NEO WAVE®

Switch Software Configuration & Operation Manual

Switch Software Configuration Guide

pages 2-220

Software version：Release 7.3.x

Release Notes：October 18, 2024

1. System Management

1.1. Command Line Interface Mode

The command line interface is divided into many different modes, The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

Table following describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the hostname SWITCH.

Table Command Mode Summary

Mode	Prompt	Enter Or Exit	About This Mode
User Exec	SWITCH>	Enter exit to quit	Use this mode to: Perform basic tests. Display system information.
Privileged Mode	SWITCH#	While in user EXEC mode, enter the enable command. Enter disable to exit.	Use this mode to: Exec network utilities. Display module information. System management operation.
Global Configuration	SWITCH(config)#	While in Privileged mode, enter the configuration terminal command. Enter exit or end to return.	Use this mode to: configure parameters that apply to the entire switch.
Interface Configuration	SWITCH(config-if)#	While in global configuration mode, e interface command (with a specific interface). Enter exit or end to return.	Use this mode to: configure parameters for the Ethernet ports.

1.2. Management IP Address

1.2.1. Configuring

- Manually Assigning IPv4 Information

Command	SWITCH(config)#**management vlan** VLANID **ip address** IPADDR/MASKLEN **gateway** IPADDR SWITCH(config)#**no management vlan**
Description	Manually assigning switch management IPv4 information.

- Configuring DHCP-Based IPv4 Information Autoconfiguration

Command	SWITCH(config)#**management vlan** VLANID **ip address dhcp** SWITCH(config)#**no management vlan**
Description	Configuring DHCP-Based IPv4 information autoconfiguration.

- Manually Assigning IPv6 Information

Command	SWITCH(config)#**management vlan** VLANID **ipv6 address** IPV6ADDR/MASKLEN **gateway** IPV6ADDR SWITCH(config)#**no management vlan**
Description	Manually assigning switch management IPv6 information.

- Configuring DHCP-Based IPv6 Information Autoconfiguration

Command	SWITCH(config)#**management vlan** VLANID **ipv6 address dhcp** SWITCH(config)#**no management vlan**
Description	Configuring DHCP-Based IPv6 information autoconfiguration.

- Display IP Information

Command	SWITCH#**show management summary**
Description	Display IP information.

1.2.2. Examples

Example 1: Manually assigning IPv4 information.

The following examples shows how to configure management IPv4 address, The management VLAN is 1, the management IP is 192.168.64.200/24, and the gateway address is 192.168.64.1.

Manually assigning IPv4 information:

```
SWITCH#configure terminal
SWITCH(config)#management vlan 1 ip address 192.168.64.200/24 gateway 192.168.64.1
```

Display IP information:

```
SWITCH#show management summary
Management interface with Ipv4:
Type:        Static
Vlan:        1
Ip address:  192.168.64.200/24
Gateway:     192.168.64.1
```

1.3. Backup/Restore Configuration

1.3.1. Configuring

- Backup Configuration

Command	SWITCH#write
Description	Save your entries in the configuration file.

- Restore Configuration

Command	SWITCH#**copy default-config startup-config** SWITCH#**reload**
Description	Restore the system default configuration, which will take effect after the device restarts.

- Configuration Import By TFTP

Command	SWITCH#**copy tftp tftp://A.B.C.D/FILE startup-config** SWITCH#**reload**
Description	A.B.C.D: remote tftp server ip address FILE: File name of configuration Import the remote configuration into the device through the tftp protocol, replacing the existing configuration. Take effect after device restart.

- Configuration Export By TFTP

Command	SWITCH#**copy startup-config tftp tftp://A.B.C.D/FILE**
Description	A.B.C.D: remote tftp server ip address FILE: File name of configuration Through the tftp protocol, the configuration is saved to the specified folder of the remote tftp server.

- Configuration Import By FTP

Command	SWITCH#**copy ftp ftp://A.B.C.D/FILE startup-config** SWITCH#**reload**
Description	A.B.C.D: remote tftp server ip address FILE: File name of configuration

	Import the remote configuration into the device through the ftp protocol, replacing the existing configuration. Take effect after device restart.

- Configuration Export By FTP

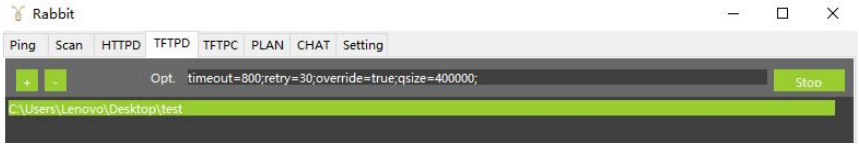
Command	SWITCH#**copy startup-config ftp ftp://A.B.C.D/FILE**
Description	A.B.C.D：remote tftp server ip address FILE：File name of configuration Through the ftp protocol, the configuration is saved to the specified folder of the remote tftp server.

1.3.2. Examples

Example 1：Export the configuration to the folder specified by the remote tftp server, the file name is startup.conf.

Environment construction：

The remote PC starts the tftp server and selects the tftp current directory.



The IP address of the remote PC is 192.168.64.1, and the management IP of the switch is configured as 192.168.64.100, and the remote PC can be pinged. Execute the configuration export command：

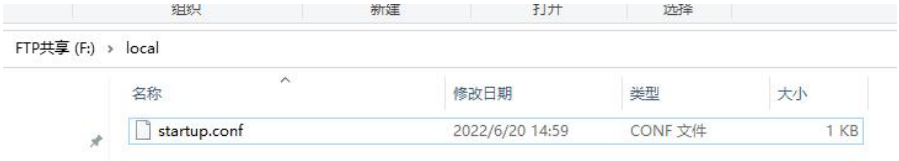
```
SWITCH#
SWITCH# copy startup-config tftp tftp://192.168.64.1/startup.conf
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1230    0     0  100  1230      0   151k --:--:-- --:--:-- --:--:--  240k
100  1230    0     0  100  1230      0   144k --:--:-- --:--:-- --:--:--  144k
Copy Success
```

In the test directory of the remote PC, you can view the newly created startup.conf file.

