.2.2 community public
SWITCH(config)# rmon statistics 1 interface GigabitEthernet0/1 owner abc
```

```
SWITCH(config)# rmon event 1 log-trap public owner abc
SWITCH(config)# rmon alarm 1 object 1.3.6.1.2.1.2.2.1.10.1 10 delta rising-threshold 1000000 1 falling-threshold 1000000 1
```

11.5. Show command

Show event group log

SWITCH#**show rmon log**

12. CONFIGURE IGMP SNOOPING

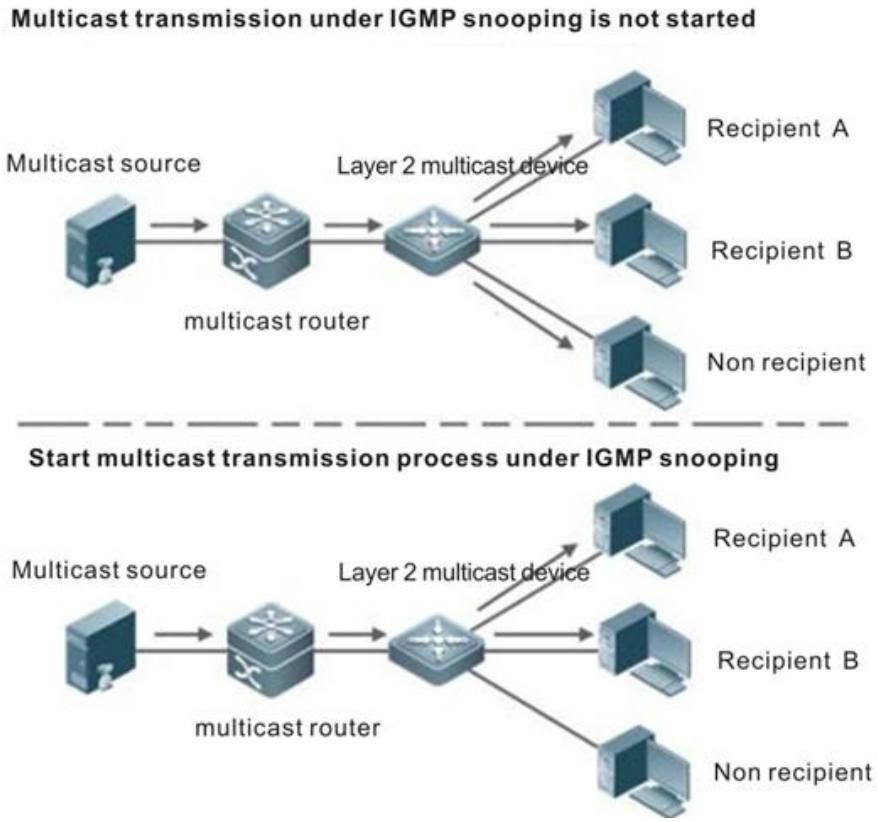
The corresponding web network management configuration path is: Home -> Exchange -> IGMP Snooping

12.1. Overview of IGMP Snooping

IGMP Snooping is the abbreviation of Internet Group Management Protocol Snooping. It is a multicast restriction mechanism running on Layer 2 devices and is used to manage and control multicast groups.

A Layer 2 device running IGMP Snooping analyzes the received IGMP messages, establishes a mapping relationship between ports and MAC multicast addresses, and forwards multicast data according to this mapping relationship. When the Layer 2 device does not run IGMP Snooping, the multicast data is broadcast at Layer 2. When the Layer 2 device runs IGMP Snooping, it is known that the multicast data of the multicast group will not be broadcast at Layer 2, but at Layer 2. It is multicast to the designated recipients.

As shown in the figure below, when the Layer 2 multicast device is not running IGMP Snooping, IP multicast packets are broadcast in the VLAN; when the Layer 2 multicast device is running IGMP Snooping, IP multicast packets are only sent to group members Receiver.



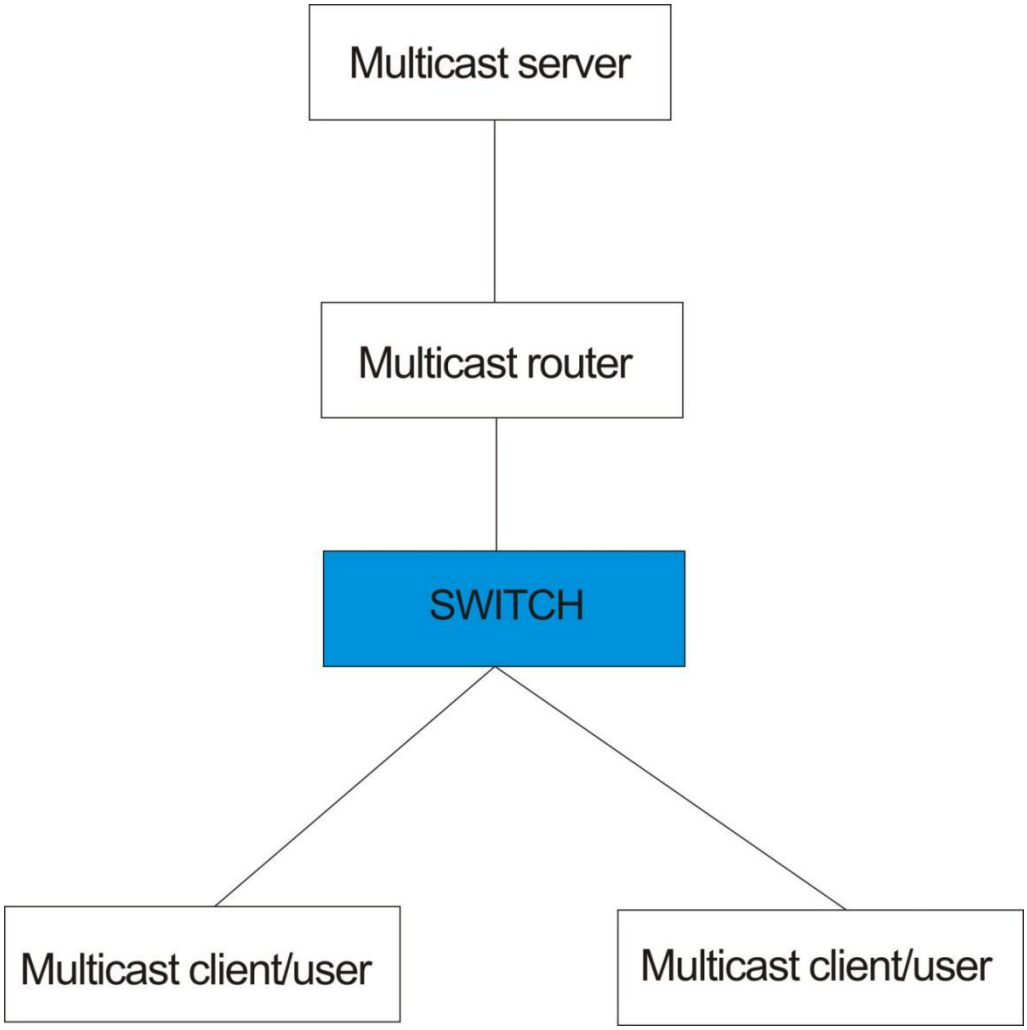
12.2. Configuration command

Enable IGMP Snooping on the port
SWITCH(config-if)#**igmp snooping**
Off by default;

Only support configuration on SVI interface;
Configure IGMP Snooping upstream port
SWITCH(config-if)#**igmp snooping mrouter interface** IFNAME
Only supports configuration on SVI interface;
The upstream port is a physical port;
Configure IGMP Snooping static group
SWITCH(config-if)#**igmp snooping static-group** IPADDR **source** IPADDR **interface** IFNAME
Only supports configuration on SVI interface;
The associated interface of the static group is a physical interface;
Configure IGMP Snooping fast leave
SWITCH(config-if)#**igmp snooping fast-leave**
Only supports configuration on SVI interface;

12.3. Configuration case

Simplify the topology:



Basic configuration/role: (from top to bottom)

Server configuration

The multicast service needs to be enabled. During the test, VLC was used as the multicast server to provide the multicast service: udp://225.0.0.1:1234, server IP 3.3.3.10

Router configuration

Run the multicast routing protocol and enable IGMP, and use Ruijie S57 Layer 3 switch to simulate during the test. The main configuration is as follows:

ip multicast-routing // enable multicast routing

interface GigabitEthernet 0/23 // On the chain, connect to the server

no switchport

no ip proxy-arp

ip pim dense-mode // Here is a simple selection of PIM dense mode. The actual network scale is large, and the sparse mode is recommended to use less multicast. For specific configuration, please refer to the configuration document of the corresponding device.

ip address 3.3.3.3 255.255.255.0

interface Vlan1 // Downlink

no ip proxy-arp

ip pim dense-mode // Here is a simple selection of PIM dense mode. The actual network scale is large, and the sparse mode is recommended to use less multicast. For specific configuration, please refer to the configuration document of the corresponding device.

ip address 2.2.2.1 255.255.255.0

SWITCH configuration

Enable multicast

```
SWITCH(config-if)#igmp snooping
```

Client configuration

Watch the server multicast video through udp://225.0.0.1:1234, IP 2.2.2.10

12.4. Show command

View IGMP Snooping multicast groups

SWITCH#**show igmp snooping groups**

View IGMP Snooping interface information

SWITCH#**show igmp snooping interface** IFNAME

```
IGMP Snooping information for Vlan1
  IGMP Snooping enabled
```

```
Snooping Querier none
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression enabled
IGMPv3 Report suppression enabled
Router port detection using IGMP Queries
Number of router-ports: 2
Number of Groups: 2
Number of Joins: 891
Number of Leaves: 4
Active Ports:
  GigabitEthernet0/1
  GigabitEthernet0/2
```

View IGMP Snooping routing port information

SWITCH#**show igmp snooping** mrouter SVI

```
SWITCH#show igmp snooping mrouter Vlan1
VLAN      Interface                IP-address      Expires
1         GigabitEthernet0/18(dynamic)          2.2.2.1         00:03:34
          GigabitEthernet0/20(static)           --              --
```

View IGMP Snooping packet statistics

SWITCH#**show igmp snooping statistics interface** SVI

```
SWITCH#show igmp snooping statistics interface Vlan1
IGMP Snooping statistics for Vlan1
  Group Count                 :  2
  IGMP reports received   :  893
  IGMP leaves received    :  4
  IGMPv1 query warnings   :  0
  IGMPv2 query warnings   :  456
  IGMPv3 query warnings   :  0
```

13. CONFIGURE STP SPANNING TREE PROTOCOL

The corresponding web network management configuration path is: Home -> Exchange -> Spanning Tree

13.1. STP overview

Spanning Tree Protocol is a layer 2 management protocol, which eliminates layer 2 loops by selectively blocking redundant links in the network. It also has the function of link backup.

Like the development process of many protocols, the Spanning Tree Protocol is constantly updated with the development of the network, from the original STP (Spanning Tree Protocol) to RSTP (Rapid Spanning Tree Protocol), and then To the latest MSTP (Multiple SpanningTree Protocol).

For Layer 2 Ethernet, there can only be one active path between two LANs, otherwise a broadcast storm will occur. However, in order to enhance the reliability of a local area network, it is necessary to establish redundant links. Some of the paths must be in a backup state. If the network fails and another link fails, the redundant link must be upgraded to Active status. Manually controlling such a process is obviously a very hard work, and the STP protocol automatically completes this work. It enables the devices in a local area network to perform the following functions:

Discover and start an optimal tree topology of the local area network.

Discovery of failures and subsequent recovery, automatically update the network topology, so that the best possible tree structure is selected at any time.

13.2. Configuration command

Configure STP mode

SWITCH(config)#**spanning-tree mode** (**stp | rstp | mstp**)

stp：Spanning tree protocol(IEEE 802.1d);

rstp：Rapid spanning tree protocol(IEEE 802.1w);

mstp：Multiple spanning tree protocol(IEEE 802.1s) ;

The default is rstp mode. After the mode is switched, the spanning tree protocol is closed by default and needs to be re-enabled;

Enable STP

SWITCH(config)#**spanning-tree enable**

Off by default;

Configure STP priority

SWITCH(config)#**spanning-tree priority** <0-61440>

Default priority: 32768;

In MSTP mode, it indicates the priority of instance 0;

Configure MST instance priority

SWITCH(config)#**spanning-tree instance** <1-63> **priority** <0-61440>

Default priority: 32768;

Only valid in MSTP mode;

Configure the period for sending STP BPDU packets

SWITCH(config)#**spanning-tree hello-time** <1-10>

The unit is seconds; the default is 2s;

Configure the STP port forwarding state delay time

SWITCH(config)#**spanning-tree forward-time** <4-30>

The unit is seconds; the default is 15s;

Configure the life cycle of STP BPDU packets

SWITCH(config)#**spanning-tree max-age** <6-40>

The unit is seconds; the default is 20s;

Hello Time, Forward-Delay Time, Max-Age Time need to follow the conditions: 2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0seconds), otherwise it may cause topology Unstable.

Configure the maximum number of hops for STP BPDU packets
SWITCH(config)#**spanning-tree max-hops** <1-40>
The default is 20;
Configure the maximum number of BPDU packets sent per second
SWITCH(config)#**spanning-tree transmit-holdcount** <1-10>
The default is 6;
Configure STP BPDU Guard
SWITCH(config)#**spanning-tree portfast bpdu-guard**
Enable BPDU Guard globally, which only takes effect for ports that enable STP port fast forwarding; Off by default;
Configure STP BPDU Filter
SWITCH(config)#**spanning-tree portfast bpdu-filter**
Enable BPDU Filter globally, which only takes effect for ports that enable STP port fast forwarding; Off by default;
Configure the wrong port timeout recovery function
SWITCH(config)#**spanning-tree errdisable-timeout enable**
It is closed by default; that is, the wrong port will never automatically recover after timeout, and must be recovered manually;

Configure the wrong port timeout recovery interval
SWITCH(config)#**spanning-tree errdisable-timeout interval** <10-1000000>
Time interval: the unit is second, the default is 300 seconds;
Enter MST mode
SWITCH(config)#**spanning-tree mst configuration**
Configure the correspondence between MST VLAN and instance
SWITCH(config-mst)# **instance** <1-63> **vlan** VLANID
The instance ID configured for the first time will be created at the same time.
Configure MST area name
SWITCH(config-mst)#**region** NAME
Configure the MST version number
SWITCH(config-mst)#**revision** <0-65535>
The default is 0;
Enable port STP
SWITCH(config-if)#**spanning-tree enable**

Turn on by default;

Configure the association relationship between the port and the MST instance

SWITCH(config-if)# **spanning-tree instance** <1-63>

By default, when configuring the relationship between the instance and the VLAN, the system will automatically generate the relationship data between the port and the instance according to the relationship between the VLAN and the port, without manual configuration;

After the instance configuration is ready, if there is a manual modification of the port and VLAN relationship, such as adding/exiting all the VLANs of an instance, you need to manually maintain the relationship between the port and the instance through this command;

When major configuration changes occur, it is recommended to reconfigure the instance-VLAN relationship or restart the device to automatically generate port and instance data;

Configure port STP priority

SWITCH(config-if)#**spanning-tree priority** <0-240>

The priority must be configured as a multiple of 16;

Default priority: 128;

In MSTP mode, it indicates the priority of instance 0;

Configure port MST instance priority

SWITCH(config-if)#**spanning-tree instance** <1-63> **priority** <0-240>

Default priority: 128;

The priority must be configured as a multiple of 16;

Only valid in MSTP mode;

Configure port STP path cost

SWITCH(config-if)#**spanning-tree path-cost** <1-200000000>

Configure port STP link type

SWITCH(config-if)#**spanning-tree link-type** (**auto | point-to-point | shared**)

auto: Automatic setting mode based on the duplex capability of link negotiation, full duplex is a point-to-point connection;

point-to-point: enable fast Forwarding;

shared: Prohibit fast Forwarding;

The default is auto;

Configure port STP port fast forwarding

SWITCH(config-if)#**spanning-tree portfast**

Indicates that the device directly connected to the port is not a bridge device and can be forwarded quickly;

Off by default;

Configure the port as an STP edge port

SWITCH(config-if)#**spanning-tree edgeport**

The command effect is equivalent to spanning-tree portfast

Configure port STP edge port detection

SWITCH(config-if)#**spanning-tree autoedge**

Indicates that the port automatically recognizes whether it is an edge port according to the BPDU;

Configure port STP Root Guard

SWITCH(config-if)#**spanning-tree guard root**

Configure port STP BPDU Guard
SWITCH(config-if)#**spanning-tree bpdu-guard enable**
After opening BPDU Guard on the port, if BPDU is received on the port, it will enter the Error-disabled (blocked) state;

It is valid only when the STP port fast forwarding is enabled on the port at the same time;
Configurable status: enable, disable, default;

The default mode is default, and the global BPDU Guard configuration status determines whether the function is enabled.

Once enable or disable is configured, the current state configuration of the port shall prevail (ie global failure);

Configure port STP BPDU Filter
SWITCH(config-if)#**spanning-tree bpdu-filter enable**
After opening the BPDU Filter, the port neither sends BPDUs nor receives BPDU packets;

It is valid only when the STP port fast forwarding is enabled on the port at the same time;
Configurable status: enable, disable, default;

The default mode is default, and the configuration status of the global BPDU Filter determines whether the function on the port is enabled.

Once enable or disable is configured, the current state configuration of the port shall prevail (ie global failure);

Configure port STP topology change notification limit
SWITCH(config-if)#**spanning-tree restricted-tcn**
After the STP topology change notification restriction is enabled, the port does not forward TC BPDUs or refresh the address table;

In MSTP mode, it indicates the priority of instance 0;

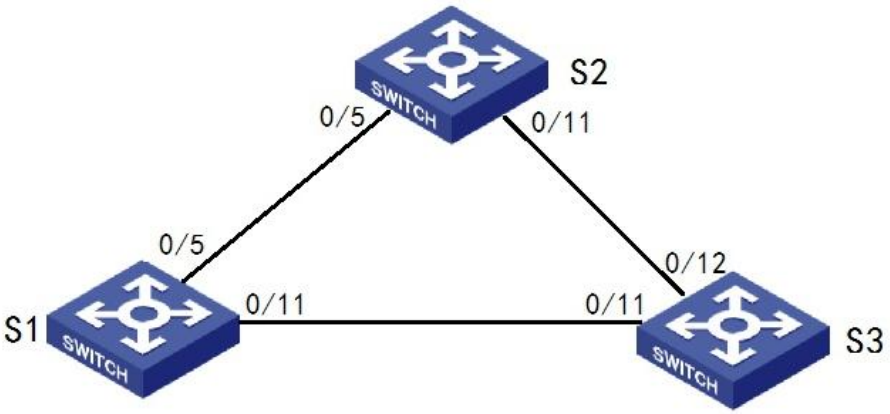
Configure the port MST instance topology change notification limit
SWITCH(config-if)#**spanning-tree instance** <1-63> **restricted-tcn**
After the STP topology change notification restriction is enabled, the port does not forward TC BPDUs or refresh the address table;

Only valid in MSTP mode;
Mandatory STP version check on all ports
SWITCH#**clear spanning-tree detected protocols**

13.3. Configuration case

Case 1: RSTP anti-loop realizes link redundancy scheme

Simplify the topology:

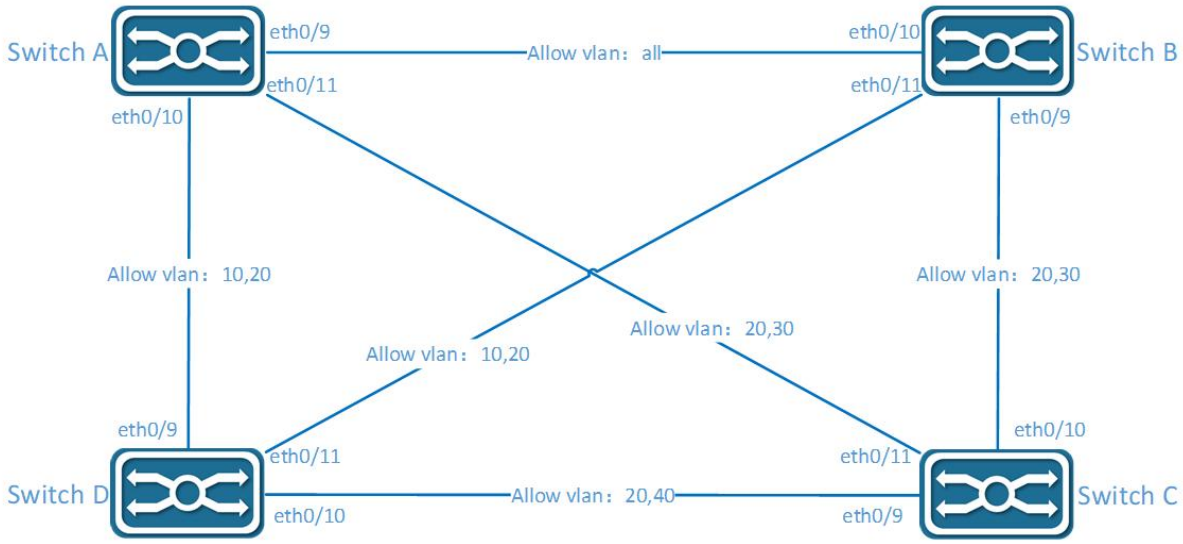


Switch S1, S2, S3 reference configuration