Example 2：Import the configuration file startup.conf under the folder specified by the remote ftp server into the device.

Environment construction：

Start the ftp server on the remote PC, select the current directory of ftp, and place the startup.conf file.



The IP address of the remote PC is 192.168.64.1, and the switch management IP is configured as 192.168.64.100, and the remote PC can be pinged. Execute the configuration import command：

```
SWITCH#
SWITCH# #copy ftp ftp://192.168.64.1/startup.conf startup-config
Enter Username:xxxxxx
Enter Password:xxxxxx
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   973  100   973    0     0  42572      0 --:--:-- --:--:-- --:--:-- 48650
Copy Success
```

After the configuration is imported, restart to take effect.

1.4. Clearing Log

- Clearing system log

Command	SWITCH# **clear logging**
Description	Clear system log

1.5. System Warm Restart

- System Warm Restart

Command	SWITCH#**reload**
Description	System warm restart.

1.6. Local User and Privilege Management

By assigning different privileges to users and defining different privilege levels for different functions, you can control user access to network devices.

The command line interface of network devices is divided into 16 levels of privileges from 0 to 15 for users . Users of different levels are allowed to execute different commands. The smaller the number, the lower the level of privilege, with 0 being the lowest level and 15 being the highest level . Levels 0 to 1 are called ordinary user levels, which do not allow configuration of the device by default. Levels 2 to 15 are called privileged user levels, which allow configuration of the device. Level 15 is the management user level, which supports all management behaviors .

1.6.1. Configuring

- Add and Delete Users , Modify User Password , Modify User Privileges

Command	SWITCH(config)# **username** NAME {| **privilege** <0-15>} {| **password** LINE} SWITCH(config)# **no username** NAME
Description	If the user NAME does not exist, add a new user ; if it exists, modify the user's password; The device comes with a factory default user "admin" and password "admin" , which supports password modification and deletion operations; User and password length is 0-32 bytes; The password is displayed in encrypted form; Password characters are case sensitive ; delete operation does not support deleting the user itself; to delete an online user, you must first kick the user offline; Create a user. If there is no privilege information, the default privilege level 15 is used;

- Configuring Command Line Privileges

Command	SWITCH(config)# **privilege** {**config** | **exec** | **show**} **level** <0-15> **command** STRING SWITCH(config)# **no privilege** {**config** | **exec** | **show**} {| **level** <0-15>} **command** STRING
Description	Configuring command line privileges Support command privilege configuration in the three modes of exec, show and config Privilege configuration range <0-15>

- Configuring Line Vty Privilege

Command	SWITCH(config)#**line vty** 0 SWITCH(config)# **privilege level** <0-15>

	SWITCH(config)# **no privilege level**
Description	Configure privilege for line vty The default privilege is 15 If the user logs in to the vty, the actual user privilege are the smaller value of the user privilege and the line vty privilege.

1.6.2. Display Information

- Display the Default Privilege and Configuration Privilege of the Command Lline in Each Mode

```
SWITCH#show privilege commands exec
Command       Default privilege Current privilege
clock         15                15
configure     10                8
copy          15                15
disable       0                 0
enable        0                 0
errdisable    10                8
ping          10                12
reload        15                8
telnet        10                12
terminal      0                 8
traceroute    10                10
upgrade       15                14
usb           15                14
write         15                10
```

1.7. Login Management

1.7.1. Configuring

1.7.1.1. Service Enablement Management

- Configure and Enable WEB Management

Command	SWITCH(config)# **web-server enable** { **all | http | https** } SWITCH(config)# **no web-server enable**
Description	Configure and enable WEB management. Default disabled state. Support IPv4 and IPv6.

- Configure and Enable Telnet Management

Command	SWITCH(config)# **telnet-server enable** SWITCH(config)# **no telnet-server enable**
Description	Configure and enable telnet management. Default disabled state. Support IPv4 and IPv6.

- Configure and Enable SSH Management

Command	SWITCH(config)# **ssh-server enable** SWITCH(config)# **no ssh-server enable**
Description	Configure and enable SSH management. Default disabled state. Support IPv4 and IPv6.

1.7.1.2. ACL Applied to Services

- IPv4 ACL Applied to Services

Command	SWITCH(config)# **ip** { **telnet** | **ssh** | **http** | **https** } **access-class** {<1-199> | <1300-2699> | ACLNAME} SWITCH(config)# **no ip** { **telnet** | **ssh** | **http** | **https** } **access-class**
Description	IPv4 ACL is applied to telnet, ssh, http, https and other services. Users who meet the ACL permit rules are allowed to access the device, otherwise users cannot access the device.

- IPv6 ACL Applied to Services

Command	SWITCH(config)# **ipv6** { **telnet** | **ssh** | **http** | **https** } **access-class** { ACLNAME } SWITCH(config)# **no ipv6** { **telnet** | **ssh** | **http** | **https** } **access-class**
Description	IPv6 ACL is applied to telnet, ssh, http, https and other services. Users who meet the ACL permit rules are allowed to access the device, otherwise users cannot access the device.