```
SWITCH(config)#spanning-tree mode rstp
SWITCH(config)#spanning-tree enable
```

Case 2: MSTP realizes loop prevention and link redundancy based on domains and instances

Simplify the topology:



Configuration planning

The devices belong to the same domain. The default domain is used here, and no additional configuration is required.

VLAN 20 is a shared VLAN and is directly included in the CST.

Instance	VLAN
0	20
1	10

3	30
4	40

Switch A reference configuration

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface GigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#interface GigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
SWITCH(config)#interface GigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30

SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40

SWITCH(config)#spanning-tree enable
```

Switch B reference configuration

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface GigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
SWITCH(config)#interface GigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#interface GigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
```

```
SWITCH(config-if)#switchport trunk allowed vlan 10,20

SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40

SWITCH(config)#spanning-tree enable
```

Switch C reference configuration

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface GigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,40
SWITCH(config)#interface GigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
SWITCH(config)#interface GigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30

SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40

SWITCH(config)#spanning-tree enable
```

Switch D reference configuration

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface GigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
SWITCH(config)#interface GigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,40
SWITCH(config)#interface GigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20


SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
# 启用 MSTP
SWITCH(config)#spanning-tree enable
```

13.4. Show command

View STP status
SWITCH#**show spanning-tree**

View MSTP instance status
SWITCH#**show spanning-tree mst instance** <1-63>

14. CONFIGURE ACL

The corresponding web network management configuration path is: Home->Security->ACL

14.1. ACL overview

ACL (Access Control List) realizes the function of packet filtering by configuring matching rules and processing operations for packets. It can effectively prevent illegal users from accessing the network, and at the same time can control the flow and save network resources.

The packet matching rules defined by ACL can also be referenced by other functions that need to distinguish traffic, such as the definition of traffic classification rules in QoS.

ACL classifies data packets through a series of matching conditions. These conditions can be SMAC, DMAC, SIP, DIP, etc. of the data packet. According to the matching conditions, ACLs can be divided into the following types:

Standard IP-based ACL: Only formulate rules based on the source IP address of the data packet.

IP-based extended ACL: formulate rules based on the source IP address, destination IP address, ETYPE, and protocol of the data packet.

MAC-based ACL: Formulate rules based on the source MAC address and destination MAC address of the data packet.

Namable ACL: the rules are the same as the standard ACL and extended ACL based on IP.

14.2. Configuration command

Configure standard IP-based ACL

SWITCH(config)#**ip-access-list** (<1-99> **|** <1300-1999>) (**permit** | **deny)** (SIPADDR SIPADDRMASK | **any**)

Configure IP-based extended ACL

SWITCH(config)# **ip-access-list** (<100-199> | <2000-2699>) (**permit** | **deny**) TYPE (SIPADDR SIPADDRMASK | **any)** (DIPADDR DIPADDRMASK | **any**)

TYPE list:

<0-255>: Specify the ID of the protocol;

any: any protocol message;

gre: GRE message;

igmp: IGMP message;

ip: IPv4 message;

ipcomp: IPComp message;

ospf: OSPF message;

pim: PIM message;

rsvp: RSVP message;

tcp: TCP message;

udp: UDP message;

vrrp: VRRP message;

Configure standard IP namable ACL

SWITCH(config)#**ip-access-list standard** ACLNAME (**permit** | **deny)** (SIPADDR SIPADDRMASK | **any**)

Configure extended IP namable ACL

SWITCH(config)#**ip-access-list extended** ACLNAME (**permit** | **deny)** TYPE (SIPADDR SIPADDRMASK | **any)** (DIPADDR DIPADDRMASK | **any)**

TYPE list:

<0-255>: Specify the ID of the protocol;

any: any protocol message;

gre: GRE message;

igmp: IGMP message;

ip: IPv4 message;

ipcomp: IPComp message;

ospf: OSPF message;

pim: PIM message;

rsvp: RSVP message;

tcp: TCP message;

udp: UDP message;

vrrp: VRRP message;

- Up to 128 rules can be configured under a single ACL-ID;
- The mask is reversed. For example, if you need to match an IP address in the 192.168.1.0/24 range, you should configure it as: 192.168.1.0 0.0.0.255;
- The ACLNAME of the ACL can be named, and the first character must not be a number;
- MAC-based ACL does not take effect for IP and ARP packets;

Configure MAC-based ACL

SWITCH(config)#**mac-access-list** <200-699> (**permit** | **deny)** (SMAC SMACMASK | **any)** (DMAC DMACMASK | **any)**

Configure ACL to be applied to the port

SWITCH(config-if)#**access-group** ACLNAME **in**

When the ACL has been applied to the port, if you need to add or delete rules, you need to cancel the application of the ACL on the port.

14.3. Configuration case

Filter the ingress packets of port GigabitEthernet0/1, pass packets with SIP 192.168.1.0/24, and discard other packets.

```
SWITCH(config)#ip-access-list 1 permit 192.168.1.0 0.0.0.255
SWITCH(config)#ip-access-list 1 deny any
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#access-group 1 in
```

14.4. Show command

Show IP-based ACL

SWITCH#**show ip-access-list** (<1-99> | <100-199> **|** <1300-1999> | <2000-2699> | ACLNAME |)

```
SWITCH#show ip-access-list 1
   Standard IP access list: 1
      permit 1.1.1.1
      deny     any
```

Show MAC-based ACL

SWITCH#**show mac-access-list** (<200-699> |)

```
SWITCH#show mac-access-list 200
   Extended MAC-ACCESS-LIST: 200
      permit host 0001.0002.0003 any
      deny     any any
```

15. CONFIGURE DHCP SNOOPING

The corresponding web network management configuration path is: Home -> Security -> DHCP Snooping

15.1. Overview of DHCP Snooping

DHCP (Dynamic Host Configuration Protocol) is a LAN network protocol, which is widely used to dynamically allocate reusable network resources. It is a means for users or internal network administrators to centrally manage all computers.

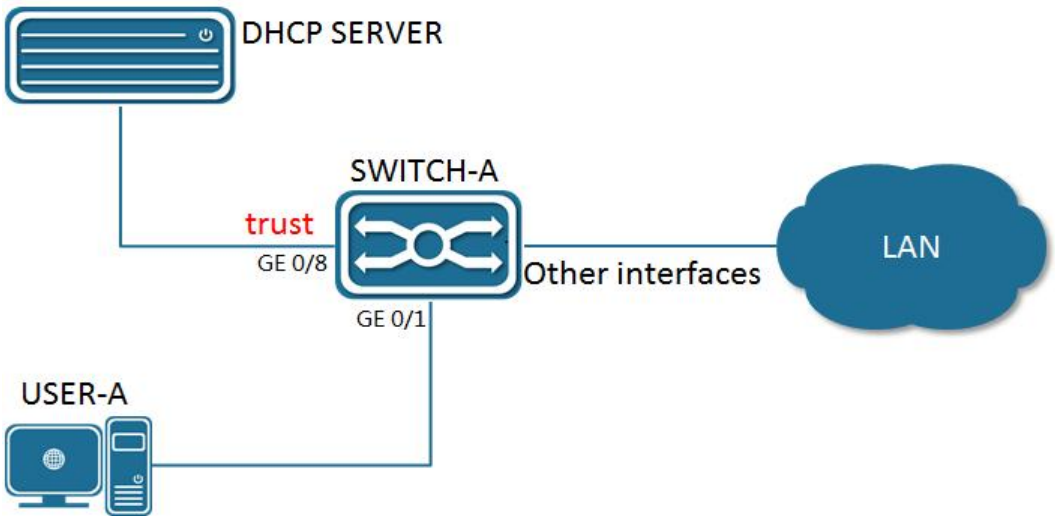
DHCP Snooping is a DHCP security technology that can isolate illegal DHCP Servers by detecting and managing DHCP exchange messages. DHCP Snooping divides ports into two types, TRUST port and UNTRUST port. The device only forwards the DHCP Offer messages received by the TRUST port, and discards all DHCP Offer messages from the UNTRUST port, thus realizing the shielding of illegal DHCP servers.

15.2. Configuration command

Configure DHCP Snooping
SWITCH(config)#**ip dhcp snooping**
Configure port DHCP Snooping trusted port
SWITCH(config-if)#**ip dhcp snooping trust**

15.3. Configuration case

For SWITCH-A, GigabitEthernet0/8 is connected to the DHCP server, and USER-A obtains an IP address dynamically. The existence of other DHCP servers in the LAN will affect the IP address allocation of USER-A.



Reference configuration

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

```
SWITCH(config)#interface GigabitEthernet0/8
SWITCH(config-if)#ip dhcp snooping trust
```

15.4. Show command

Show DHCP Snooping configuration information

SWITCH#show ip dhcp snooping

```
SWITCH#show ip dhcp snooping
IP DHCP Snooping status: Enabled

Interface                TRUSTED
------------------------------
GigabitEthernet0/1       NO
GigabitEthernet0/2       NO
GigabitEthernet0/3       NO
GigabitEthernet0/4       NO
GigabitEthernet0/5       NO
GigabitEthernet0/6       NO
GigabitEthernet0/7       NO
GigabitEthernet0/8       YES
GigabitEthernet0/9       NO
GigabitEthernet0/10      NO
GigabitEthernet0/11      NO
GigabitEthernet0/12      NO
GigabitEthernet0/13      NO
GigabitEthernet0/14      NO
GigabitEthernet0/15      NO
GigabitEthernet0/16      NO
GigabitEthernet0/17      NO
GigabitEthernet0/18      NO
GigabitEthernet0/19      NO
GigabitEthernet0/20      NO
```

GigabitEthernet0/21	NO
GigabitEthernet0/22	NO
GigabitEthernet0/23	NO
GigabitEthernet0/24	NO
TenGigabitEthernet0/25	NO
TenGigabitEthernet0/26	NO
TenGigabitEthernet0/27	NO
TenGigabitEthernet0/28	NO

16. CONFIGURE QOS

The corresponding web network management configuration path is: Homepage -> Security -> QoS, Homepage -> Interface -> Port Speed Limit

16.1. QoS overview

QoS (Quality of Service) refers to the ability of a network to use various basic technologies to provide better service capabilities for specified network communications.

Traditional networks use a "best effort" forwarding mechanism. When the network bandwidth is sufficient, all data streams are better processed. When the network is congested, all data streams may be discarded. In order to meet the different service quality requirements of different applications, the network is required to allocate and schedule resources according to user requirements and provide different service qualities for different data streams.

Devices that support QoS functions can provide transmission quality services. For a certain type of data flow, a certain level of transmission priority can be assigned to it to identify its relative importance and use the various priorities provided by the device Mechanisms such as forwarding strategies and congestion avoidance provide special transmission services for these data streams.

The network environment configured with QoS increases the predictability of network performance, effectively allocates network bandwidth, and makes more reasonable use of network resources.

16.2. Configuration command

Configure QoS
SWITCH(config)#**mls qos enable**
Off by default;

Configure queue scheduling algorithm
SWITCH(config)#**mls qos algorithm** (**sp | wrr**)
Configure queue scheduling algorithm, support 2 modes: WRR (balanced scheduling), SP (absolute scheduling);
The default is WRR mode;
Configure queue weight
SWITCH(config)#**mls qos wrr-weight** <0-7> <0-32>
Configure the queue weight, which is only valid for WRR mode;
The default weight of all queues is 1;
When in WRR mode, the configuration queue weight is 0, and the queue scheduling weight is infinite;
Configure port default Cos
SWITCH(config-if)#**mls qos cos** <0-7>
Configure the port default Cos, which takes effect for the ingress port without tag messages;
The default port Cos is 0;
Configure Cos-Dscp mapping relationship
SWITCH(config)#**mls qos cos-dscp** <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63>
Default mapping relationship: 0-0, 1-8, 2-16, 3-24, 4-32, 5-40, 6-48, 7-56;
Configure Cos-Queue mapping relationship

SWITCH(config)#**mls qos cos-queue** <0-7> <0-7>
Default mapping relationship: 0-0, 1-1, 2-2, 3-3, 4-4, 5-5, 6-6, 7-7;

When the configured port is no Trust, Trust Cos, or Trust Dscp and non-IP packets: the Cos-Dscp configuration takes effect, the packet Dscp is modified according to the mapping relationship, the Cos-Queue configuration takes effect, and the packet egress queue is modified according to the mapping relationship.

Configure Dscp-Cos mapping relationship
SWITCH(config)#**mls qos dscp-cos** <0-63> to <0-7>
Default mapping relationship: <0-7>-0, <8-15>-1, <16-23>-2, <24-31>-3, <32-39>-4, <40-47>- 5, <48-55>-6, <56-63>-7;
Configure the Dscp-Dscp mapping relationship
SWITCH(config)#**mls qos dscp-mutation** <0-63> to <0-63>
Default mapping relationship: one-to-one correspondence;
Configure Dscp-Queue mapping relationship
SWITCH(config)#**mls qos dscp-queue** <0-63> <0-7>
Configure Dscp-Queue mapping relationship
Default mapping relationship: <0-7>-0, <8-15>-1, <16-23>-2, <24-31>-3, <32-39>-4, <40-47>- 5, <48-55>-6, <56-63>-7;
Configure port QoS trust mode
SWITCH(config-if)#**mls qos trust** (**cos | dscp**)
Configure port trust mode, default No Trust;
When the port is configured in No Trust mode, the message will modify the Cos field and Dscp field of the message according to the default Cos of the port;
When the port is configured with Trust Cos, it is the same as the No Trust mode for untagged packets, and for tagged packets, select the packet with its own Cos;
When the port is configured with Trust Dscp, for IP packets, select the packet with Dscp, and for non-IP packets, it is the same as Trust Cos mode;

When the configured port is Trust Dscp and IP packets are processed: the Dscp-Cos configuration takes effect, the packet Dscp is modified according to the mapping relationship, the Dscp-Queue configuration takes effect, and the packet export queue is modified according to the mapping relationship. When Dscp-Dscp is configured at the same time, Dscp-Dscp conversion is performed first, and the result is Dscp-Cos mapping.

Configure QoS Class-map mode
SWITCH(config)#**class-map** CNAME
After creating the Class-map, it automatically enters the Class-map mode;
Configure QoS flow matching ACL
SWITCH(config-cmap)# **match access-group** ACLNAME
Configure Class-map based on ACL, support standard IP, extended IP, MAC ACL;
Configure QoS flow to match Dscp
SWITCH(config-cmap)#**match ip-dscp** <0-63>
Configure the Dscp field in the matching IP packet, up to 8 different Dscp values can be configured;

Configure QoS flow matching Cos

SWITCH(config-cmap)#**match cos** <0-7>
Configure the Cos field in the matching message, up to 8 different Cos values can be configured;

Configure QoS flow to match the Ethernet protocol
SWITCH(config-cmap)#**match ethertype** ETYPE
Match the Ethernet protocol type field of the message;
Configure QoS flow to match VLAN
SWITCH(config-cmap)#**match** (**vlan** <1-4094> | **vlan-range** <1-4094> **to** <1-4094>)
Match the configuration of packet VLAN and VLAN Range;
Configure QoS flow to match the layer 4 port number of IPv4 protocol packets
SWITCH(config-cmap)#**match layer4** (**tcp | udp**) (**source-port | destination-port**) VALUE
Support IPv4 protocol message Layer 4 port number configuration;
Configure QoS flow to match VLAN and Ethernet protocol
SWITCH(config-cmap)#**match vlan-range** <1-4094> to <1-4094> **ethertype** ETYPE
Match the VLAN Range and Ethernet protocol type of the packet at the same time;
Configure QoS Policy-map mode
SWITCH(config)#**policy-map** PNAME
After the Policy-map is created, it will automatically enter the Policy-map mode;
Configure QoS Policy-map to associate with Class-map
SWITCH(config-pmap)#**class-map** CNAME
A Policy-map is associated with up to 8 Class-maps;
Configure QoS to modify Cos policy
SWITCH(config-pmap-c)#**set cos** <0-7>
Configure QoS to modify Dscp policy
SWITCH(config-pmap-c)#**set ip-dscp** <0-63>
Configure QoS to modify VLAN policy
SWITCH(config-pmap-c)#**set vlan** <1-4094>
Configure QoS to add a new VLAN policy
SWITCH(config-pmap-c)#**nest vlan** <1-4094>
Add an outer tag to the matched message;
Configure QoS to add traffic shaping strategy
SWITCH(config-pmap-c)#**police cir** <32-1000000> **cbs** <4-31250> **exceed-action drop**

The cir value is determinable. For example, if the speed limit is 1M, then the cir value is 1024, but the cbs value is taken from the empirical value. When the cbs value is large, the flow peak is higher and the speed limit is more stable, but the average speed may be higher than the speed limit; when the cbs value is small, the flow peak is lower, and the speed limit fluctuates greatly, and the average speed may be less than the speed limit value. . It is recommended that the cbs configuration takes 4 times the value of cir and the smaller value of 31250.

Configure QoS policy to be applied on the port
SWITCH(config-if)#**service-policy input** PNAME
Only one Policy-map can be applied to an interface;
Configure port ingress rate limit
SWITCH(config-if)#**rate-limit input** <64-1000000> <32-16384>
The first parameter is limit, the unit is kbps;
The second parameter is burst, the unit is kbyte;
Configure port egress rate limit

SWITCH(config-if)#**rate-limit output** <64-1000000> <32-16384>
The first parameter is limit, the unit is kbps;
The second parameter is burst, the unit is kbyte;

In the rate limit strategy, the limit value is determinable. For example, if the rate limit is 1M, the limit value is 1024, but the burst value is taken from the empirical value. When the burst value is large, the flow peak is higher and the speed limit is more stable, but the average rate may be higher than the speed limit value; when the burst value is small, the flow peak is lower, and the speed limit fluctuates greatly, and the average rate may be less than the speed limit value. . It is recommended that the burst configuration take the smaller value of 4 times the limit and 16384.

16.3. Configuration case

On port GigabitEthernet0/1, the ingress rate is limited to 1024kbps and the egress rate is limited to 1024kbps.