1.7.1.3. ACL Applied to Vty

- ACL Applied to Vty

Command	SWITCH(config-line)# **access-class** {<1-199> | <1300-2699> | ACLNAME } **in** SWITCH(config-line)# no **access-class** {<1-199> | <1300-2699> | ACLNAME } **in**
Description	ACL applied to vty. For telnet, ssh and other servers on vty. Users who meet the ACL permit rules are allowed to login by this line.

1.7.1.4. Service Management Based on Line

- Configure Services Supported on Line Vty

Command	SWITCH(config-line)# **transport input** { **telnet** | **ssh** | **all** | **none** } SWITCH(config-line)# no **transport input**
Description	Configure services supported on vty. telnet: only supports telnet service. ssh: only supports ssh service. all: supports telnet and ssh services. none: No services are supported. Supports telnet and ssh services by default.

1.7.1.5. Other Commands

- Kick Online Users Offline

Command	SWITCH# **clear line** { **vty | console** } LINE
Description	Vty represents the remote login user. Console represents the serial port login user. LINE information can be viewed in the show users command. Kicking the user itself is not supported.

- Show Online User Commands

```
SWITCH#show users
Type        Line    User                        Idle        Host
con         0       admin                       00:00:03    --
vty         0       admin                       00:00:11    192.168.64.1
```

Users display elements are as follows:

Field	illustrate
Type	console or vty
Line	console: fixed 0 vty : 0-7
User	username
Idle	Time in idle state, if the timeout time is exceeded, the terminal automatically exits.
Host	Login user ip address

1.7.2. Examples

Case 1 : The device enables the telnet service. Only users with the IP address 192.168.64.100 are allowed to access the device through telnet, and other users are denied access.

```
SWITCH(config)#telnet-server enable
SWITCH(config)#ip-access-list standard 1
SWITCH(config-std-acl)#permit host 192.168.64.100
SWITCH(config-std-acl)#exit
SWITCH(config)#ip telnet access-class 1
```

Case 2 : The device enables the telnet service, and the device only allows one user to log in to the device through telnet at the same time.

```
SWITCH(config)#telnet-server enable
SWITCH(config)#line vty 1 7
SWITCH(config-line)#transport input none
```

1.8. System Hostname Configuration

- Configuring Hostname

Command	SWITCH(config)# **hostname** WORD
Description	The name must consist of printable characters and the length cannot exceed 63 bytes. This configuration takes effect immediately.

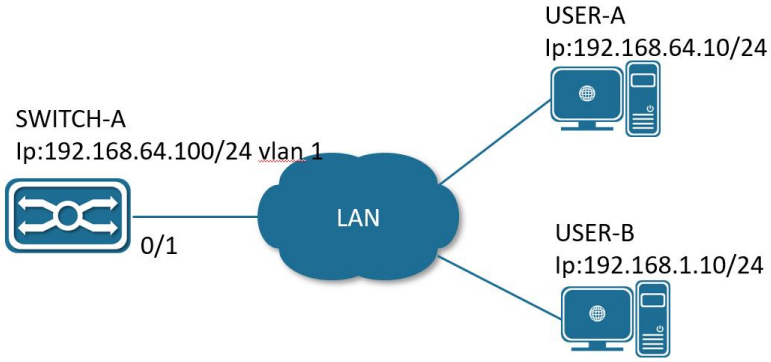
1.9. Firmware Upgrade

- Firmware Upgrade

Command	SWITCH# **upgrade firmware tftp://**SERVER/FILENAME
Description	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, reboot the device to complete the firmware upgrade. Do not power off the device during the upgrade process.

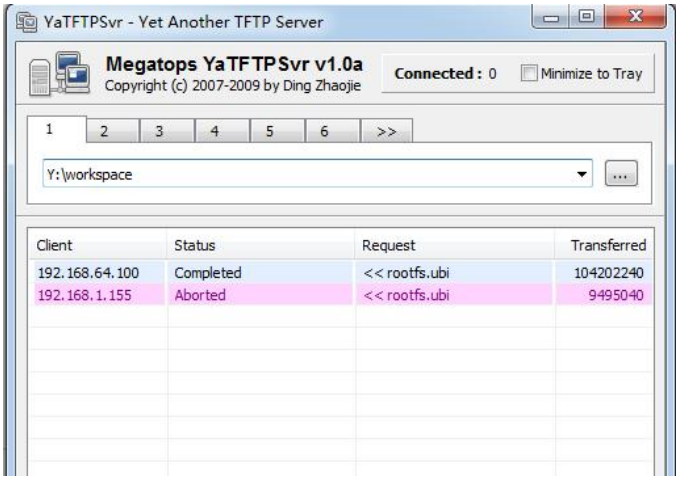
Example 1: The following examples shows firmware upgrade via tftp.

Step 1: As shown in the figure below, SWITCH-A is the device to be upgraded, and the telnet function is enabled; USER-A is the host on the same network segment in the LAN, and USER-B is the management device in the LAN, both of which can log in to SWITCH-A by telnet.



Firmware upgrade connection diagram

Step 2: Select USER-B to perform the version upgrade operation. Open the TFTP server on USER-B and place the upgrade file xcat-release-3.2.0.bin in the Y:/workspace directory.TFTP server as shown in the figure below.