```
SWITCH(config-if)#rate-limit input 1024 4096
SWITCH(config-if)#rate-limit output 1024 4096
```

For port GigabitEthernet0/1, the ingress rate is limited for the flow that meets the SIP 192.168.64.1, and the rate is limited to 1024kbps.

```
SWITCH(config)#mls qos enable
SWITCH(config)#ip-access-list 1 permit 192.168.64.1
SWITCH(config)#class-map c1
SWITCH(config-cmap)#match access-group 1
SWITCH(config-cmap)#exit
SWITCH(config)#policy-map p1
SWITCH(config-pmap)#class-map c1
SWITCH(config-pmap-c)#police cir 1024 cbs 4096 exceed-action drop
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#service-policy input p1
```

16.4. Show command

Show QoS scheduling mode, weight configuration information
SWITCH#**show mls qos algorithm**

```
SWITCH#show mls qos algorithm
```

Mls qos algorithm is WRR.

Queue-id	0	1	2	3	4	5	6	7
Weight	1	1	1	1	1	1	1	1

Show QoS Cos-map configuration information

SWITCH#**show mls qos cos-maps**

SWITCH#show mls qos cos-maps

Cos	Dscp	Queue
0	0	0
1	8	1
2	16	2
3	24	3
4	32	4
5	40	5
6	48	6
7	56	7

Show QoS Dscp-map configuration information

SWITCH#**show mls qos dscp-maps**

SWITCH#show mls qos dscp-maps

Dscp	Cos	Mutation	Queue
0	0	0	0
1	0	1	0
2	0	2	0
3	0	3	0
4	0	4	0
5	0	5	0
6	0	6	0

7	0	7	0
8	1	8	1
9	1	9	1
10	1	10	1
11	1	11	1
12	1	12	1
13	1	13	1
14	1	14	1
15	1	15	1

Show QoS port configuration information

SWITCH#**show mls qos interfaces**

```
SWITCH#show mls qos interfaces
----------------------------------------
Interface                Trust mode  Cos
----------------------------------------
GigabitEthernet0/1       Not         0
GigabitEthernet0/2       Not         0
GigabitEthernet0/3       Not         0
GigabitEthernet0/4       Not         0
GigabitEthernet0/5       Not         0
GigabitEthernet0/6       Not         0
GigabitEthernet0/7       Not         0
GigabitEthernet0/8       Not         0
GigabitEthernet0/9       Not         0
GigabitEthernet0/10      Not         0
GigabitEthernet0/11      Not         0
GigabitEthernet0/12      Not         0
GigabitEthernet0/13      Not         0
GigabitEthernet0/14      Not         0
GigabitEthernet0/15      Not         0
GigabitEthernet0/16      Not         0
```

```
GigabitEthernet0/17      Not          0
GigabitEthernet0/18      Not          0
GigabitEthernet0/19      Not          0
GigabitEthernet0/20      Not          0
GigabitEthernet0/21      Not          0
GigabitEthernet0/22      Not          0
GigabitEthernet0/23      Not          0
GigabitEthernet0/24      Not          0
TenGigabitEthernet0/25   Not          0
TenGigabitEthernet0/26   Not          0
TenGigabitEthernet0/27   Not          0
TenGigabitEthernet0/28   Not          0
```

Show QoS Class-map configuration information

SWITCH#**show class-map**

```
SWITCH#show class-map


    CLASS-MAP-NAME: c1
      Match Cos: 3
```

Show QoS Policy-map configuration information

SWITCH#**show policy-map**

```
SWITCH#show policy-map


  POLICY-MAP-NAME: p1
    State: detached


    CLASS-MAP-NAME: c1
      Match Cos: 3
      Police: Mode: SrTCM
              cir (1024 Kbps)
              cbs (4096 KBytes)
              exceed-action (drop)
```

Show QoS port speed limit configuration information

SWITCH#**show rate-limit**

```
SWITCH#show rate-limit
------------------------------------------------------------
Interface                In limit    In burst    Out limit    Out burst
------------------------------------------------------------
GigabitEthernet0/1       --          --          --           --
GigabitEthernet0/2       --          --          --           --
GigabitEthernet0/3       1024        4096        --           --
GigabitEthernet0/4       --          --          --           --
GigabitEthernet0/5       --          --          --           --
GigabitEthernet0/6       --          --          --           --
GigabitEthernet0/7       --          --          --           --
GigabitEthernet0/8       --          --          --           --
GigabitEthernet0/9       --          --          --           --
GigabitEthernet0/10      --          --          1024         4096
GigabitEthernet0/11      --          --          --           --
GigabitEthernet0/12      --          --          --           --
GigabitEthernet0/13      --          --          --           --
GigabitEthernet0/14      --          --          --           --
GigabitEthernet0/15      --          --          --           --
GigabitEthernet0/16      --          --          --           --
GigabitEthernet0/17      --          --          --           --
GigabitEthernet0/18      --          --          --           --
GigabitEthernet0/19      --          --          --           --
GigabitEthernet0/20      --          --          --           --
GigabitEthernet0/21      --          --          --           --
GigabitEthernet0/22      --          --          --           --
GigabitEthernet0/23      --          --          --           --
GigabitEthernet0/24      --          --          --           --
TenGigabitEthernet0/25   --          --          --           --
TenGigabitEthernet0/26   --          --          --           --
```

TenGigabitEthernet0/27	--	--	--	--
TenGigabitEthernet0/28	--	--	--	--

17. CONFIGURE QINQ

The corresponding web network management configuration path is: Home->Exchange->QinQ

17.1. QinQ overview

QinQ technology [also known as Stacked VLAN or Double VLAN]. The standard comes from IEEE 802.1ad, which refers to encapsulating the public network VLAN tag of a service provider network before the user message enters the service provider network, and the private network user VLAN tag in the user message is regarded as data, so that the message carries Two-layer VLAN Tag traverses the service provider network.

In the metropolitan area network, a large number of VLANs are needed to isolate users. The IEEE 802.1Q protocol only supports 4094 VLANs, which is far from meeting the demand. Through QinQ technology double-tag encapsulation, in the service provider network, messages are only transmitted according to the unique outer VLAN tag allocated on the public network, so that different private network user VLANs can be reused, which expands the number of VLAN tags that users can use. It also provides a simple Layer 2 VPN function, so QinQ technology is actually a VLAN VPN technology.

In addition to QinQ, common VLAN VPN technologies also include VLAN Mapping. The only difference between the two is that QinQ stacks VLANs, and VLAN Mapping maps VLANs.

- VLAN Stacking: From the user network to the provider network, a single tag becomes a double tag, and the C-Tag remains in the message as the inner tag; in the reverse direction, the double tag becomes a single tag.
- VLAN Mapping: From the user network to the provider network, there is still a single-layer tag, but the C-Tag becomes S-Tag; the reverse, from S-Tag to C-Tag.

17.2. Configuration instructions

QinQ is divided into three categories:

- Type A: Basic QinQ, which is enabled or disabled based on the interface. When the basic QinQ-enabled interface receives a message, it is treated as an Untag message. On the basis of the original message, a VLAN Tag of the default VLAN of the port is added.
- Type B: C-tag-based flexible QinQ, according to the C-VLAN Tag on the user side, according to the configured mapping strategy, add a layer of S-VLAN Tag on the basis of the original message. There are two options for the configuration of this type of QinQ, and only one of the two can be selected. One method is to directly configure the mapping relationship between C-VLAN and S-VLAN on the interface; the other method is to configure VLAN VPN globally (including the mapping relationship between C-VLAN and S-VLAN), and then associate the VPN on the interface. When the same mapping strategy is used for multiple interfaces, the latter configuration method is generally selected. For this type of QinQ, if the packet received by the interface is Untag, C-tag is the default VLAN Tag of the interface.
- Type C: ACL-based flexible QinQ, adding outer tags according to the configured flow policy. The configuration of this type of QinQ is placed in the "QOS" module. For details, please refer to the

"Configuring QOS" chapter. Policy-map and Class-map policy pairing: "nest vlan <1-4094>" is used to configure ACL-based Flexible QinQ.

The above three types of QinQ can be enabled on the same port at the same time, and the priority relationship is: Type C> Type B> Type A.

VLAN Mapping is divided into 1:1 VLAN Mapping and 1:N VLAN Mapping (the reverse is N:1). Currently, only 1:1 VLAN Mapping is supported. The configuration method of VLAN Mapping is: configure VLAN VPN globally, and then associate the VPN on the interface. VLAN Mapping only takes effect on tagged packets, which is very different from the QinQ function.

When configuring QinQ and VLAN Mapping, there are some points to note when configuring:

- Only the physical interface supports the configuration of QinQ and VLAN Mapping, and the aggregation interface does not.
- VLAN Mapping is only effective for tagged messages. For upstream flow, the original message must carry the tag to realize the mapping from CVLAN to SVLAN; for downstream flow, the VLAN output rule of the downstream link port must be Tag output to realize SVLAN to CVLAN. Mapping.
- When the QinQ function or VLAN Mapping function is used, it needs to be used in conjunction with the VLAN configuration. In the input and output directions, the VLAN filtering function, and the rules for whether the VLAN carries tags, are subject to the VLAN configuration. Specific requirements are as follows:
  - Both CVLAN and SVLAN need to be added to the allow list of the lower link port (connected to the Customer network), otherwise the flow will be filtered;
  - SVLAN needs to be added to the allow list of the uplink port (connected to the Provider network), otherwise the flow will be filtered;
  - For QinQ, in the downstream link port, SVLAN should be configured with Untag output so that the outer tag of QinQ downstream can be stripped;
  - For VLAN-Map, since it is only effective for Untag messages, for the downstream interface, SVLAN should be configured with Tag output, otherwise the downstream flow cannot complete the mapping from SVLAN to CVLAN.
- The globally configured VLAN VPN is either used for VLAN Stacking (QinQ) or VLAN Mapping, and cannot be applied to both at the same time.
- Since VLAN Mapping only supports 1:1 mapping, there is a VLAN VPN with N:1 mapping and cannot be associated with an interface as a VLAN Mapping VPN; similarly, if it has been associated with an interface VPN as a VLAN Mapping, the mapping relationship cannot be Change to N:1.
- The mapping relationship of VLAN Mapping must be globally consistent. Therefore, different interfaces can only be associated with the same VLAN VPN.
- On the same interface, if you need to apply VLAN Mapping and QinQ at the same time, it should be noted that the two functions need to control different CVLAN and SVLAN. The specific constraints are as follows:
  - If VLAN Mapping and basic QinQ are used together, basic QinQ takes effect, and VLAN Mapping becomes invalid.
  - If VLAN Mapping and flexible QinQ are used together, if a flow passes through the SVLAN mapped by VLAN Mapping and can be used as a CVLAN to hit the flexible QinQ mapping strategy at the

same time, then the final message will take effect with flexible QinQ, adding SVLAN as the outer layer TAG, the inner TAG remains unchanged (not the VLAN after VLAN Mapping).

- Because of the above constraints, when opening two applications on the same interface, you need to pay attention to the intersection of the VLANs controlled by the two. If there is an intersection, the packets that hit the intersection will fail when the packets are encapsulated. .

- Type B QinQ either chooses to directly configure the mapping policy under the interface or chooses to associate with the VPN, and cannot be configured at the same time.

17.3. Configuration command

Create VLAN VPN

SWITCH(config)#**vlan-vpn** VPN-NAME
SWITCH(config-vlan-vpn)#
There can be multiple VPNs in the system, and each VPN maintains an independent mapping relationship between CVLAN and SVLAN. VPN will take effect only when it is applied to the interface. A VPN can be applied to VLAN Stacking (QinQ) or VLAN Mapping, but you can only choose one of the two;

Add VPN mapping

SWITCH(config-vlan-vpn)#**cvlan** VLAN_LIST **svlan** VLANID
The valid range of VLAN_LIST and VLANID is <1,4094>, VLAN_LIST supports standard multi-vlan representation methods ("-" and "," and a combination of the two);

When no cvlan does not contain any parameters, all mapping relationships in the VPN will be cleared;

Configure basic QinQ for interface mapping

SWITCH(config-if)#**switchport vlan-stacking basic**
Basic QinQ is enabled, the packets entering from the interface all match the QinQ rules, and the mapped SVLAN is the default VLAN ID of the interface;

Configure interface QinQ mapping

SWITCH(config-if)#**switchport vlan-stacking cvlan** VLAN_LIST **svlan** VLANID
Only when the interface is not associated with a VPN, can the mapping relationship configuration be directly performed;

Configure interface QinQ VPN

SWITCH(config-if)#**switchport vlan-stacking vpn** VPN-NAME
An interface can only be associated with one VPN. Only when the interface is not configured with a mapping relationship, the VPN association configuration can be performed;

Configure interface association VLAN Mapping VPN

SWITCH(config-if)#**switchport vlan-mapping vpn** VPN-NAME

To configure VLAN Mapping on different interfaces, they must be associated with the same VPN. And the mapping relationship in the corresponding VPN must be 1:1;

17.4. Configuration case

Case 1: Implementing Layer 2 VPN services based on ports

The service provider provides VPN for enterprise A and enterprise B:

- On the public network, enterprise A and enterprise B belong to different VLANs, and each communicate through their own public network VLAN.

- The VLANs in enterprise A and enterprise B are transparent to the public network, and the user VLANs in enterprise A and enterprise B can be reused without conflict.
- Tunnel will encapsulate a layer of Native VLAN VLAN Tag for user data packets. In the public network, user data packets are transmitted in Native VLAN, which does not affect the use of VLANs in different enterprise user networks, and implements a simple Layer 2 VPN.

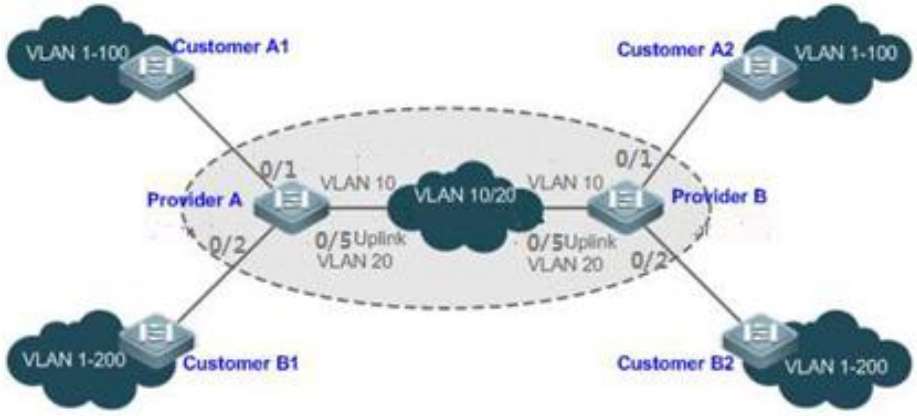


Illustration:

- Customer A1 and Customer A2, Customer B1 and Customer B2 are the edge devices of the network where enterprise user A and enterprise user B are located. Provider A and Provider B are service provider network edge devices, and enterprise A and enterprise B access the public network through the provider edge devices.
- The office network VLAN range used by enterprise A is VLAN 1-100.
- The office network VLAN range used by enterprise B is VLAN 1-200.

ProviderA and ProviderB are completely symmetrical and the configuration is exactly the same

```
SWITCH(config)#vlan 2-200
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 1-100
SWITCH(config-if)#switchport trunk native vlan 10
SWITCH(config)#interface GigabitEthernet0/2
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk native vlan 10
SWITCH(config-if)#interface GigabitEthernet0/5
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#interface GigabitEthernet0/1-2
SWITCH(config-if)#switchport vlan-stacking basic
```

Case 2: Flexible QinQ based on C-Tag realizes Layer 2 VPN and service flow management

Basic QinQ can only encapsulate user data packets with a native VLAN outer tag, that is, the outer tag encapsulation depends on the native VLAN of the tunnel port. Flexible QinQ provides flexible

encapsulation of the external tag (ie S-Tag) of the service provider (ISP) according to the Tag (ie C-Tag) of user messages, so as to implement VPN transparent transmission and service flow QOS strategies more flexibly.

- Broadband Internet access and IPTV services are both important parts of the services carried by the metropolitan area network. The metropolitan area network service provider network divides VLANs for different business flows to differentiate management, and provides the service of setting QOS policies for these VLANs. C-Tag-based QinQ can be used on the edge equipment of the service provider to encapsulate the user's service flow with the relevant VLAN, and the QOS strategy of the service provider network can be used for guaranteed transmission while transparently transmitting.
- A unified VLAN planning has been implemented between enterprise branches. Important services and general services are in different VLAN ranges. The enterprise network can use the flexible QinQ based on C-Tag to transparently transmit the internal services of the company, and use the service provider network. The QOS strategy prioritizes data transmission for important services.

As shown in the figure below, the user-end equipment in the metropolitan area network is converged through the corridor switch in the community, and broadband Internet access and IPTV services are differentiated by assigning different VLANs, and they can enjoy different QOS service strategies.

- In the public network, different service streams of broadband Internet access and IPTV are transmitted in different VLANs to realize transparent transmission of user services.
- The ISP network sets the QOS strategy for VLAN, and the corresponding VLAN can be encapsulated for user services on the edge devices of the service provider, so that the IPTV service is transmitted preferentially in the ISP network.

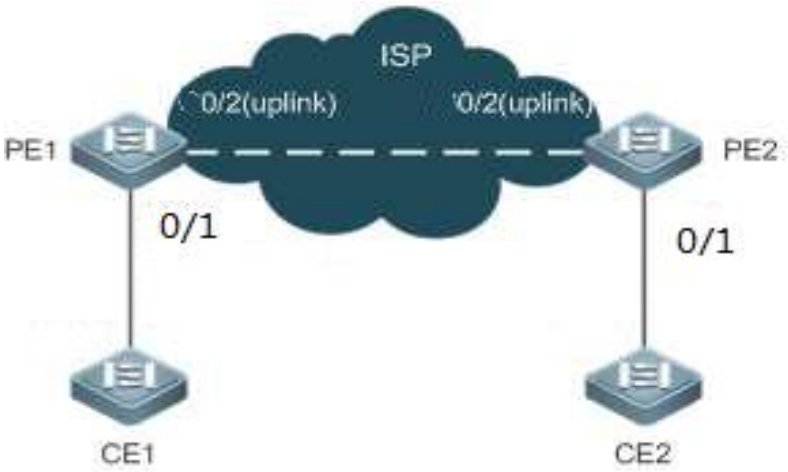


Illustration:

- CE1 and CE2 are edge devices connected to the user's network, and PE1 and PE2 are edge devices of the provider service network.
- On CE1 and CE2 devices, VLAN 1-100 is the user's broadband Internet access service flow, and VLAN 101-200 is the user's IPTV service flow.
- PE1 and PE2 devices encapsulate different S-Tags for VLANs of different services to distinguish different service data. VLAN 1-100 encapsulates VLAN 100, and VLAN 101-200 encapsulates VLAN 200.

The configurations of PE1 and PE2 are exactly the same

```
SWITCH(config)#vlan 2-200
```

```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#switchport mode hybrid
SWITCH(config-if)#switchport hybrid untagged vlan 100,200
SWITCH(config-if)#switchport hybrid vlan 100
SWITCH(config-if)#interface GigabitEthernet0/2
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#exit
SWITCH(config)#vlan-vpn isp
SWITCH(config-vlan-vpn)# cvlan 1-100 svlan 100
SWITCH(config-vlan-vpn)# cvlan101-200 svlan 200
SWITCH(config-vlan-vpn)# interface GigabitEthernet0/1
SWITCH(config-if)#switchport vlan-stacking vpn isp
```

Case 3: VLAN Mapping based on C-Tag to realize Layer 2 VPN and service flow management

Similar to case two, it distinguishes users' broadband Internet access services and IPTV services. For example, the broadband Internet access services are VLAN2 and the IPTV services are VLAN3. In the ISP network, VLAN200 and VLAN300 are used to represent broadband Internet access services and IPTV services. All ports 1-10 of the PE device are connected to the CE device, and the upper link port is GigabitEthernet0/11

The configurations of PE1 and PE2 are exactly the same

```
SWITCH(config)#vlan 2-3,200,300
SWITCH(config)#interface GigabitEthernet0/1-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#interface GigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#exit
SWITCH(config)#vlan-vpn isp-map
SWITCH(config-vlan-vpn)#cvlan 2 svlan 200
SWITCH(config-vlan-vpn)#cvlan 3 svlan 300
SWTICH(config-vlan-vpn)#interface GigabitEthernet0/1-10
SWITCH(config-if)#switchport vlan-mapping vpn isp-map
SWITCH(config-if)#exit
```

17.5. Show command

Show VPN configuration

SWITCH#**show vlan-vpn** VPN-NAME

```
SWITCH#show vlan-vpn test
------------------------------------------------------------
VLAN VPN: test
Class: vlan-stacking
Mapping attributes:
  cvlan 1-25,73,75-80 svlan 3
  cvlan 200 svlan 4
Applied interfaces:
  GigabitEthernet0/17
  GigabitEthernet0/18
```

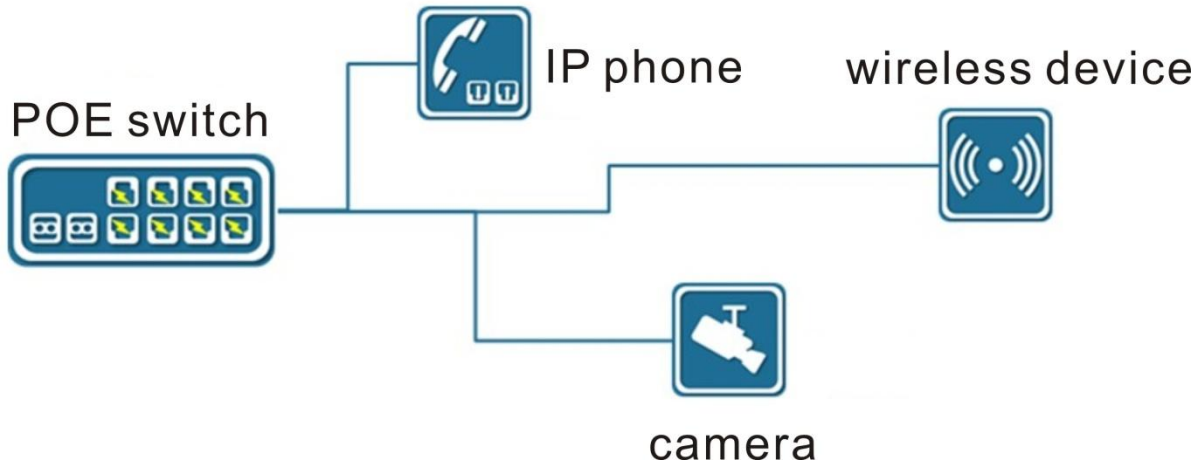
18. CONFIGURE POE

The corresponding web network management configuration path is: Home->Interface->PoE Management

18.1. PoE overview

Power over Ethernet, abbreviated as PoE, is a technology that can exchange data with the terminal through a twisted pair in an Ethernet circuit while providing DC power supply. It is commonly used to supply power to devices such as VoIP, WIFI AP, network cameras, hubs, and computers.

According to the standard, the longest power supply distance is 100m.



PSE (Power Sourcing Equipment), such as the PoE switch in the figure above. The PSE looks for and detects the PD on the line of the PoE port, classifies the PD, and supplies power to it. After detecting that the PD is unplugged, the PSE stops supplying power. PD is a device that accepts PSE power supply, such as IP phones, wireless devices, and cameras in the picture above.

The development of PoE has experienced two sets of standards:

IEEE 802.3af (15.4W) is the first PoE power supply standard and specifies the power over Ethernet standard, which is now the mainstream implementation standard for PoE applications. It clearly specifies the power detection and control items in the remote system, and regulates the way that routers, switches, and hubs supply power to devices such as IP phones, security systems, and wireless LAN access points through Ethernet cables. IEEE802.3at (25.5W) was born in response to the needs of high-power terminals. On the basis of being compatible with 802.3af, it provides greater power supply requirements to meet new needs. According to the IEEE 802.3af specification, the PoE power consumption on the powered device (PD) is limited to 12.95W. IEEE 802.3at, which defines devices with power requirements higher than 12.95W as Class 4 (this level is described in IEEE 802.3af, but reserved for future use), which can extend the power level to 25W or higher.

The POE of this device supports the Watchdog function, which is mainly used to detect the abnormality of the PD terminal device, and power off the PD through the PSE, power-on control, and reset the PD terminal device to recover from the abnormal state. The watchdog function is turned off by default, and it can be turned on based on the port. The abnormal detection of the PD device mainly depends on two parameters:

- Tokens: If the number of packets received within the time interval of a port exceeds the defined number of tokens, the corresponding PD device is considered to be abnormal and a recovery action is triggered. The default number of tokens is 3, which can be configured globally.
- interval: The time interval for collecting statistics on the number of packets, the default is 20S, which can be modified globally.

18.2. Configuration command

Configure PoE external power supply

SWITCH(config)#**poe powersupply** POWER

Configure external power supply;

The default power calculation method: the product of the number of PoE power supply ports and 15.4W per port;

If the configured power is less than the power consumption of the current device, power off the PD device of the low-priority port, and the port priority is the higher priority with the smaller port ID.

Configure PoE port power supply enable

SWITCH (config-if)#**poe enable**

Configure PoE port power supply;

It is turned on by default.

Configure PoE port watchdog enable

SWITCH (config-if)#**poe watchdog enable**

Configure the PoE port to enable watchdog;

Off by default.

Configure the PoE watchdog time interval

SWITCH (config)#**poe watchdog interval** *<5-3600>*

Configure the time interval of PoE watchdog;

The unit is second, the configurable range is 5S-3600S, and the default is 20S.

Configure the number of PoE watchdog tokens

SWITCH (config)#**poe watchdog token** *<1-100000>*

Configure the number of PoE watchdog tokens;

The unit is the number of packets, the configurable range is 1-100,000, and the default is 3.

18.3. Configuration case

Configure port GigabitEthernet0/1 power supply enable

```
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#poe enable
```

18.4. Show command

Show PoE system power supply information

SWITCH#show poe powersupply

```
SWITCH#show poe powersupply
  Power supply          : 123.2W
  Power consume         : 44.1W
```

```
Power management        : energy-saving
Disconnect mode         : DC
Powered ports           : 2
Watchdog interval       : 20 S
Watchdog token          : 3
```

Show PoE port power supply information

SWITCH#show poe interfaces