TFTP Server

Step 3: USER-B telnet logs in to SWITCH-A and executes the upgrade command in privileged mode. Upgrade information as shown in the figure below.

```
SWITCH#upgrade firmware tftp://192.168.64.1/lite-release-6.2.0.bin
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 82.1M    0 82.1M    0     0  1091k      0 --:--:--  0:01:17 --:--:-- 1093k
100 82.1M    0 82.1M    0     0  1091k      0 --:--:--  0:01:17 --:--:-- 1091k
Un-packet install file, this will last about 60 seconds.
Read configure from config file.
Validation.
Check upgrade file success.
Start erase and write bin to flash, this will last about 120 seconds.
Erasing 128 Kibyte @ d7e0000 -- 100 % complete
Reboot system to finish upgrade? (y/n):
```

Upgrade Information

Step 4: After the upgrade is over, select "y" to restart the device to complete the upgrade, select "n" to continue running the device, and the upgrade operation will be completed after restart.

1.10. System Data And Time Configuration

- Setting the System Clock

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

Description	Setting the system clock. For example：Clock set 15:30:00 1 october 2017.

- Setting NTP Server

Command	SWITCH(config)# **ntp server {**A.B.C.D | **ipv6** X.X::X.X }
Description	Configure the IP address of the NTP server (domain name configuration is not supported). After the configuration is complete, if the device and the server are connected to the network, the device will automatically synchronize the time information from the server. It takes about 4-8 minutes to complete the time synchronization for the first time.

- Setting Time zone

Command	SWITCH(config)# **clock timezone** ZONE
Description	Configure the system time zone. The default timezone is UTC. Supports standard time zone configuration, such as Shanghai time zone keyword "Shanghai", Hong Kong time zone keyword "Hong_Kong", etc.

- Display System Clock

Command	SWITCH# **show clock**
Description	Display system clock.

- Display NTP Status

Command	SWITCH# **show ntp status**
Description	Display ntp status.

2. Configuring Ethernet Interface

2.1. Overview of Interface Types

The interfaces of switch can be divided into the following two categories: Layer 2 interfaces and Layer 3 interfaces.

L2 interface，Including common physical ports (Switch Port) and aggregate ports (Port Channel).

Switch Port consists of a single physical port on the device and only support Layer 2 switching. The port can be an Access Port, Hybrid Port or a Trunk Port.

Port Channel 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 aggregate port. For Layer 2 switching, the aggregation port can superimpose the bandwidth of multiple ports to expand the link bandwidth.

L3 interface，Here mainly refers to the SVI port.

SVI is a switching virtual interface, a logical interface used to implement Layer 3 switching. SVI can be used as the local management interface, through which the administrator can manage the device. You can create an SVI with the interface vlan interface configuration command, and then assign an IP address to the SVI to establish routing between VLANs.

2.2. Configuring

- Interface Range Mode

Command	SWITCH(config)# **interface** IFNAME_RANGE
Description	Specify the range of interfaces to be configured, and enter interface-range configuration mode. When there are multiple range combinations, separate them with ',' without spaces. For example, the command interface range gigabitEthernet 0/1-4, gigabitEthernet 0/9-12 is a valid range. You can use the interface range command to configure up to five port ranges; Each interface-range must consist of the same port type.

- Adding a Description for an Interface

Command	SWITCH(config-if)# **description** DESC
Description	Add a description (up to 80 characters) for an interface.

- Shutdown the Interface

Command	SWITCH(config-if)# shutdown SWITCH(config-if)# no shutdown
Description	Shut down an interface.

- Configuring Interface Speed

Command	SWITCH(config-if)# **speed** {**10 | 100 | 1000 | auto**} SWITCH(config-if)# **no speed**
Description	Enter auto to enable the interface to autonegotiate speed with the connected device. If you use the 10, 100, or the 1000 keywords with the auto keyword, the port autonegotiates only at the specified speeds;

- Configuring Interface Duplex Mode

Command	SWITCH(config-if)# **duplex** {**auto	full	half**} SWITCH(config-if)# **no duplex**
Description	Enable half-duplex mode (for interfaces operating only at 10 or 100 Mbps). You cannot configure half-duplex mode for interfaces operating at 1000 Mbps

Attention:

✦ When both speed and duplex exit auto mode, port auto-negotiation is disabled.

- Configuring Interface Flowcontrol

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

Command	SWITCH(config-if)# **flowcontrol** {**on	off** }
Description	Configure the flow control mode for the port. on: The port cannot send pause frames but can operate with an attached device that is required to or can send pause frames; the port can receive pause frames. off: Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner, and no pause frames are sent or received by either device.

- Configuring Interface MTU

When a port performs high-throughput data exchange, it may encounter a frame larger than the Ethernet standard frame length, which is called a jumbo frame.

The user can control the maximum frame length that the port is allowed to send and receive by setting the MTU of the port.

Frames received or forwarded by the port, if the length exceeds the set MTU, will be discarded.

Due to chip limitations, the MTU value only supports even numbers. If the user configures an odd number, the device will auto-align to even. For example, if the MTU is configured as 127, it actually works as 128.

Command	SWITCH(config-if)# **mtu** LENGTH SWITCH(config-if)# **no mtu**
Description	Change the MTU size for the interface on the switch. The range is 46 to 10222 bytes; the default is 1500 bytes.

- Configuring SFP Interface Mode

Command	SWITCH(config-if)# **port mode** {**sgmii	2500BASE-X	1000BASE-X	10G}** SWITCH(config-if)# **no port mode**
Description	1000BASE-X:The port operate at 1000Mbps, full-duplex only. Sgmii: Enables connection to external copper transceivers. 2500BASE-X: The port operate at 2.5G, full-duplex only. 10G: The port operate at 2.5G, full-duplex only.

- Configuring Interface Medium Type

If a port can be configured both fiber and copper medium types, you can only use one of them. Once the medium type is determined, configure the properties of the port, such as duplex, flow control, and rate, which all refer to the properties of the currently selected type of port.