```
SWITCH#show poe interfaces
Interface              En    Wdog  Sts   Reason    Class  Icut(mA) Power(W)
-------------------------------------------------------------------------
GigabitEthernet0/1     Yes   No    Off   short     4      --       --
GigabitEthernet0/2     Yes   No    Off   --        -      --       --
GigabitEthernet0/3     Yes   No    Off   --        -      --       --
GigabitEthernet0/4     Yes   No    Off   --        -      --       --
…
```

19. CONFIGURE IP

The corresponding web network management configuration path is:

Layer 3 port management: Homepage->Routing->VLAN interface

ARP: Home->Routing->ARP

Static routing: Home->Routing->IPv4 routing

19.1. IP overview

Internet Protocol, IP uses a logical virtual address to send data packets from the source to the destination, that is, the IP address. At the network layer, routing devices use IP addresses to complete data packet forwarding.

Protocol specification: RFC 1918: Address Allocation for Private Internets

RFC 1166：Internet Numbers

19.2. Detailed function

The functions described in this chapter correspond to the three-layer functions of weak three-layer devices, that is, it does not include routing management and routing protocols. For details on routing management and routing protocol configuration of Layer 3 devices, please refer to "FRRouting Configuration Guide".

19.2.1. Three-layer port management

The network layer belongs to the third layer (the OSI seven-layer model and the TCP/IP protocol stack are both), so the interface for forwarding the network layer IP data packet is called the three-layer interface (referred to as the three-layer interface). Layer 3 ports are relative to Layer 2 (switching) ports, and are generally divided into routing ports (ordinary physical ports or aggregate ports are switched to Layer 3 ports) or SVI ports (Switch Virtual Interface, corresponding to a VLAN). The SVI port is a logical interface, which is structured on all member ports included in the corresponding VLAN. Unlike routing ports, packets that are forwarded through SVI through Layer 3 will pass through Layer 2 (such as VLAN filtering, address learning).) Go through the third layer again, first go through the third layer and then go through the second layer when outputting (such as VLAN output rules). **This device only supports SVI port.**

L3 port management includes the creation/deletion of L3 port, IP address maintenance, and other interface management functions.

- Create/delete

  The VLAN corresponding to the SVI port is used as the unique identifier of the Layer 3 port, and the name of the corresponding Layer 3 port is "Vlan+vlan_number". There is no separate creation/delete command for the SVI port. The creation and deletion of VLAN will create and delete the corresponding Layer 3 port. For example, "vlan 100" creates VLAN 100 and at the same time creates an SVI port "Vlan100". When "no vlan 100" deletes VLAN 100, it also deletes the corresponding SVI port "Vlan100".

  The SVI port is the same as the ordinary interface, and the corresponding interface mode can be entered through "interface + interface name".

- IP address maintenance

To use the Layer 3 port normally, an IP address must be configured. The IP address is composed of 32-bit binary. For the convenience of writing and description, it is generally expressed in dotted decimal notation. When expressed in dotted decimal notation, it is divided into four groups, each group has 8 digits, ranging from 0 to 255, and the groups are separated by "." signs. For example, "192.168.1.1" is the IP address expressed in decimal. As the name implies, the IP address is naturally the interconnection address of the IP layer protocol. A 32-bit IP address consists of two parts: 1) the network address part, which indicates which network it is; 2) the host address part, which indicates which host in the network. The network address part of the IP address and the host address address part are divided by the network mask. The network mask is also a 32-bit value, consisting of several bits "1" in the front and several bits "0" in the back. The IP address and the network What you get from the mask is the part of the corresponding network address. Similarly, the network mask can also be directly represented by the length of the mask. For example, "192.168.1.1 255.255.255.0" and "192.168.1.1/24" indicate the same IP address.

The Layer 3 port of this device does not support configuring the Second IP address, that is, a Layer 3 port can be configured with at most one IP address. When an IP address is configured for a Layer 3 port, a network segment is determined. Different Layer 3 ports of the same device must belong to different network segments, and the IP addresses configured for different Layer 3 ports must belong to different network segments. After the different Layer 3 ports of the device are divided into different network segments, the forwarding between these different network segments (such as VLAN 1 and VLAN 2) is called "Layer 3 forwarding" (across the network segment, or across different VLANs).

This device supports DHCPv4 Client, that is, it dynamically obtains the IPv4 address of the interface. Choose either static configuration or enabling DHCPv4 Client. The later configuration will overwrite the previous configuration. This chapter does not describe the DHCPv4 Client. For details, please refer to the chapter "Configuring the DHCP Client".

■ Interface management function

For interface management functions, please refer to the chapter "Configuring Interfaces". **For Layer 3 interfaces, only interface descriptors, interface enable, and interface MTU functions are supported.**

For interface enablement, the SVI port is a logical interface, so "shutdown/no shutdown" will not change the link state of a physical port, only the logical interface will have a link state change. When the SVI port is created, its link status is UP, and only when it is shut down, the link status changes to DOWN (even if the VLAN corresponding to the SVI port does not contain any physical ports). For dynamic data or status based on the three-layer port, when the link status changes to DOWN, it will be automatically cleared, and when the link status changes to UP again, these dynamic data or status will be regenerated. When you need to pay attention, the statically configured data will exist consistently. For example: statically configured ARP, when the corresponding IP address corresponds to a L3 port whose link status is UP, it will be added to the ARP Cache (can be viewed by show arp), when the link status of the corresponding L3 port becomes DOWN When the time, it will be automatically cleared from the ARP Cache. When the link status of the corresponding Layer 3 port becomes UP, it will be automatically added to the ARP Cache. But in the whole process of the link status change, the corresponding configuration information can be seen through show run (the ARP Cache is dynamic data, and the configuration information seen by show run is static data). Static routing is similar, show run sees static data, show ip route sees dynamic data.

According to the above description of static data and dynamic data according to the link status change of the three-layer port. The trigger condition is changed to delete the IP address configuration of the L3 interface, and it still holds. In the process of generating dynamic data and

status, in addition to caring about the link status of the Layer 3 port, we also care about the IP address of the Layer 3 port, because many dynamic data and status associated Layer 3 ports are dependent on the network segment information (according to the IP address and IP mask). Code OK).

The functions of the MTU of the Layer 3 port and the MTU of the Layer 2 port are different. The Layer 2 MTU is mainly used to discard ultra-long frames when data is sent and received. In addition to the three-layer MTU, it is also used to **select the length of IP fragments when the message is sent**. For example, for OSPF LSU packets, when there are many LSAs that need to be updated, the MTU of the sending interface (Layer 3 interface) may be exceeded. At this time, the packet will be fragmented. It should be noted that the IP fragmentation and reassembly process is end-to-end, and the intermediate device forwarding at the network layer will not fragment and reorganize IP packets. Therefore, for network devices, this process only occurs on the control plane, not the forwarding plane. In addition, the three-layer MTU has another function, which is **used to negotiate and/or check the MTU when the protocol is established**. For example, in the process of establishing adjacency, OSPF will check the MTU. When the MTU does not match, the adjacency will not be established. You can turn off the MTU check through the configuration.

19.2.2. ARP

In a local area network, each IP network device has two addresses: 1) The local address, because it is contained in the frame header of the data link layer, it should be the data link layer address more accurately, but it is actually a local address. Address processing is the MAC sublayer in the data link layer, so it is customarily called the MAC address. The MAC address represents the IP network device on the local area network; 2) The network address represents the IP network device on the Internet, and it It also explains the network to which the device belongs.

To communicate between two IP devices on the local area network, they must know each other's 48-bit MAC address. The process of obtaining the MAC address based on the IP address is called address resolution. There are two types of address resolution methods: 1) Address Resolution Protocol (ARP); 2) Proxy ARP. About ARP and Proxy ARP, they are described in RFC 826 and RFC 1027 respectively.

- ARP

ARP (Address Resolution Protocol) is used to bind MAC address and IP address. With IP address as input, ARP can know its associated MAC address. Once the MAC address is known, the corresponding relationship between the IP address and the MAC address will be stored in the ARP cache of the device. With the MAC address, the IP device can encapsulate the link layer frame, and then send the data frame to the LAN. The encapsulation of IP and ARP on Ethernet is Ethernet II type.

ARP entries are divided into two categories: dynamic entries derived from the ARP protocol, and static entries derived from static configuration. The dynamic ARP entry is formed by triggering the opening of IP packets. The opening process is an ARP request/response process. If the ARP entry formed after opening is unreachable, it will automatically age. Static ARP entries do not need to be opened up and will not age.

ARP entries are stored in the ARP Cache and can be viewed through show arp. When the ARP entry is generated, it is necessary to clearly associate the Layer 3 port according to the network segment information. Because each layer 3 port is configured with an IP address, a network segment is determined, and the IP address of the ARP table entry will look for which network segment it belongs to, thereby clarifying which layer 3 port it is associated with. If the associated Layer 3 port cannot be found, no ARP entry will be generated. Similarly, if an ARP

entry has been generated, the IP address configuration associated with the Layer 3 port is cleared, or shutdown, or the Layer 3 port is deleted, the ARP entry will be automatically deleted.

- Proxy ARP

The proxy ARP function of the device can help the host without routing information to obtain the MAC address of the IP address of other subnets. For example, when the device receives an ARP request, the sender IP address of the ARP request **does not belong to the same network segment** as the target IP address, and the device knows the route of the requested IP address, the device will send an ARP response, and the MAC address of the response is the device itself This process is the function of proxy ARP.

There are two ways to enable the Proxy ARP function:

1) Enable proxy **based on interface**: Configure "ip proxy-arp" on the Layer 3 port, as long as the target IP address requested by the ARP received from the Layer 3 port is not on the same network segment as the Layer 3 port and **the device is reachable (with Reachable route)**, it will respond to the device's own Ethernet MAC address.

2) Enable proxy **based on IP address**: statically configure alias ARP entries. **The configured IP address must belong to a directly connected network segment** before the ARP entry will be placed in the ARP Cache. No matter which layer 3 port receives the ARP request for the IP address (the layer 3 port does not need to be configured with ip proxy-arp), it will respond to the device's own Ethernet MAC address. Through show arp, you can see the configured alias arp entry (type is Alias). This entry will not display the MAC address and related information about the associated Layer 3 interface.

Noted: when the IP address of the sender and the target IP address of the received ARP request belong to the same network segment, no proxy will be performed.

19.2.3. Static routing

The routing table of the device is divided into three categories (without considering dynamic routing):

- Directly connected route: The route discovered by the link layer protocol, also known as the interface route. The direct route is automatically generated when the Layer 3 port is configured with an IP address, and the route prefix is the network directly connected to the Layer 3 port.
- Static routing: manually configured by the network administrator.
- Default route: It is a special case of static routing, which refers to the routing table entries that hit all IP packets. (The length of the prefix mask is 0)

The routing table entry consists of two parts:

- Prefix: It is represented by an IP address and network mask (or mask length), and refers to the destination network or host determined by the routing table entry (when the mask length is 32, it means the host).
- Direct connection or next hop: Direct connection means that the destination network or host belongs to a directly connected network. This is the case for direct routing. When configuring a static route, specify a Layer 3 port instead of an IP address, and this type of routing table entry will also be generated ; The next hop is represented by an IP host address, which means that to reach the destination network or host, it needs to be forwarded to the IP network device indicated by the IP address.

When forwarding IP packets based on routing table entries, if the routing table entry specifies the next hop, when link layer encapsulation queries ARP, the next hop IP is used, that is, the destination MAC address of the link layer encapsulation is the next hop. The destination MAC address of the hop. If the routing table entry is directly connected, the destination IP of the message is directly used for ARP query, that is, the destination MAC address encapsulated at the link layer is the final

destination MAC address of the message. Either way, if the ARP query fails, it will trigger routing through (generate dynamic ARP entries), if it fails, the IP packet cannot be forwarded and will be discarded.

There may be a containment relationship between routing table entries (depending on the length of the mask), so the routing lookup process satisfies LPM (Longest Prefix Match). That is, when IP packets are forwarded for route lookup, if multiple routing table entries are hit at the same time, the routing table entry with the longest prefix mask length is selected.

19.3. Configuration command

Enter the SVI interface

SWITCH(config)#**interface vlan** VLANID

SVI port automatically completes the creation/deletion according to the creation/deletion of VLAN;

Configure the Layer 3 port IP address

SWITCH(config-if)#**ip address** IPADDR

IPADDR adopts the format of A.B.C.D/M;

When the SVI is deleted, the IP address configured on it will be cleared automatically;

The Layer 3 port supports IP address configuration update, which has the same effect as deleting and reconfiguring. The IP addresses configured for different Layer 3 ports must belong to different network segments;

The Layer 3 port does not support the configuration of Second IP;

Configure static ARP

SWITCH(config)#**arp** IPADDR MACADDR

IPADDR uses the format of A.B.C.D, and MACADDR uses the format of XXXX.XXXX.XXXX;

The static ARP configured IP address will take effect only if it belongs to the directly connected network segment (you can see that this entry exists through show arp). When the IP address of the L3 port is deleted or the L3 port is deleted, if the IP address of the static ARP belongs to the directly connected network segment of the L3 port, the static ARP is invalid (you can see that the entry does not exist through show arp, but show run, you can see that the configuration is still there); similarly, when an IP address is configured for a Layer 3 port, the static ARP entry of the IP address belonging to the directly connected network segment of the Layer 3 port will change from an invalid state to a valid state. (You can see that the entry exists through show arp);

Static ARP has a higher priority than dynamic ARP. When the two conflict, static ARP takes effect.

Configure interface-based proxy ARP

SWITCH(config-if)#**ip proxy-arp**

This command can only be configured on Layer 3 ports. Proxy ARP is performed on the configured Layer 3 port, and when a non-ARP request is received, it responds to the Ethernet MAC address of the device itself.

When the three-layer port is deleted, the configuration is automatically cleared.

Configure IP-based proxy ARP

SWITCH(config)#**arp** IPADDR MACADDR **alias**

IPADDR uses the format of A.B.C.D.

The purpose of the Alias ARP table entry is to perform proxy ARP for the configured IP address. When an ARP request requesting the IP address is received, it responds to the device's own Ethernet MAC address.

Only when the IP address configured by Alias ARP belongs to the directly connected network segment will take effect (the entry can be seen through show arp). When the IP address of the L3 port is deleted or the L3 port is deleted, if the IP address of the Alias ARP belongs to the directly connected network segment of the L3 port, the Alias ARP becomes invalid (you can see that the entry does not exist through show arp, but show run, you can see that the configuration is still there); Similarly, when an IP address is configured for a Layer 3 port, the Alias ARP table entries whose IP address belongs to the directly connected network segment of the Layer 3 port will change from invalid state to valid state. (You can see the entry exists through show arp).

Alias ARP entries and ARP entries (including static and dynamic) are completely independent, and there is no conflict.

The proxy ARP function is only for the situation where the sender IP address and the target IP address of the ARP request are not in the same network segment;

Proxy ARP is implemented in two ways: proxy the configured IP address; proxy the configured interface. The two methods can be used flexibly according to needs.

Clear ARP cache

SWITCH#**clear arp-cache**

This command only clears dynamic ARP entries, static ARP entries and Alias ARP entries will not be cleared.

Static routing

SWITCH(config)#**ip route** PREFIX (NH_IP | IFNAME)

PREFIX adopts one of two formats: A.B.C.D/M or A.B.C.D A.B.C.D;

NH_IP adopts the format of A.B.C.D;

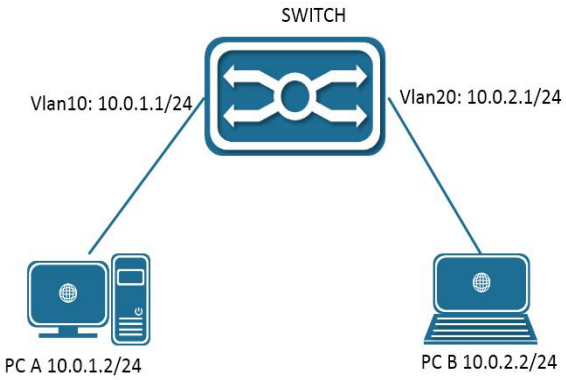
Does not support ECMP configuration (a routing prefix corresponds to multiple next hops);

Recursive routing is not supported (the configured next hop IP must belong to the directly connected network segment);

The routing prefix cannot belong to the directly connected network segment (that is, the directly connected route is automatically generated and cannot be statically configured);

19.4. Configuration case

Case 1: Subnet Gateway



In different IP LANs, a transparent subnet gateway is realized. PC A and PC B can be interconnected across network segments.

Configure PC

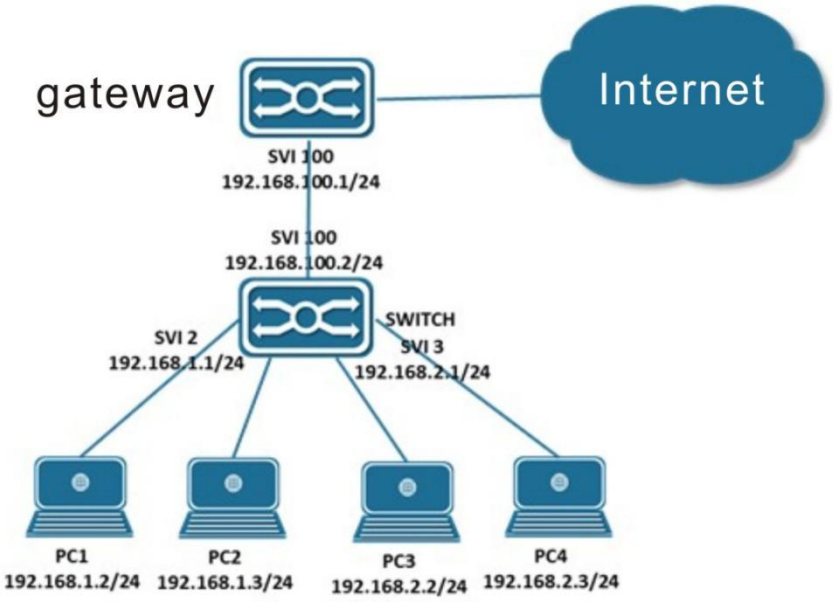
PC1, PC2, and PC3 are configured with IP addresses as shown in the figure, and **the default gateway is not configured.**

Switch SWITCH reference configuration

Configure the Layer 3 port and IP address (assuming that the interface connected to PC A is GigabitEthernet0/1, and the interface connected to PC B is GigabitEthernet0/2), and proxy ARP is configured on the SVI port.

```
SWITCH(config)#vlan 10,20
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#switch access vlan 10
SWITCH(config)#interface GigabitEthernet0/2
SWITCH(config-if)#switch access vlan 20
SWITCH(config)#interface Vlan10
SWITCH(config-if)#ip address 10.0.1.1/24
SWITCH(config)#interface Vlan20
SWITCH(config-if)#ip address 10.0.2.1/24
SWITCH(config-if)#exit
SWITCH(config)#interface Vlan10
SWITCH(config-if)#ip proxy-arp
SWITCH(config)#interface Vlan20
SWITCH(config-if)#ip proxy-arp
```

Case 2: Weak Layer 3 Gateway



As a weak Layer 3 gateway, Switch reduces the burden of ARP for real gateways.

Configure PC

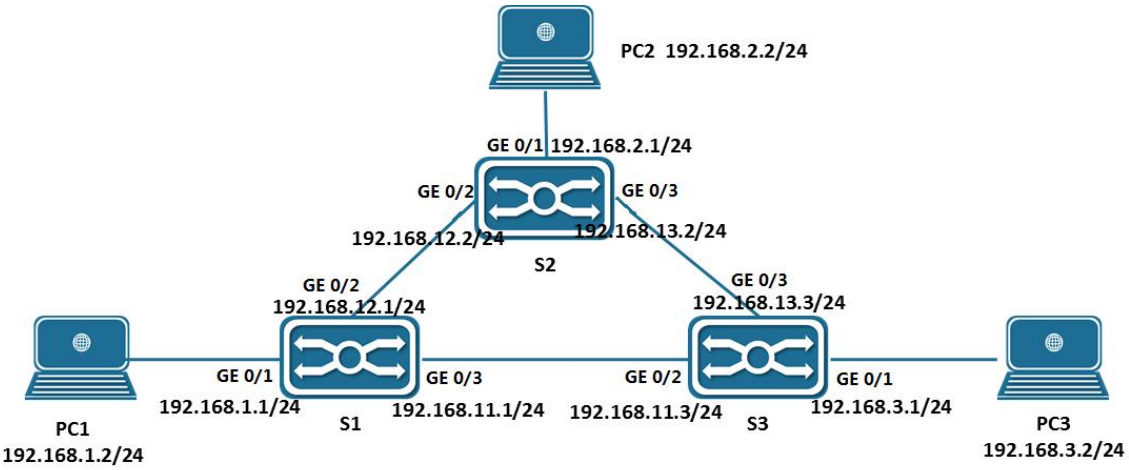
PC1, PC2, and PC3 configure the IP addresses as shown in the figure, and specify the gateway at the same time. For example, the gateway of PC1 and P2 is 192.168.1.1.

Switch reference configuration

Configure the Layer 3 port and IP address (assuming that the interface connected to PC1-PC4 is GigabitEthernet0/1-4, and the upper link port is GigabitEthernet0/17), and configure the static route (default route).

```
SWITCH(config)#vlan 2-3,100
SWITCH(config)#interface GigabitEthernet0/1-2
SWITCH(config-if)#switch access vlan 2
SWITCH(config)#interface GigabitEthernet0/3-4
SWITCH(config-if)#switch access vlan 3
SWITCH(config)#interface GigabitEthernet0/17
SWITCH(config-if)#switch access vlan 100
SWITCH(config)#int Vlan2
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config)#int Vlan3
SWITCH(config-if)#ip address 192.168.2.1/24
SWITCH(config)#int Vlan100
SWITCH(config-if)#ip address 192.168.100.2/24
SWITCH(config-if)ip route 0.0.0.0/0 192.168.100.1
```

Case 3: Three-layer interconnection of the intranet



In the network environment as shown in the figure above, PC1, PC2 and PC3 are interconnected through S1, S2 and S3 respectively.

Configure PC

PC1, PC2 and PC3 configure the IP addresses as shown in the figure, and specify the gateway at the same time. For example, the gateway of PC1 is 192.168.1.1.

Switch S1 reference configuration

Configure Layer 3 port and IP address and static routing

```
SWITCH(config)#vlan 2-4
SWITCH(config)#interface GigabitEthernet0/1
SWITCH(config-if)#switch access vlan 2
SWITCH(config)#interface GigabitEthernet0/2
SWITCH(config-if)#switch access vlan 3
SWITCH(config)#interface GigabitEthernet0/3
SWITCH(config-if)#switch access vlan 4
SWITCH(config)#int Vlan2
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config)#int Vlan3
SWITCH(config-if)#ip address 192.168.12.1/24
SWITCH(config)#int Vlan4
SWITCH(config-if)#ip address 192.168.13.1/24
SWITCH(config)#ip route 192.168.2.0/24 192.168.12.2
SWITCH(config)#ip route 192.168.3.0/24 192.168.11.3
```

Switch S2, S3 reference configuration

The configuration of S2 and S3 is similar to that of S1 and will not be repeated.

19.5. Show command

View the information of the third floor

It is the same as the L2 port command, please refer to the related content in the chapter "Configuring the interface" for details.

View ARP cache

SWITCH#**show arp**

```
SWITCH#show arp
Address                  HWaddress              Interface       Type
192.168.3.2              00:00:00:00:00:34      Vlan1           Static
192.100.4.10             00:00:00:40:00:01      Vlan4           Static
192.168.3.1              00:0e:c6:d8:c7:f7      Vlan1           Dynamic
192.100.3.10             00:00:00:00:00:00      *               Alias
```

Show routing table entries

SWITCH#**show ip route**

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
IP Route Table for VRF "default"
Gateway of last resort is 192.168.1.3 to network 0.0.0.0
S*       0.0.0.0/0 [1/0] via 192.168.1.3, Vlan2
S        192.168.0.0/16 [1/0] via 192.168.0.10, Vlan1
C        192.168.0.0/24 is directly connected, Vlan1
C        192.168.1.0/24 is directly connected, Vlan2
C        192.168.2.0/24 is directly connected, Vlan3
C        192.168.3.0/24 is directly connected, Vlan4
```

20. CONFIGURE IPV6

The corresponding web network management configuration path is:

IPv6 address: Homepage->Routing->VLAN Interface

Default route: Home->Route->IPv6 route

20.1. IPv6 overview

With the rapid growth of the Internet and the gradual exhaustion of the IPv4 address space, the limitations of IPv4 have become more and more obvious. The research and practice of the Internet Protocol Next Generation (IPng) has become a hot spot. The IPng working group of the Internet Engineering Task Force (IETF) has determined the protocol specification of IPng and called it "IP Version 6" (IPv6), the specification of this protocol is described in detail in RFC2460.

Protocol specification: RFC4291-IP Version 6 Addressing Architecture.

RFC2460 - Internet Protocol, Version 6 (IPv6) Specification

RFC4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

RFC4861 - Neighbor Discovery for IP version 6 (IPv6)

20.2. Detailed function

The current device's support for IPv6 is limited to the management plane.

- Support the configuration of IPv6 addresses on multiple SVI ports (Layer 3 ports);
- The same SVI port can be configured with several IPv6 static addresses;
- Support DHCPv6 Client;
- Support the configuration of the default route.
- Stateless IPv6 address acquisition methods are not supported, either static configuration or DHCPv6 Client is used.

20.2.1. IPv6 address

The basic expression of an IPv6 address is X:X:X:X:X:X:X:X, where X is a 4-digit hexadecimal integer (16 bits). Each number contains 4 bits, each integer contains 4 hexadecimal numbers, and each address contains 8 integers, a total of 128 bits. Here are some legal IPv6 addresses:

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800:0:0:0:0:0:0:1

1080:0:0:0:8:800:200C:417A

These integers are hexadecimal integers, where A to F represent 10 to 15. Each integer in the address must be represented, but the starting 0 does not need to be represented. Some IPv6 addresses may contain a long string of 0s (like the second and third examples above). When this happens, "::" is allowed to represent this long string of 0s. That is, the address 800:0:0:0:0:0:0:1 can be expressed as: 800::1

These two colons indicate that the address can be extended to a full 128-bit address. In this method, only when the 16-bit group is all 0s will it be replaced by two colons, and the two colons can only appear once in the address.

Since the IPv6 address is divided into two parts: the subnet prefix and the interface identifier, it can be represented as an address with an additional value in a similar way to a CIDR address, where the value indicates how many bits in the address represent the network part (Network prefix), that is, the prefix length is indicated in the IPv6 node address. This length is distinguished from the IPv6 address by a slash, for example: 12AB::CD30:0:0:0:0/60, the address used for routing The prefix length is 60 bits.

20.2.2. Default route

The IPv6 routing of the current device is divided into two types:

- Directly connected route: The route discovered by the link layer protocol, also known as the interface route. The direct route is automatically generated when the IPv6 address is configured on the Layer 3 port, and the route prefix is the network directly connected to the Layer 3 port.
- Default route: The current device only supports default routes when configuring static routes. , Refers to the routing table entries that hit all IPv6 packets. (::/0)

According to LPM (Longest Prefix Match), the prefix length of the direct route is definitely longer than that of the default route. Therefore, when reaching the destination of the directly connected network, the direct route is hit, and when reaching the destination of the non-directly connected network, all the default routes are adopted. Configured next hop.