Command	SWITCH(config-if)# **medium {copper	fiber	auto [prefer (copper | fiber)]}**

	SWITCH(config-if)# **no medium**
Description	Configuring interface medium type. Default is auto mode，prefer copper. Copper：Indicates the choice of copper medium type. Fiber：Indicates the choice of fiber medium type. Auto：Indicates the adaptive port media type，Determine whether it is an copper or fiber port based on the access medium, prefer copper. Auto prefer copper： Indicates the adaptive port media type， When both fiber and copper are connected, prefer the copper port. Auto prefer fiber：Indicates the adaptive port media type，When both fiber and copper are connected, prefer the fiber port. No operation restores the media type to copper.

- Configuring Interface Isolate

In some situations, you need to prevent Layer 2 (L2) connectivity between end devices on a switch, you can use the isolate function.

When some ports are set as isolated ports, 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.

Command	SWITCH(config-if)#**switchport isolate** SWITCH(config-if)# **no switchport isolate**
Description	Setting the port as an isolated port.

- Configuring Interface Auto negotiation

Command	SWITCH(config-if)# autoneg on SWITCH(config-if)# no autoneg
Description	Configure port auto-negotiation on and off. Only applicable to 1000M optical port, If this command is configured on other ports, it prompts failure. Default is on. By show interface brief command, You can view the auto-negotiation status of the link up ports.

2.3. Examples

- Enter gigabitEthernet0/1 Interface Configuration Mode：

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#
```

- Configure the Port Description Information as "TEST_A"

```
SWITCH(config-if)#description TEST_A
```

- No Shutdown Port

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

- Setting the Port Speed 100M, Duplex Full, and Flowcontrol On

```
SWITCH(config-if)#speed 100
SWITCH(config-if)#duplex full
```

```
SWITCH(config-if)#flowcontrol on
```

- Setting the Port MTU value 1024

```
SWITCH(config-if)#mtu 1024
```

2.4. Display Information

- Display Brief Information of All Ports

```
SWITCH#show interface brief

--------------------------------------------------------------------------------
Ethernet   Type  Status  Reason  Speed  Duplex  Flowcontrol  Autoneg  Port
Interface                                                              Ch #
--------------------------------------------------------------------------------
GiE0/1     ETH   down    none    --     --      --           --       --
GiE0/2     ETH   up      none    1000M  FULL    OFF          ON       --
GiE0/3     ETH   down    none    --     --      --           --       --
GiE0/4     ETH   down    none    --     --      --           --       --
GiE0/5     ETH   down    none    --     --      --           --       --
GiE0/6     ETH   down    none    --     --      --           --       --
GiE0/7     ETH   down    none    --     --      --           --       --
GiE0/8     ETH   up      none    100M   FULL    OFF          ON       --
GiE0/9     ETH   down    none    --     --      --           --       --
GiE0/10    ETH   down    none    --     --      --           --       --
GiE0/11    ETH   down    none    --     --      --           --       --
GiE0/12    ETH   down    none    --     --      --           --       --
```

- Display Single Port Configuration and Status

```
 SWITCH#show interface gigabitethernet0/1
Interface gigabitethernet0/1
  Hardware is eth  current hw addr: 0050.4c82.89a0
  Physical:0050.4c82.89a0
  Description: test_a
  Index 1 metric 0 mtu 1024 speed-unknown duplex-unknown flowcontrol-unknown
  Port mode is invalid
  <up>
    vrf binding: not bound
  Bandwidth -8
  Input packets 0677, bytes 072690,
  Multicast packets 0327 broadcast packets 0350 fcs error 00 undersizeerrors 00
oversizeerrors 00
  Output packets 00, bytes 00,
  Multicast packets 00 broadcast packets 00
```

- Display Port Packet Statistics

```
SWITCH#show interface gigabitEthernet0/1 counters
Interface gigabitEthernet16/1
Good Octets Tx          : 1914949
Good Octets Rx          : 0
Bad Octets Rx           : 0
Mac Tx Err Pkts         : 0
Good Packets Tx         : 1913
Good Packets Rx         : 0
Bad Packets Rx          : 0
```

```
Broadcast Packet Tx     : 24
Broadcast Packets Rx    : 0
Multicast Packet Tx     : 55
Multicast Packets Rx    : 0
pkts_64_octets          : 285
pkts_65_127_octets      : 263
pkts_128_255_octets     : 42
pkts_256_511_octets     : 36
pkts_512_1023_octets    : 91
pkts_1024_max_octets    : 1196
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

```
SWITCH#show switchport isolate
interface      config
GiE0/1          isolated
GiE0/2          normal
GiE0/3          normal
GiE0/4          normal
GiE0/5          normal
GiE0/6          normal
GiE0/7          normal
GiE0/8          normal
GiE0/9          normal
GiE0/10         normal
```

3. Configuring Storm Control

3.1. Overview of Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.。

Storm control uses bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic, to measure traffic activity.

because of hardware limitations and the way in which packets of different sizes are counted, threshold percentages are approximations.

3.2. Configuring

- Configuring Storm Control

Command	SWITCH(config-if)#**storm-control** {**broadcast | multicast | unicast | all | unicast-broadcast | multicast-broadcast**} **level** LINE SWITCH(config-if)#**no storm-control**
Description	Configure broadcast, multicast, or unicast storm control. By default, storm control is disabled. If you set the threshold to the maximum value (100 percent), no limit is placed on the traffic. If you set the threshold to 0.0, traffic on that port is blocked. The range is 0.00 to 100.00. Support adaptive port rate change. Unicast only containing unknown unicast packets.