IPv6 routes are only used for searching when the management plane sends IPv6 packets.

20.3. Configuration command

Enter the SVI interface

SWITCH(config)#**interface vlan** VLANID

SVI port automatically completes the creation/deletion according to the creation/deletion of VLAN;

Configure the Layer 3 port IPv6 address

SWITCH(config-if)#**ipv6 address** IPADDR

IPADDR uses the format of X:X::X:X/M;

When the SVI is deleted, the IPv6 address configured on it will be automatically cleared;

Several IPv6 addresses can be configured on a L3 port.

Configure the default route

SWITCH(config)#**ipv6 route** ::/0 *NH-IP*

PREFIX must be ::/0, other prefixes are not supported.

NH_IP uses the format of X:X::X:X.

20.4. Show command

Check the L3 interface information, you can see the configured IPv6 address.

```
SWITCH#show int vlan 2
```

```
Interface Vlan2
  Hardware is SVI  Current HW addr: 00ed.2d34.9b24
  Logical:(not set)
  Port Mode is Router
  Index 2002 metric 0 mtu 1500
  Interface status:
    Link status: UP
  no switchport
  ARP ageing timeout 0

  DHCP client is disabled.
  inet 192.168.2.1/24 broadcast 192.168.2.255
  inet6 2030::1/64
  inet6 fe80::2ed:2dff:fe34:9b24/64
```

Show routing table entries

```
SWITCH#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
S       ::/0 [1/0] via 2030::3, Vlan2, 00:00:17
C       2030::/64 via ::, Vlan2, 02:05:14
C       fe80::/64 via ::, Vlan10, 02:04:11
```

21. CONFIGURE DHCP CLIENT

The corresponding web network management configuration path is: Homepage -> Routing -> VLAN interface.

21.1. DHCP Client overview

DHCP (Dynamic Host Configuration Protocol) is a network protocol for local area networks. It works with UDP protocol and is widely used to dynamically allocate reusable network resources, such as IP addresses.

DHCP is based on the Client/Server working mode. The DHCP client obtains the IP address and other configuration information by sending a request message to the DHCP server.

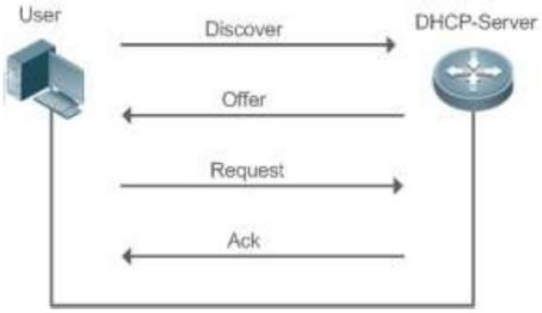
This device supports both DHCPv4 Client and DHCPv6 Client.

The DHCPv4 Client obtains the IPv4 address, IPv4 mask, and Router parameters from the Server (Router parameters will automatically generate a default route. The Router parameters can be closed without obtaining).

The DHCPv6 Client obtains the IPv6 address and prefix length from the Server, but does not obtain the default route.

21.2. Detailed function

21.2.1. DHCPv4



The process of DHCP requesting an IP address is as follows:

- The host sends a DHCP DISCOVER broadcast packet to find a DHCP server on the network;
- The DHCP server sends a DHCP OFFER unicast/broadcast (determined according to the relevant attributes of the host message) data packet to the host, which contains information such as IP address, MAC address, and address lease period;
- The host sends a DHCP REQUEST broadcast packet to formally request the server to allocate the provided IP address;
- The DHCP server sends a DHCP ACK unicast packet to the host to confirm the host's request.

A DHCP client can receive DHCP OFFER packets from multiple DHCP servers, and then may accept any DHCP OFFER packet, but the client usually only accepts the first DHCP OFFER packet received. In addition, the address specified in the DHCP OFFER of the DHCP server may not be the

address finally allocated. Normally, the DHCP server will reserve the address until the client sends a formal request.

Formally request the DHCP server to assign an address. The DHCP REQUEST uses a broadcast packet to allow all other DHCP servers that send DHCP OFFER packets to receive the packet, and then release the IP address that has been OFFER (pre-allocated) to the client.

If the DHCP OFFER packet sent to the DHCP client contains invalid configuration parameters, the client will send a DHCP DECLINE packet to the server to refuse to receive the allocated configuration information.

During the negotiation process, if the DHCP client does not respond to the DHCP OFFER packet in time, the DHCP server will send a DHCP NAK message to the DHCP client, causing the client to re-initiate the address request process.

The hostname of DHCPv4 is not specified, and the client-id is fixed as interface information + MAC information, as follows:

V1	V2	M1	M2	M3	M4	M5	M6

Each byte corresponds to two bits.

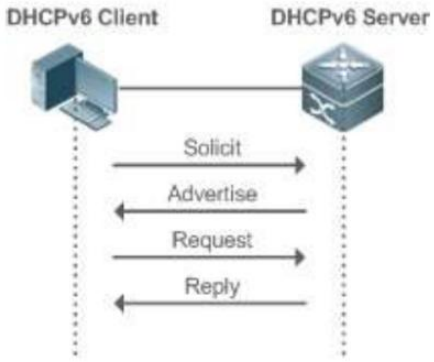
- VLAN ID: Occupies 2 bytes, corresponding to V1 and V2. Indicates the VLAN ID of the corresponding SVI port. Use decimal notation and fill with 0 in front.
- MAC address: occupies 6 bytes, corresponding to M1-M6.

For example, if the Vlan 100 of the switch has a MAC address of 00:01:02:03:04:05, its client-id is:

“01 00 00 01 02 03 04 05”。

The hostname and client-id of DHCPv4 of this device cannot be configured and modified.

21.2.2. DHCPv6



The process of DHCPv6 requesting an IP address is as follows:

- The DHCPv6 Client sends a SOLICIT message with a destination address of FF02::1:2 and a destination port of 547 within this link to request address allocation. All DHCPv6 Server or DHCPv6 Relay Agent in this link will receive SOLICIT message.
- After the DHCPv6 Server receives the SOLICIT message, if the requested information in the SOLICIT message can be provided locally, it will respond with an ADVERTISE message in unicast mode, which contains the address, prefix and other information that the DHCPv6 Server can provide.

- The DHCPv6 Client may receive ADVERTISE messages from multiple DHCPv6 Servers. After selecting the most suitable DHCPv6 Server, the DHCPv6 Client sends a REQUEST message with a destination address of FF02::1:2 and a destination port of 547 to request address allocation.
- After receiving the REQUEST message, the DHCPv6 Server creates binding information locally and responds with a REPLY message unicast, including the address, prefix, and configuration parameters that the DHCPv6 Server will assign to the DHCPv6 Client. The DHCPv6 Client completes the address assignment, prefix assignment, or configuration parameter assignment according to the information in the REPLY message.

If the DHCPv6 Client needs to release an address, it sends a Release message to the DHCPv6 Server to notify the DHCPv6 Server of the addresses that are no longer used, so that the DHCPv6 Server can allocate these addresses to other DHCPv6 Clients again. After receiving the Release message, the DHCPv6 Server removes the relevant bindings according to the address information in the Release message, and replies a Reply message with status options to the DHCPv6 Client.

The DUID of DHCPv6 uses type 1. details as follows:

Ty1	Ty2	H1	H2	T1	T2	T3	T4	M1	M2	M3	M4	M5	M6

Each byte occupies 2 bits.

- Type: Occupies 2 bytes, corresponding to Ty1 and Ty2. It is fixed at 00 01.
- Hardware Type: occupies 2 bytes, corresponding to H1 and H2. It is fixed at 00 01.
- Time: Time value, occupies 4 bytes, corresponding to T1-T4.
- MAC address: occupies 6 bytes, corresponding to M1-M6.

The following is a legal DUID:

“00 01 00 01 c7 92 dd 07 7c ec 9b 10 8a ff”。

The DHCPv6 DUID of this device cannot be configured and modified.

21.3. 2.84 configuration commands

Enable DHCP service

SWITCH(config)#**service dhcp**

Regardless of whether you are using a DHCPv4 Client or a DHCPv6 Client, you must enable the DHCP service.

Enter the SVI interface

SWITCH(config)#**interface vlan** VLANID

SVI port automatically completes the creation/deletion according to the creation/deletion of VLAN;

Configure the Layer 3 port IPv4 address to be obtained through DHCP

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

When the configured IPv4 address is obtained through DHCP, the static IPv4 address configured on it will be automatically deleted.

If the IPv4 address is statically configured, if the DHCP Client is enabled on the interface, it will be automatically closed.

This command will obtain the Router parameters to generate a default route (the next hop refers to the IP address indicated by the Router parameters).

Configure the Layer 3 port IPv4 address to be obtained through DHCP, but not to obtain the Router parameters

SWITCH(config-if)#**ip address dhcp none-default-route**

The only difference between this command and the above "ip address dhcp" command is that it does not get the Router parameters.

When multiple Layer 3 ports of the same switch enable DHCPv4 Client, at most one Layer 3 port is allowed to obtain Router parameters. Otherwise, multiple default routes will cause the device's default IPv4 forwarding behavior to be wrong.

Configure the Layer 3 port IPv6 address to be obtained through DHCP

SWITCH(config-if)#**ipv6 address dhcp**

The same Layer 3 port supports the simultaneous configuration of multiple IPv6 addresses. Therefore, the statically configured IPv6 address and DHCPv4 Client can be opened at the same time without conflict.

The DHCPv6 Client will not generate a default route.

21.4. Configuration case

Configure Vlan10 of the switch to enable DHCPv4 Client and DHCPv6 Client. Vlan20 opens the DHCPv4 Client, Vlan30 opens the DHCPv6 Client, and the Vlan20 DHCPv4 Client opens to obtain the Router parameters.

```
SWITCH(config)#service dhcp
SWITCH(config)#vlan 10,20,30
SWITCH(config)#int vlan 10
SWITCH(config-if)#ip address dhcp none-default-route
SWITCH(config-if)#ipv6 address dhcp
SWITCH(config-if)#exit
SWITCH(config)#int vlan 20
SWITCH(config-if)#ip address dhcp
SWITCH(config-if)#exit
SWITCH(config)#int vlan 30
SWITCH(config-if)#ipv6 address dhcp
```

21.5. Show command

Check the Layer 3 port information, you can see whether the DHCPv4 Client and DHCPv6 Client are enabled, and the IP addresses obtained through the DHCPv4 Client and DHCPv6 Client.

```
SWITCH#show int vlan 2
Interface Vlan2
```

```
Hardware is SVI  Current HW addr: 7cec.9b10.8aff
Logical:(not set)
Port Mode is Router
Index 2002 metric 0 mtu 1500
Interface status:
  Link status: UP
no switchport
ARP ageing timeout 0

IPV4 DHCP client is enabled <client-id=00:02:7c:ec:9b:10:8a:ff, hostname=n/a>.
IPV6 DHCP IA-NA client is enabled.
inet 192.168.2.77/24 broadcast 192.168.2.255
inet6 2030::5e/64
inet6 fe80::7eec:9bff:fe10:8aff/64
```

By viewing the IPv4 routing information, you can view the default route automatically generated by the Router parameters obtained through the DHCPv4 Client.

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 192.168.2.1 to network 0.0.0.0