3.3. Examples

Example 1： Configure the unknown multicast storm control on port gigabitEthernet0/1 to 10% of the total bandwidth.

Step 1: Specify the interface gigabitEthernet0/1 to be configured, and enter interface configuration mode.

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#
```

Step 2: Configure the unknown multicast storm control on port gigabitEthernet0/1 to 10%.

```
SWITCH(config-if)#storm-control multicast level 10
```

3.4. Display information

- Display All Port Storm Control Configurations

```
SWITCH#show storm-control
Port        BcastLevel     McastLevel     Unicastlevel
GiE0/1      100.00%          10.00%       100.00%
GiE0/2      100.00%        100.00%        100.00%
GiE0/3      100.00%        100.00%        100.00%
GiE0/4      100.00%        100.00%        100.00%
GiE0/5      100.00%        100.00%        100.00%
GiE0/6      100.00%        100.00%        100.00%
```

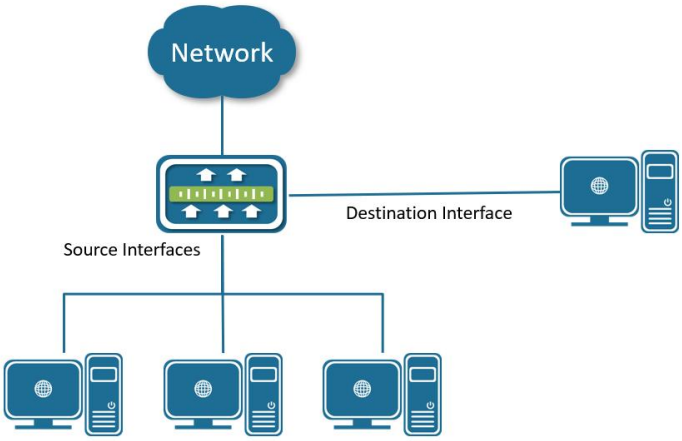
GiE0/7	100.00%	100.00%	100.00%
GiE0/8	100.00%	100.00%	100.00%
GiE0/9	100.00%	100.00%	100.00%
GiE0/10	100.00%	100.00%	100.00%
GiE0/11	100.00%	100.00%	100.00%
GiE0/12	100.00%	100.00%	100.00%

4. Configuring SPAN

4.1. Overview of SPAN

You can analyze network traffic passing through ports by using SPAN（Local Switched Port Analyzer）to send a copy of the traffic to another port on the switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies traffic received or sent (or both) on source ports to a destination port for analysis.

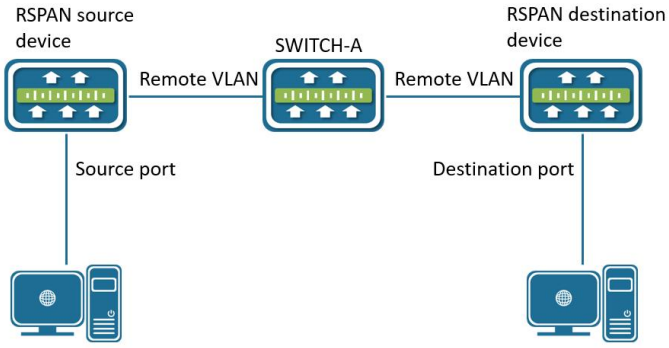
SPAN does not affect the switching of network traffic on the source ports. You must dedicate the destination port for SPAN use.



Example of SPAN configuration

SPAN supports a session entirely within one switch. all source ports and destination ports are in the same switch.

RSPAN (Remote Switch Port Analyzer, remote port mirroring) is an extension of SPAN . The remote mirroring source port and destination port can span multiple network devices. The principle of remote mirroring is that the source device, intermediate device and destination device create a Remote VLAN, and all ports participating in the session must be added to the Remote VLAN. The mirrored message is broadcast in the Remote VLAN, so that the mirrored message is transmitted from the source port of the source device to the destination port of the destination device.



Example of RSPAN configuration

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

4.2. Configuring

- Creating a Session

Command	SWITCH(config)#**monitor session** SESSION-ID SWITCH(config)#**no monitor session** SESSION-ID
Description	Create a SPAN session, create a session and enter session mode at the same time For session-id, the range is 1 to 7

- Configuring Session Description

Command	SWITCH(config-monitor)#**description** DESC
Description	Configure the session descriptor , which supports a maximum of 32 characters.

- Configuring Session Mode

Command	SWITCH(config-monitor)# **remote {source | destination}** SWITCH(config-monitor)# no **remote**
Description	Configuring Session Mode The default is local mirror Source: source device of remote mirroring Destination : destination device of the remote mirroring

Illustrate

✦ Changing the session mode will cause the source and destination configurations to be deleted

- Configuring SPAN/RSPAN Source Interfaces

Command	SWITCH(config-monitor)#**source interface** IFNAME {**both | rx | tx**} SWITCH(config-monitor)#**no source interface** IFNAME {**both | rx | tx**}
Description	Create/delete source interfaces Both: monitors the ingress and egress directions of the interface Rx: monitors the ingress direction of the interface Tx: monitors the egress direction of the interface

- Configuring SPAN/RSPAN Source VLAN

Command	SWITCH(config-monitor)# **source vlan <1-4094> rx** SWITCH(config-monitor)# **no source vlan <1-4094>**
Description	Create/delete source VLAN Vlan supports range mode, for example: source vlan 20-25 rx Supports monitoring of up to 8 source VLANs

Illustrate

✦ The source VLAN can be configured in at most one session.

✦ The source VLAN and source interface cannot coexist, whether in the same session or across different sessions.

- Configuring the SPAN Destination Interface

Command	SWITCH(config-monitor)# **destination interface** IFNAME { | **switch** }

	SWITCH(config-monitor)# **no destination interface** IFNAME
Description	Create/delete SPAN destination interface Switch: destination interface participates in forwarding

- Configuring the RSPAN Destination Interface

Command	SWITCH(config-monitor)# **destination interface** IFNAME **remote-vlan** <1-4094> { | **switch** } SWITCH(config-monitor)# **no destination interface** IFNAME
Description	Create/delete RSPAN destination interface Switch: destination interface participates in forwarding When the session type is remote-destination, switch is a required option.

Illustrate

- ✦ Only one RSPAN can be configured on a device.
- ✦ It is not recommended to add common interfaces to the Remote VLAN.
- ✦ The remote VLAN cannot be within the range of the source VLAN.

4.3. Examples

Case 1

SPAN based on interface mirroring : This example Use interface gigabitEthernet0/8 to monitor the ingress packets of gigabitEthernet0/1 and the ingress/egress packets of gigabitEthernet0/2. Set the monitoring session name to "TRAFFIC_MONITOR".

Step 1: Create session.

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#monitor session 1
SWITCH(config-monitor)#
```