K*        0.0.0.0/0 [0/0] via 192.168.2.1, Vlan2
C         192.168.1.0/24 is directly connected, Vlan1
C         192.168.2.0/24 is directly connected, Vlan2
```

22. CONFIGURE DHCP SERVER

Web network management configuration is not currently supported.

22.1. DHCP Server overview

DHCP (Dynamic Host Configuration Protocol) is a network protocol for local area networks. It works with UDP protocol and is widely used to dynamically allocate reusable network resources, such as IP addresses.

DHCP is based on the Client/Server working mode. The DHCP client obtains the IP address and other configuration information by sending a request message to the DHCP server.

This device supports both DHCPv4 Server and DHCPv6 Server.

The DHCP Server of this device supports the configuration of address range, static binding address, and all option settings.

22.2. Detailed function

22.2.1. Address pool

The address pool of the DHCP Server is used to dynamically allocate IP addresses. This device has two address pools: IPv4 address pool and IPv6 address pool. The two address pools are independent of each other.

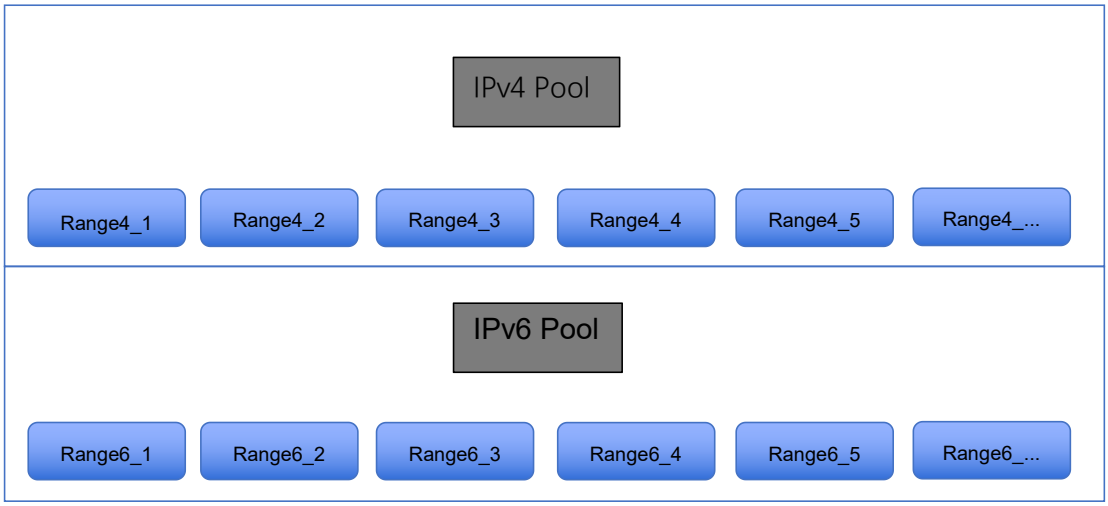
The address pool contains one or more address ranges, and each range has a name. If the addresses of the address pool are not continuous, multiple ranges are needed to represent the address pool.

For example:range a1 192.168.1.1 192.168.1.20

range a2 192.168.1.31 192.168.1.200

This address pool is the address range 192.168.1.1-192.168.1.200 (but 192.168.1.21-192.168.1.30 is excluded).

The entire structure of the address pool is as follows:



The address pools may not all belong to the same network segment. Different ranges can be configured with different network segments.

It is especially important to note that if the IP address of the L3 port of the machine is included in the range, this IP address will be automatically skipped during allocation. Therefore, when configuring the range, there is no need to deliberately bypass the IP address corresponding to the L3 port.

22.2.1.1. IPv4 address pool

When the IPv4 address pool receives a DHCPv4 request message, it will select an appropriate range for address assignment. details as follows:

- When applying for a directly connected network segment, a matching range (one or more) will be selected based on the IPv4 address of the Layer 3 interface that received the DHCPv4 request message.
- When applying for a non-directly connected network segment, in the DHCPv4 request message sent by the DHCPv4 Relay agent, the Relay agent IP field will carry the IPv4 address of the DHCPv4 Relay device. The IPv4 address belongs to the target distribution network segment, therefore, the matching range will be selected according to the IPv4.

If no matching range is found, the DHCPv4 Server will not respond to the DHCPv4 message.

When configuring the range, you can optionally configure the Netmask parameter, using the format of A.B.C.D. For the range applied for directly connected network segment, this parameter is optional. If this parameter is not carried, the mask of the assigned IPv4 address will inherit the mask configuration of the associated Layer 3 interface. If this parameter is carried, the configuration value is used. For ranges applied for non-directly connected network segments, this parameter is recommended to be manually set, otherwise it will be automatically selected according to the type of IPv4 address, type A address with a mask length of 8, type B address with a mask length of 16, and type C address , The mask length is 24.

22.2.1.2. IPv6 address pool

When the IPv6 address pool receives a DHCPv6 request message, it will select an appropriate range for address assignment.

- When applying for a directly connected network segment, a matching range (one or more) will be selected based on the IPv6 address of the Layer 3 interface that received the DHCPv6 request message.
- When applying for a non-directly connected network segment, the DHCPv6 RELAY-FORW message sent through the DHCPv6 Relay agent will carry the Relay message, and the matching range can be selected through the Relay message information.

After the DHCPv6 Client obtains the IPv6 address from the Server, its prefix length is obtained according to the RA message sent by the gateway device. See the description of "IPv6 RA" in the next section for details.

If no matching range is found, the DHCPv6 Server will not respond to the DHCPv6 message.

22.2.1.3. IPv6 RA

IPv6 dynamic address acquisition is divided into stateless and stateful. When using stateless to dynamically allocate addresses, it does not rely on the DHCP protocol, but is done through RA messages. The device as the gateway will periodically send RA messages, and all nodes in the network segment will be notified of the prefix and prefix length of the network segment through

multicast IP. When an RS message is received, an RA response message will also be sent out with unicast IP.

- When using stateless to dynamically apply for an IPv6 address, the client will obtain the prefix and prefix length of the network segment according to the RA message, thereby automatically generating an IPv6 address (that is, SLAAC address, Stateless address autoconfiguration), and pass the ND protocol (NS and NA) Avoid conflicts between the IPv6 addresses of multiple nodes in this network segment. Other parameters such as DNS Server, Domain name, etc. are still obtained through the DHCP protocol.
- When using stateful to dynamically apply for an IPv6 address, the IPv6 address and other parameters are all done through the DHCP protocol. Only the prefix length is obtained through RA packets.

There are two types of IPv6 range configurations: address range-based and interface-based. There are three modes based on the address range: stateless, stateful, and stateful-less (stateful + stateless). Based on the interface, two modes can be configured, stateless and ra-only. The specific description is as follows:

Configuration Method	Model	DHCP-assigned Address	SLAAC Address	Other Parameters
Address range	Stateless	No	Yes	DHCP protocol
	Stateful	Yes	No	DHCP protocol
	Stateful-less	Yes	Yes	DHCP protocol
Interface	Stateless	No	Yes	DHCP protocol
	Ra-only	No	Yes	No

22.2.1.4. Other parameters

- Lease: Indicates the lease period of the assigned IP address, the default is 1 hour. Before the lease expires, the DHCP Client will reconfirm. If the lease expires, the DHCP Client is no longer online. The DHCP Server will reclaim the IP address to the address pool. This parameter can revise the lease value of the IP address in the corresponding range.
- Set-tag: This parameter can be marked with a tag for the range. When used for Option setting, if a certain tag is matched, Opiton does not take effect for all ranges, but only takes effect for the range identified by the tag. For details, see the detailed description of "Tag Parameters" below.

22.2.2. Static binding

The IP addresses in the address pool are dynamically allocated, and in some scenarios, it is hoped that some clients will use a certain IP address. At this time, the method of dynamic allocation through the address pool cannot meet the demand. DHCP Server can achieve this goal through statically bound IP addresses.

The static binding configuration function and the address pool function of the range configuration are completely independent. In order to avoid IP conflicts, the statically bound configured IP address needs to be excluded from the address pool (manual configuration is required to remove it), otherwise, there may be two nodes with the same IP address in the network.

The static binding of DHCPv4 can be based on one or more of the following three parameters:

- MAC address: selected from the source MAC address of the DHCP message sent by the DHCPv4 Client.
- Client-id: selected from option 61 (client-id field) of the DHCP message sent by the DHCPv4 Client.
- Hostname: Select option 12 (hostname field) of the DHCP message sent by the DHCPv4 Client.

The static binding of DHCPv6 is based on the DUID parameter:

- DUID: selected from option1 (client-id field) of the DHCPv6 message sent by the DHCPv6 Client.

The lease period of the IP address configured by static binding is 1 hour by default, which can be set and modified by carrying the lease parameter. You can also set tag parameters through set-tag, which is used for matching when setting option.

22.2.3. Option setting

DHCP Server option settings are divided into three categories: well-known options, based on option ID settings, and based on option names. The latter two cases can cover all options. Through the command show dhcp server opt-list and show dhcp server opt6-list, you can view all the options of DHCPv4 and DHCPv6 respectively.

The well-known options only support the following three, and DHCPv6 only supports dns-server among them.

- Dns-server: Configure DNS server, corresponding to Option 6 of DHCPv4 or Option 23 of DHCPv6.
- Default-router: Only supports DHCPv4, the default gateway. If it is not set, the IP address is assigned to the directly connected network, the gateway is the local Layer 3 IPv4 address of the Server, and the IP address assigned by the non-directly connected DHCP Realy is the gateway The IP address of the Relay node (Relay agent IP). Corresponds to Option 3 of DHCPv4.
- Domain-name: Only supports DHCPv4, domain name. Corresponds to Option 15 of DHCPv4.

Special attention is needed: when setting Option based on option ID or option name, if the corresponding Value is an IPv6 address, you need to add "[ ]" before and after the IPv6 address. When setting the IPv6 address for the well-known option Dns-server, it is not required.

22.2.4. Tag parameters

Sometimes, we need to set different options for different address pool ranges or different statically bound IP addresses, we need to use the Tag parameter to complete.

By setting the Tag parameter, the range of the address pool or statically bound IP addresses can be grouped. Then when setting the option, through the match tag parameter, you can set it only for a certain group. In this way, the purpose of group control is achieved.

For example:range 1 is 192.168.1.50 – 192.168.1.100

range2 is 192.168.1.150-192.168.1.180

range3 is 192.168.2.1-192.168.2.254

range4 is 192.168.3.10-192.168.3.80

Statically bound 192.168.1.33

If you need the IP address assigned by range1 and range2 and the corresponding gateway of 192.168.1.33 is 192.168.1.2; the IP address assigned by range3 corresponds to the local Layer 3 port IP address of the Server (default behavior); the IP address assigned by range4 corresponds to the gateway 192.168 .3.8

You can configure as follows:

- Set the tag of range1 and range2 to tag1; set the statically bound 192.168.1.33 tag to tag1; set the tag of range4 to tag2.
- Set the default-router option of match tag1 to 192.168.1.2; set the default-router option of match tag2 to 192.168.3.8.

22.3. Configuration command

Enable DHCP service

SWITCH(config)#**service dhcp**

To use the DHCP Server, the DHCP service must be enabled.

Enter DHCP Server configuration mode

SWITCH(config)#**dhcp server**

SWITCH(config-dhcp-server)#

Use "exit" to exit the dhcp server mode.

In configuration mode, use the "no dhcp server" command to clear all DHCP Server-related configurations.

Configure IPv4 address pool range

SWITCH(config-dhcp-server)#**range** *RANGE-NAME START-IP END-IP* (*{***netmask** *A.B.C.D* | **lease** *<0-65535>* | **set-tag** *TAG-NAME}* | *)*

The range must have a name and the length cannot exceed 63 characters. The names of different ranges must be different.

The range cannot be modified. If you need to modify it, you can only delete it first and then reconfigure it.

Use the command "no range RANGE-NAME" when deleting a range.

Start-IP and End-IP indicate the range of addresses included in the range and must belong to a network segment. Use the format of A.B.C.D to represent.

netmask, lease and set-tag are optional parameters. For a detailed description of netmask, please refer to the chapter "Detailed Functions-Address Pool-IPv4 Address Pool".

The unit of Lease is minutes, and the default lease period is 1 hour. If set to 0, the lease period is permanent and never expires.

The length of set-tag cannot exceed 63 characters, and multiple ranges can set the same tag.

Configure IPv6 address pool range

SWITCH(config-dhcp-server)#**range** *RANGE-NAME START-IP END-IP* (**{lease** *<0-65535>* | ***mode*** (***stateful*** | ***stateless*** | ***stateful-less***) **set-tag** *TAG-NAME}* |)

The START-IP and END-IP addresses use the X:X::X:X format. According to the address format, it is judged whether the range is the range of the IPv4 address pool or the IPv6 address pool.

mode, Lease and Set-tag are optional parameters.

Mode can choose one of three modes: stateful, stateless and stateful-less. If the mode parameter is not configured, the stateful mode is used by default.

The unit of Lease is minutes, and the default lease period is 1 hour. If set to 0, the lease period is permanent and never expires.

The length of set-tag cannot exceed 63 characters, and multiple ranges can set the same tag. The option settings for DHCPv4 and DHCPv6 are independent. Therefore, the tag name space of the IPv4 address pool and the tag name space of the IPv6 address pool are also independent.

Use the command "no range RANGE-NAME" when deleting a range.

Configure interface-based IPv6 range

SWITCH(config-dhcp-server)#**range** *RANGE-NAME* **interface** IFNAME ***mode*** (***stateless*** (**set-tag** *TAG-NAME* |) | ***ra-only***)

The interface-based IPv6 range uses interface as a keyword to distinguish the above-mentioned IPv4 and IPv6 address pools.

。Mode is a required parameter, you can choose one of two modes: stateless and ra-only.

When the mode is stateless, Set-tag is an optional parameter, and the length cannot exceed 63 characters. Multiple ranges can set the same tag.

Use the command "no range RANGE-NAME" when deleting a range.

Configure static binding IPv4 address

SWITCH(config-dhcp-server)#**host** *A.B.C.D* **{match-mac** *XX:XX:XX:XX:XX:XX* | **match-hostname** *WORD* | **match-client-id** *WORD***}** **({lease** *<0-65535>* | **set-tag** *TAG-NAME***} |)**

The static binding configuration function and the address pool function of the range configuration are completely independent. In order to avoid IP conflicts, the IP address configured by static binding needs to be excluded from the address pool (it needs to be removed by manual configuration).

There are three match parameters for statically binding IPv4 addresses: MAC address, hostname, and client-id. One or more of these three parameters can be selected. For the detailed introduction of the Match parameter, please refer to the chapter "Detailed Function-Static Binding".

Lease and Set-tag are optional parameters. The unit of Lease is minutes, and the default lease period is 1 hour. If set to 0, the lease period is permanent and never expires. The length of the set-tag cannot exceed 63 characters.

Use the command "no host A.B.C.D" to delete the statically bound IPv4 address.

Configure static binding IPv6 address

SWITCH(config-dhcp-server)#**host6** *X:X::X:X* **match-duid** *WORD* (**{lease** *<0-65535>* | **set-tag** *TAG-NAME}* |)

The static binding configuration function and the address pool function of the range configuration are completely independent. In order to avoid IP conflicts, the IP address configured by static binding needs to be excluded from the address pool (it needs to be removed by manual configuration).

The match parameter for statically bound IPv6 addresses is only DUID. For details, please refer to the chapter "Functional Details-Static Binding".

Lease and Set-tag are optional parameters. The unit of Lease is minutes, and the default lease period is 1 hour. If set to 0, the lease period is permanent and never expires. The length of the set-tag cannot exceed 63 characters.

Use the command "no host6 X:X::X:X" to delete the statically bound IPv6 address.

Configure well-known option: Default-router

SWITCH(config-dhcp-server)#**default-router** *A.B.C.D (***tag** *TAG-NAME |)*

This option is only for DHCPv4 and corresponds to DHCPv4 option 3.

Tag is an optional parameter. If the tag parameter is carried, it will only take effect for the range or statically bound IP with the tag set; if the tag parameter is not carried, it will take effect for all ranges or statically bound IPs.

Tag will also be used as the key of the option, that is, the two commands are configured with the same IP value, but one carries the tag and the other does not carry the tag, the two commands will be considered as different commands.

The corresponding delete command is "no default-router A.B.C.D (tag TAG-NAME |)". If the tag parameter is carried when setting, the same tag parameter must be carried when deleting, otherwise it cannot be deleted.

Configure well-known option: Dns-server

SWITCH(config-dhcp-server)#**dns-server** *(A.B.C.D | X:X::X:X) (***tag** *TAG-NAME |)*

This option can be used for DHCPv4, corresponding to option 6. It can also be used for DHCPv6, corresponding to option23. Determine whether it is DHCPv4 or DHCPv6 according to the format of the IP address. It should be noted that there is no need to add "[ ]" to the IPv6 address here.

Tag is an optional parameter. If the tag parameter is carried, it will only take effect for the range or statically bound IP with the tag set; if the tag parameter is not carried, it will take effect for all ranges or statically bound IPs.

Tag will also be used as the key of the option, that is, the two commands are configured with the same IP value, but one carries the tag and the other does not carry the tag, the two commands will be considered as different commands.

The corresponding delete command is "no dns-server (A.B.C.D | X:X::X:X) (tag TAG-NAME |)". If the tag parameter is carried when setting, the same tag parameter must be carried when deleting, otherwise it cannot be deleted.

Configure well-known option: domain-name

SWITCH(config-dhcp-server)#**domain-name** *DOMAIN (***tag** *TAG-NAME |)*

This option is only for DHCPv4 and corresponds to DHCPv4 option 15.

The DOMAIN parameter is a character string with a length not exceeding 255.

Tag is an optional parameter. If the tag parameter is carried, it will only take effect for the range or statically bound IP with the tag set; if the tag parameter is not carried, it will take effect for all ranges or statically bound IPs.

Tag will also be used as the key of the option, that is, two commands are configured with the DOMAIN parameter, but one carries the tag and the other does not carry the tag, the two commands will be considered as different commands.

The corresponding delete command is "no domain-name DOMAIN (tag TAG-NAME |)". If the tag parameter is carried when setting, the same tag parameter must be carried when deleting, otherwise it cannot be deleted.

Configure option based on ID

DHCPv4 option:

SWITCH(config-dhcp-server)#**option id <0-255>** *OPT-VALUE (***tag** *TAG-NAME |)*

DHCPv6 option:

SWITCH(config-dhcp-server)#**option6 id <0-255>** *OPT-VALUE (***tag** *TAG-NAME |)*

You can view the DHCPv4 Option list and DHCPv6 Option list through "show dhcp server opt-list" and "show dhcp server opt6-list" in privileged mode. Which lists the Option ID and name.

The OPT-VALUE parameter is a string with a length not exceeding 255. It should be noted that if OPT-VALUE corresponds to an IPv6 address, then the IPv6 address needs to be added with "[ ]" before and after it.

Tag is an optional parameter. If the tag parameter is carried, it will only take effect for the range or statically bound IP with the tag set; if the tag parameter is not carried, it will take effect for all ranges or statically bound IPs.

Tag will also be used as the key of the option, that is, the two commands are configured with the OPT-VALUE parameter, but one carries the tag and the other does not carry the tag, the two commands will be considered as different commands.

The corresponding delete command is "no option id <0-255> OPT-VALUE (tag TAG-NAME |)" or "no option6 id <0-255> OPT-VALUE (tag TAG-NAME |)". If the tag parameter is carried when setting, the same tag parameter must be carried when deleting, otherwise it cannot be deleted.

Configure option based on name

DHCPv4 option:

SWITCH(config-dhcp-server)#**option name** *OPT-NAME OPT-VALUE (***tag** *TAG-NAME |)*

DHCPv6 option:

SWITCH(config-dhcp-server)#**option6 name** *OPT-NAME OPT-VALUE (***tag** *TAG-NAME |)*

You can view the DHCPv4 Option list and DHCPv6 Option list through "show dhcp server opt-list" and "show dhcp server opt6-list" in privileged mode. Which lists the Option ID and name (name).

When configuring option by name, the name must be exactly the same as the name of the option list from show, and fuzzy matching or abbreviation is not supported. If the corresponding option cannot be found based on the name, the setting fails.

The OPT-VALUE parameter is a string with a length not exceeding 255. It should be noted that if OPT-VALUE corresponds to an IPv6 address, then the IPv6 address needs to be added with "[ ]" before and after it.

Tag is an optional parameter. If the tag parameter is carried, it will only take effect for the range or statically bound IP with the tag set; if the tag parameter is not carried, it will take effect for all ranges or statically bound IPs.

Tag will also be used as the key of the option, that is, the two commands are configured with the OPT-VALUE parameter, but one carries the tag and the other does not carry the tag, the two commands will be considered as different commands.

The corresponding delete command is "no option name OPT-NAME OPT-VALUE (tag TAG-NAME |)" or "no option6 name OPT-NAME OPT-VALUE (tag TAG-NAME |)". If the tag parameter is carried when setting, the same tag parameter must be carried when deleting, otherwise it cannot be deleted.

22.4. Configuration case

Configure a DHCP Server.

- IPv4 three network segments, VLAN 10, IP is 192.168.10.1/24, assigned IP range is 192.168.10.30-192.168.10.100, statically assigned IP 192.168.10.50 (according to MAC 00:00:2a:3f:2e:3d) , 192.168.10.51 (according to the hostname MY-TEST-COMPUTER, the lease time is 40 minutes); VLAN 20, IP is 192.168.20.10/24, the gateway of this network segment is 192.168.20.1, and the assigned IP range is 192.168.20.2-192.168 .20.100, the lease time of this network segment is 30 minutes. VLAN 30, the IP is 192.168.30.1/24, and the assigned IP range is 192.168.30.1-192.168.30.100, and 192.168.30.150-192.168.30.200.

  There is a DHCP Relay device connected to VLAN30, and there will be two network segments applying for IP addresses on it, and the assigned IP ranges are 192.168.100.1-192.168.100.200 and 192.168.101.1-192.168.101.200 respectively.

  The dns-server of VLAN30 is 192.168.5.1, and the dns-server of other network segments is 192.168.5.2.

- IPv6 two network segments, VLAN 10, IP is 2030::1/64, the assigned IP range is 2030::1-2030::ff.

  VLAN 40, the IP is 2040::1/64, and the assigned IP range is 2040::1-2040::ff.

  There are DHCPv6 Realy devices connected to VLAN40, and there will be two network segments applying for IPv6 addresses on them, and the assigned IPv6 ranges are 2050::1-2050::ff,2051::1-2051::ff.

  The dns-server of VLAN10 is 2030::101, and the dns-server of VLAN40 is 2060::1.

As the above requirements, the configuration is as follows:

Configure L3 port and IP address

```
SWITCH(config)#int vlan 10
SWITCH(config-if)#ip address 192.168.10.1/24
SWITCH(config-if)#ipv6 address 2030::1/64
SWITCH(config-if)#exit
SWITCH(config)#int vlan 20
```

```
SWITCH(config-if)#ip address 192.168.20.10/24
SWITCH(config-if)#exit
SWITCH(config)#int vlan 30
SWITCH(config-if)#ip address 192.168.30.1/24
SWITCH(config-if)#exit
SWITCH(config)#int vlan 40
SWITCH(config-if)#ipv6 address 2040::1/64
SWITCH(config-if)#exit
SWITCH(config)#
```

Enable DHCP service

```
SWITCH(config)#service dhcp
```

Configure DHCP Server range

```
SWITCH(config)#dhcp server
SWITCH(config-dhcp-server)#range vlan10-ipv4-1 192.168.10.30 192.168.10.49
SWITCH(config-dhcp-server)#range vlan10-ipv4-2 192.168.10.52 192.168.10.100
SWITCH(config-dhcp-server)#range vlan20-ipv4 192.168.20.2 192.168.20.100 lease 30 set-tag vlan20-ipv4
SWITCH(config-dhcp-server)#range vlan30-ipv4-1 192.168.30.1 192.168.30.100 set-tag vlan30-ipv4
SWITCH(config-dhcp-server)#range vlan30-ipv4-2 192.168.30.150 192.168.30.200 set-tag vlan30-ipv4
SWITCH(config-dhcp-server)#range vlan10-ipv6 2030::1 2030::ff set-tag vlan10-ipv6
SWITCH(config-dhcp-server)#range vlan40-ipv6 2040::1 2040::ff set-tag vlan40-ipv6
SWITCH(config-dhcp-server)#range vlan30-ipv4-relay-1 192.168.100.1 192.168.100.200
SWITCH(config-dhcp-server)#range vlan30-ipv4-relay-2 192.168.101.1 192.168.101.200
SWITCH(config-dhcp-server)#range vlan40-ipv6-relay-1 2050::1 2050::ff
SWITCH(config-dhcp-server)#range vlan40-ipv6-relay-2 2051::1 2051::ff
```

Configure DHCP Server host

```
SWITCH(config-dhcp-server)#host 192.168.10.50 match-mac 00:00:2a:3f:2e:3d
SWITCH(config-dhcp-server)#host 192.168.10.51 match-hostname MY-TEST-COMPUTER lease 40
```

Configure DHCP Server Option

```
SWITCH(config-dhcp-server)#default-router 192.168.20.1 tag vlan20-ipv4
SWITCH(config-dhcp-server)#dns-server 192.168.5.1 tag vlan30-ipv4
SWITCH(config-dhcp-server)#dns-server 192.168.5.2
SWITCH(config-dhcp-server)#dns-server 2030::101 tag vlan10-ipv6
SWITCH(config-dhcp-server)#dns-server 2060::1 tag vlan40-ipv6
```

22.5. Show command

View DHCP Server configuration information

show dhcp server (range | host | option |) If it carries range, or host, or option, only the configuration information of the corresponding item will be viewed. If it does not carry any parameters, all configuration information will be viewed.

```
SWITCH#show dhcp server
DHCP dynamic IP allocation configuration
--------------------------------------------------------------------
Name            Start IP        End IP          Tag             Mask/Len        Lease
-------------+---------------+---------------+------------+---------------+-----
vlan20-ipv4     192.168.20.2    192.168.20.100  vlan20-ipv4                     30
vlan10-ipv4-2 192.168.10.52     192.168.10.100
vlan30-ipv4-r 192.168.100.1     192.168.100.200
vlan30-ipv4-2 192.168.30.150    192.168.30.200  vlan30-ipv4
vlan30-ipv4-r 192.168.101.1     192.168.101.200
vlan10-ipv4-1 192.168.10.30     192.168.10.49
vlan30-ipv4-1 192.168.30.1      192.168.30.100  vlan30-ipv4
vlan40-ipv6-r 2051::1           2051::ff
vlan40-ipv6-r 2050::1           2050::ff
vlan10-ipv6     2030::1         2030::ff        vlan10-ipv6
vlan40-ipv6     2040::1         2040::ff        vlan40-ipv6

DHCP static IP allocation configuration
---------------------------------------
IPaddr          Tag             Lease Match-Key
---------------+-------------+-----+-----------------------------------------
192.168.10.51                   40      Hostname:MY-TEST-COMPUTER
192.168.10.50                           MAC:00:00:2a:3f:2e:3d

DHCP options configuration
(known:individual command, id:configure with id, name:configure with name)
--------------------------
Tag             Opt ID  Opt Name        Conf Type Opt Value
---------------+-------+-------------+---------+--------------------
vlan20-ipv4     [4]:3   router          known     192.168.20.1
vlan30-ipv4     [4]:6   dns-server      known     192.168.5.1
                [4]:6   dns-server      known     192.168.5.2
```

```
vlan10-ipv6     [6]:23   dns-server     known     [2030::101]
vlan40-ipv6     [6]:23   dns-server     known     [2060::1]
```

View DHCP Server lease information

show dhcp server lease

```
SWITCH#show dhcp server lease
(Hostname + Clinet_id) is printed in the next row if it's exist.
Expire Time              Macaddr/DUID                                  Ipaddr
--------------------+-----------------------------------------+-----------------
Jan  1 01:10:54 1970 7c:ec:9b:10:8a:ff                                 192.168.2.195
  (* + 00:02:7c:ec:9b:10:8a:ff)

Jan  1 01:10:56 1970 00:01:00:01:c7:92:ce:82:7c:ec:9b:10:8a:ff 2020::21
  (* + 2601552639)
```

View the DHCP option list

Show dhcp server opt-list View the DHCPv4 option list

```
SWITCH#show dhcp server opt-list
Opt ID        Opt Name
-----------+-----------------------------
1             netmask
2             time-offset
3             router
6             dns-server
7             log-server
9             lpr-server
12            hostname
13            boot-file-size
15            domain-name
16            swap-server
17            root-path
18            extension-path
19            ip-forward-enable
20            non-local-source-routing
21            policy-filter
22            max-datagram-reassembly
23            default-ttl
26            mtu
27            all-subnets-local
```

```
28              broadcast
31              router-discovery
32              router-solicitation
33              static-route
34              trailer-encapsulation
35              arp-timeout
36              ethernet-encap
37              tcp-ttl
38              tcp-keepalive
… …
```

Show dhcp server opt6-list View the DHCPv6 option list

```
SWITCH#show dhcp server opt6-list
Opt ID          Opt Name
-----------+-----------------------------
1               client-id
2               server-id
3               ia-na
4               ia-ta
5               ia-address
6               oro
7               preference
8               elapsed-time
9               relay-msg
11              auth
12              unicast
13              status-code
14              rapid-commit
15              user-class
16              vendor-class
17              vendor-opts
18              interface-id
19              reconf-msg
20              reconf-accept
21              sip-server-d
22              sip-server-a
23              dns-server
24              domain-list
```

25	ia-pd
26	ia-prefix
27	nis-servers
28	nisp-servers
29	nis-domain-name
30	nisp-domain-name
31	sntp-servers
… …	

23. CONFIGURE 802.1X AUTHENTICATION

The corresponding web network management configuration path is: Home->Security->802.1X authentication, MAC authentication, RADIUS

23.1. Protocol overview

The IEEE802 LAN/WAN committee proposed the 802.1X protocol in order to solve the problem of wireless LAN network security. Later, the 802.1X protocol was widely used in Ethernet as a common access control mechanism for LAN ports, mainly to solve the problems of authentication and security in the Ethernet.

The 802.1X protocol is a port-based network access control protocol (port based network access control protocol). "Port-based network access control" means that at the port level of the LAN access device, the accessed user equipment is authenticated to control access to network resources.

23.1.1. 802.1X architecture

The 802.1X system is a typical Client/Server structure, as shown in the figure below, including three entities: client (Client), device (Device) and authentication server (Server).

- The client is an entity located at one end of the LAN segment and is authenticated by the device at the other end of the link. The client is generally a user terminal device, and the user can initiate 802.1X authentication by starting the client software. The client must support EAPOL (Extensible Authentication Protocol over LAN).
- The device end is another entity located at one end of the LAN segment, which authenticates the connected client. The device side is usually a network device that supports the 802.1X protocol. It provides a port for the client to access the LAN. The port can be a physical port or a logical port.
- The authentication server is an entity that provides authentication services for the device. The authentication server is used to implement authentication, authorization, and accounting for users, and is usually a RADIUS (Remote Authentication Dial-In User Service) server.

23.1.2. 802.1X authentication method

The 802.1X authentication system uses EAP (Extensible Authentication Protocol) to realize the exchange of authentication information between the client, the device and the authentication server.

- Between the client and the device, the EAP protocol message uses the EAPOL encapsulation format and is directly carried in the LAN environment.
- There are two ways to exchange information between the device and the RADIUS server. One is that the EAP protocol message is relayed by the device and carried in the RADIUS protocol using the EAPOR (EAP over RADIUS) encapsulation format; the other is that the EAP protocol message is terminated by the device and adopts the password authentication protocol (PAP). , Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) attribute messages interact with the RADIUS server for authentication.

23.1.3. Basic concepts of 802.1X

Controlled/uncontrolled port

The device side provides a port for the client to access the LAN. This port is divided into two logical ports: a controlled port and an uncontrolled port. Any frame arriving at this port is visible on both the controlled port and the uncontrolled port.

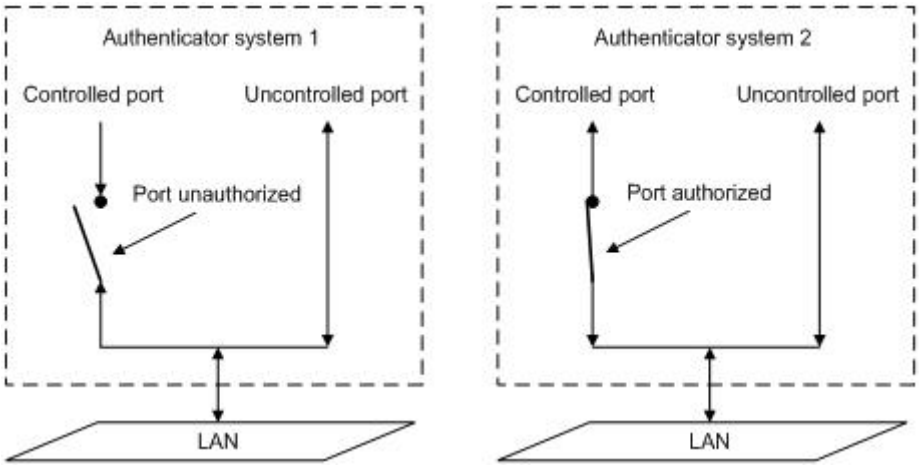
- The uncontrolled port is always in a two-way connection state, and is mainly used to transmit EAPOL protocol frames to ensure that the client can always send or receive authentication messages.
- The controlled port is in a two-way connection state in the authorized state, and is used to transmit business packets; in the unauthorized state, it is forbidden to receive any packets from the client.

Authorized/non-authorized status

The device uses the authentication server to perform authentication on the clients that need to access the LAN, and according to the authentication result (Accept or Reject), it controls the authorized/unauthorized status of the controlled port accordingly.

Figure 19-2 shows the influence of different authorization states on the controlled port on packets passing through the port. The figure compares the port status of two 802.1X authentication systems. The controlled port of system 1 is in an unauthorized state (equivalent to the port switch is turned on), and the controlled port of system 2 is in an authorized state (equivalent to the port switch is turned off).

Figure 19-2 Impact of authorization status on controlled ports



The user can control the authorization status of the port through the access control mode configured under the port. The port supports the following three access control modes:

- Authorized-force mode (authorized-force): indicates that the port is always in an authorized state, allowing users to access network resources without authentication and authorization.
- Unauthorized-force mode (unauthorized-force): indicates that the port is always in an unauthorized state, and users are not allowed to authenticate. The device does not provide authentication services to clients that access through this port.
- Automatic recognition mode (auto): indicates that the initial state of the port is unauthorized, and only allows EAPOL messages to be sent and received, and does not allow users to access network resources; if the authentication is passed, the port switches to an authorized state, allowing users to access network resources. This is also the most common situation.

Controlled direction

In the non-authorized state, the controlled port can be set to one-way controlled and two-way controlled.

- When two-way control is implemented, the sending and receiving of frames is prohibited;
- When implementing one-way control, it is forbidden to receive frames from the client, but it is allowed to send frames to the client.

Currently, only one-way control is supported.

23.2. Configuration command

Enable 802.1X authentication globally

SWITCH(config)# **dot1x enable**

Enable 802.1X authentication on the port

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

Configure RADIUS server
SWITCH(config)# **radius-server host** A.B.C.D [**auth-port** <0-65535>] [**acct-port** <0-65535>] [**key** WORD]

The default authentication port is 1812, and the accounting port is 1813;

Please ensure that the RADIUS server and the device management address are interoperable;

Configure the EAPOL protocol version number
SWITCH(config-if)# **dot1x protocol-version** <1-2>

The default version number is 2;

Configure the authentication quiet time
SWITCH(config-if)# **dot1x quiet-period** <1-65535>

The unit is seconds, and the default silent time is 60 seconds;

Configure the re-authentication function
SWITCH(config-if)# **dot1x reauthentication**

Off by default;

Configure the maximum number of re-authentication
SWITCH(config-if)# **dot1x reauthMax** <1-10>

Configure the maximum number of port re-authentication. If the number of re-authentication requests exceeds the limit and there is no response, the port becomes unauthorized;

The default maximum number of times is 2;

Configure the enable key transmission capability
SWITCH(config-if)# **dot1x keytxenabled** (**disable | enable**)

Off by default;

Configure port 802.1X timer timeout time

SWITCH(config-if)# **dot1x timeout** (**re-authperiod** <1-4294967295> **| server-timeout** <1-65535> **| supp-timeout** <1-65535> **| tx-period** <1-65535>)

The unit is seconds;

The default re-authentication period is 3600 seconds;

The default server timeout period is 30 seconds;

The default client authentication timeout period is 30 seconds;

The default client request timeout time is 30 seconds;

Enable MAC authentication globally
SWITCH(config)# **mac-auth enable**

Port opening and closing MAC authentication
SWITCH(config-if)# **mac-auth** (**enable | disable**)

Port opening and closing MAC authentication dynamic VLAN delivery
SWITCH(config-if)# **mac-auth dynamic-vlan-creation (enable | disable**)

The current version does not support;

Configure MAC authentication failure handling behavior
SWITCH(config-if)# **mac-auth auth-fail-action** (**drop-traffic | restrict-vlan** <2-4094>)

The default is drop-traffic: drop traffic.

The current version does not support;

Configure the RADIUS server dead time
SWITCH(config)# **radius-server deadtime** <0-1440>

Configure the dead time of the RADIUS server. During the authentication process, the dead server is automatically skipped, and the undead server is selected for authentication.

Unit: minutes, the default is 0 minutes;

Configure the default key of the RADIUS server
SWITCH(config)# **radius-server key** STRING

Configure RADIUS server retransmission times
SWITCH(config)# **radius-server retransmit** <1-100>

The default is 3 times;

Configure the timeout period of the RADIUS server
SWITCH(config)# **radius-server timeout** <1- 60>

Unit: seconds, the default is 5 seconds;

23.3. Configuration case

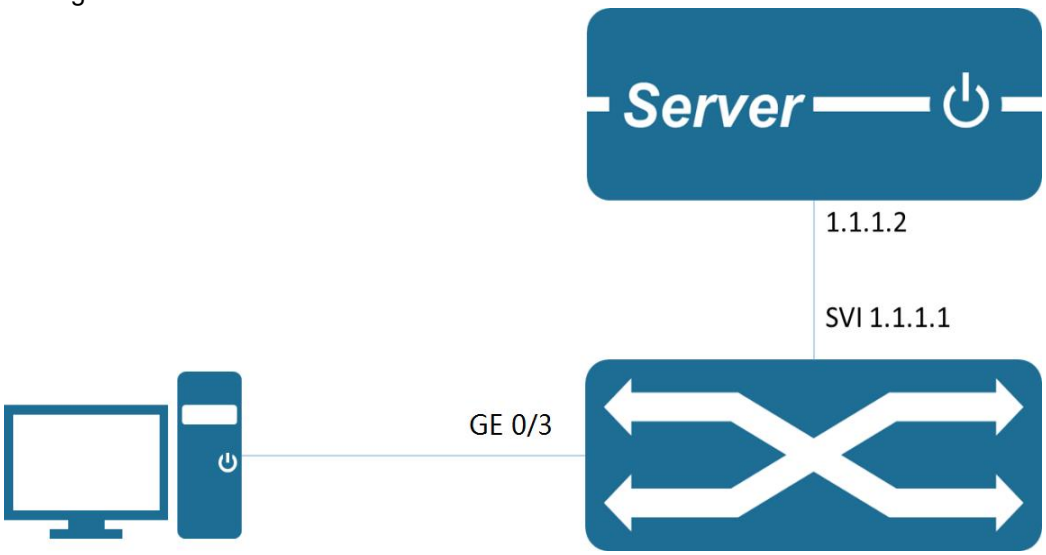
802.1X port authentication scenario

1) Demand

- It is required to authenticate access users on port GigabitEthernet0/3 to control their access to the Internet.

- The IP address of the RADIUS server group is 1.1.1.2.
- Set the shared key to be used when the system exchanges messages with the RADIUS server as name.

2) Network diagram



3) Typical configuration example

Switch reference configuration

```
SWITCH(config)#dot1x enable
SWITCH(config)#interface GigabitEthernet0/3
SWITCH(config-if)#dot1x port-control auto
SWITCH(config-if)#exit
SWITCH(config)#radius-server host 1.1.1.2 key name
```

Server-side reference configuration

Configure NAS authentication device 1.1.1.1 and communication key name.

Add user account test password test.

Need to support the corresponding authentication method, such as EAP-MSCHAPv2

Client reference configuration

Open the 802.1X authentication client and log in with the account test.

Need to support the corresponding authentication method, such as EAP-MSCHAPv2 method..

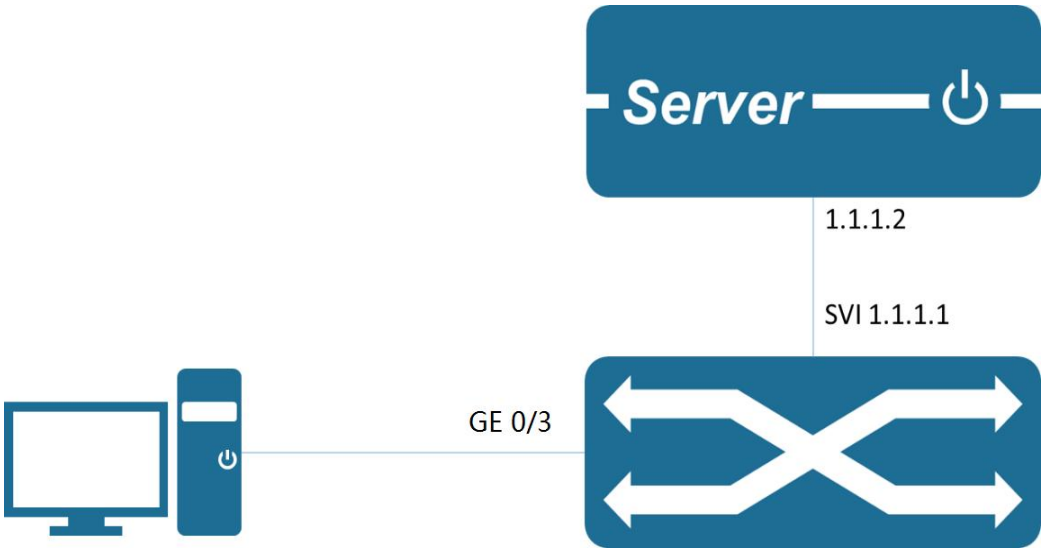
MAC authentication scenario

1) Demand

- It is required to authenticate access users on port GigabitEthernet0/3 to control their access to the Internet.
- The IP address of the RADIUS server group is 1.1.1.2.

- Set the shared key to be used when the system exchanges messages with the RADIUS server as name.

2) Network diagram



3) Typical configuration example

Switch reference configuration

```
SWITCH(config)# mac-auth enable
SWITCH(config)#interface GigabitEthernet0/3
SWITCH(config-if)#mac-auth enable
SWITCH(config-if)#exit
SWITCH(config)#radius-server host 1.1.1.2 key name
```

Server-side reference configuration

Configure NAS authentication device 1.1.1.1 and communication key name.

Configure the corresponding authentication method as EAP-MD5.

Add the client MAC address as the user account and password to the user database.

Client reference configuration

Open the 802.1X authentication client and log in with any account.

23.4. Show command

Show 802.1X port authentication information

SWITCH#**show dot1x all**

```
SWITCH#show dot1x all
802.1X Port-Based Authentication Enabled
```

```
  RADIUS server address: 1.1.1.2:1812
  Next radius message id: 0
  RADIUS client address: not configured


802.1X info for interface GigabitEthernet0/6
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 1
  protocol version: 2
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connecting - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 0
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
```

Show MAC authentication information

SWITCH#**show bridge**

```
SWITCH#show bridge
 Bridge      CVLAN   SVLAN   BVLAN   Port              MAC Address          FWD
Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
SWITCH#
```

24. CONFIGURE OUTLET FILTERING

The corresponding web network management configuration path is: Home -> Interface -> Export Filter

24.1. Overview of Outlet Filtration

Unknown unicast and multicast packets in the network will be flooded in the device. This function can be used to filter and protect the port to prevent flooded packets from being output from the designated port.

Export filtering supports filtering unicast and multicast packets.

24.2. Configuration command

Configure egress unicast filtering
SWITCH(config-if)#**switchport block unicast**
Only supports configuration on physical ports;
Configure egress multicast filtering
SWITCH(config-if)#**switchport block multicast**
Only supports configuration on physical ports;