Step 2: Configuring session description.

```
SWITCH(config-monitor)#description TRAFFIC_MONITOR
```

Step 3: Configuring session source interfaces.

```
SWITCH(config-monitor)#source interface gigabitEthernet0/1 rx
SWITCH(config-monitor)#source interface gigabitEthernet0/2 both
```

Step 4: Configuring session destination interface.

```
SWITCH(config-monitor)#destination interface gigabitEthernet0/8
```

Case 2

SPAN based on VLAN mirroring : Use interface gigabitEthernet0/8 to monitor the ingress packets of VLAN 1 , and set the monitoring session name to "TRAFFIC_MONITOR_VLAN ".

- Enter global mode and establish a session:

```
SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH(config)#monitor session 1
SWITCH(config-monitor)#
```

- Configure the session description to "TRAFFIC_MONITOR _VLAN "

```
SWITCH(config-monitor)#description TRAFFIC_MONITOR_VLAN
```

- Configuring the session source interface

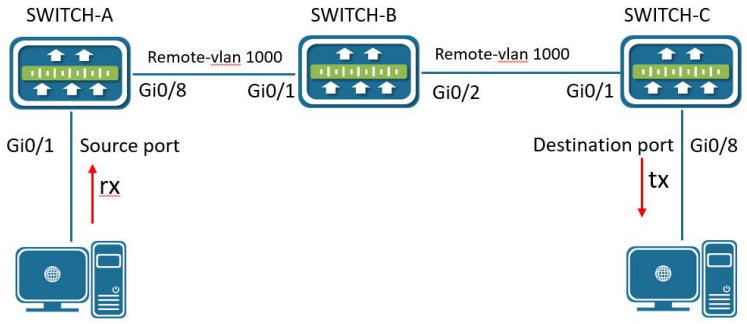
```
SWITCH(config-monitor)#source vlan 1 rx
```

- Configure the session destination interface

```
SWITCH(config-monitor)#destination interface gigabitEthernet0/8
```

Case 3

RSPAN mirroring : Use the interface gigabitEthernet0/8 of the remote device SWITCH-C to monitor the rx packets of the ineterface gigabitEthernet0/1 of the local device SWITCH-A . The remote-vlan is 1000, and the intermediate device supports the packets broadcast of VLAN1000 .



Configure SWITCH-A:

- Enter global mode and establish a session:

```
SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH(config)#monitor session 1
SWITCH(config-monitor)#
```

- Configure the session description to "TRAFFIC_MONITOR _SOURCE "

```
SWITCH(config-monitor)#description TRAFFIC_MONITOR _SOURCE
```

- Configuring session mode

```
SWITCH(config-monitor)#remote source
```

- Configuring the session source interface

```
SWITCH(config-monitor)#source interface gigabitEthernet0/1 rx
```

- Configure the session destination interface

```
SWITCH(config-monitor)#destination interface gigabitEthernet0/8 remote-vlan
1000
```

Configure SWITCH-B:

- Create VLAN 1000

```
SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH(config)# vlan 1000
```

- The interface is configured as a trunk port.

```
SWITCH(config)# interface gigabitEthernet0/1-2
SWITCH(config-if)#switchport mode trunk
```

Configure SWITCH-C:

- Create VLAN 1000

```
SWITCH#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH(config)# vlan 1000
```

- Enter global mode and establish a session:

```
SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH(config)#monitor session 1
SWITCH(config-monitor)#
```

- Configure the session description to "TRAFFIC_MONITOR _DESTINATION "

```
SWITCH(config-monitor)#description TRAFFIC_MONITOR_DESTINATION
```

- Configure session mode

```
SWITCH(config-monitor)# remote destination
```

- Configure the session destination interface

```
SWITCH(config-monitor)#destination interface gigabitEthernet0/8 remote-vlan
1000 switch
SWITCH(config-monitor)#exit
```

- Configure the VLAN of the destination interface

```
SWITCH(config)#interface gigabitEthernet 0/8
SWITCH(config-if)#switchport access vlan 1000
```

4.4. Display Information

- Display Session of SPAN

```
SWITCH#show  monitor session 1
session 1
-------------------------------------------------
description       : TRAFFIC_MONITOR
type              : span
source intf       :
    tx only       :
    rx only       : gigabitEthernet0/1
    both          : gigabitEthernet0/2

source VLANs
    rx only       :

destination intf  : gigabitEthernet0/8
    switch        : false
```

- Display Session of RSPAN

```
SWITCH#show  monitor session 1
session 1
-------------------------------------------------
description       : TRAFFIC_MONITOR_SOURCE
type              : remote-source

source intf
    tx only       :
    rx only       : gigabitEthernet0/1
    both          :
```

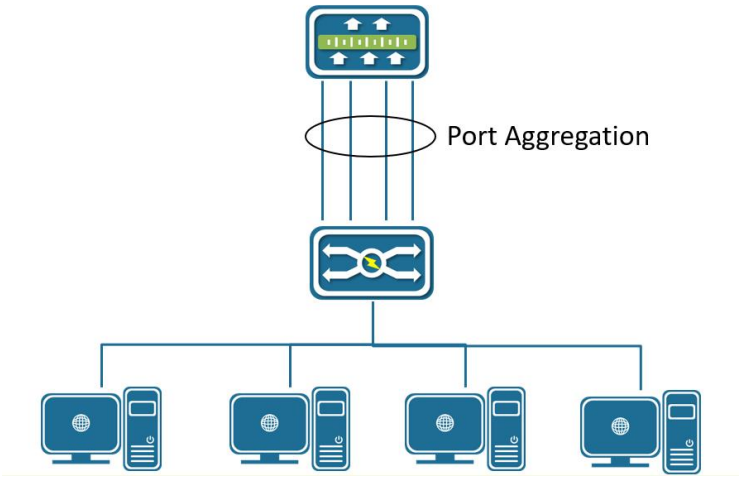
```
        source VLANs      :
            rx only       :
        destination intf  : gigabitEthernet0/8
            remote vlan   : 1000
            switch        : false
```

5. Configuring Port Aggregation

5.1. Overview of Port Aggregation

Port aggregation provides fault-tolerant high-speed links between switches, routers, and servers. You can use it to increase the bandwidth between the wiring closets and the data center, and you can deploy it anywhere in the network where bottlenecks are likely to occur. Port aggregation provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, port aggregation redirects traffic from the failed link to the remaining links in the channel without intervention.

Port aggregation consists of individual Fast Ethernet or Gigabit Ethernet links bundled into a single logical link called channel, as shown in Figure below.



Typical Port Aggregation application

Each Channel can consist of up to eight compatibly configured Ethernet ports. All ports in each Channel must be configured as Layer 2 ports. The number of Channels is limited to 12.

You can configure an Channel in one of these modes: Manual(Static), Active(LACP), or Passive(LACP).

5.2. Overview of LACP

LACP (Link Aggregation Control Protocol) based on the IEEE802.3ad standard is a dynamic link aggregation protocol. If a port enables the LACP, the port will send LACPDU message to announce its system priority, system MAC, port priority, port number and operation key, etc. After the connected device receives the LACP message from the peer end, it compares the system priorities of the two ends according to the system ID in the message. On the side with the higher system ID priority, the ports in the aggregation group are set to be in the aggregation state according to the order of port ID priority from high to low, and the updated LACP message is sent out. It will also set the corresponding port to the aggregation state, so that the two sides can reach the same agreement when the port exits or joins the aggregation group.

After the LACP member interface link is bound, periodic LACP packet exchange will be carried out. When no LACP packet is received for a period of time, it is considered that the packet reception timed out, the member interface link is unbound, and the port is in a state of non-forwarding again. There are two modes of timeout here: long timeout mode and short timeout mode. In the long timeout mode, the port sends a packet every 30 seconds. If it does not receive a packet from the peer for 90 seconds, it will be in a packet receiving timeout.； In the short timeout mode, the port sends a packet every 1

second. If it does not receive a packet from the peer for 3 seconds, it is in the packet receiving timeout.

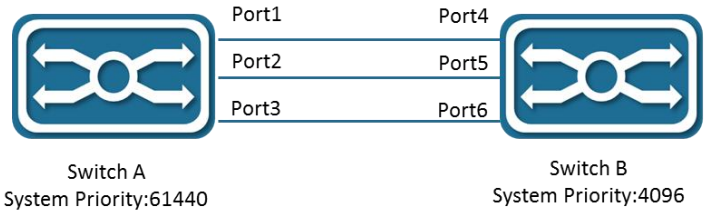


Figure Typical LACP application

As shown Figure, switch A and switch B are connected together through 3 ports. We set the system priority of switch A to 61440, and set the system priority of switch B to 4096. Enable LACP link aggregation on the three directly connected ports of switches A and B.

After receiving the LACP message from the peer, switch B finds that its system ID has a higher priority (switch B has a higher system priority than switch A), so it follows the order of port ID priority (in the case of the same port priority) , in the order of port numbers from small to large) set ports 4, 5, and 6 to be in the aggregation state.

After switch A receives the updated LACP packet from switch B, it finds that the system ID of the peer end has a higher priority, and set the ports 1, 2, and 3 to the aggregation state.

5.3. Configuring

- Configuring Layer 2 Channels

Command	SWITCH(config-if)#**channel-group** ID **mode manual** SWITCH(config-if)#**channel-group** ID **mode** {**active** | **passive**} SWITCH(config-if)#**no channel-group**
Description	Assign the port to a channel group, and specify the mode. For ID, the range is 1 to 12.

Note

✦ When the first port is added to the aggregation port, a PO port is actively created, and the default attribute of the PO port is the first port attribute.

✦ For Layer 2 Channels:

Ports with different native VLANs cannot form an EtherChannel.

- Configuring LACP System Priority

Command	SWITCH(config)#**lacp system-priority** SYSTEM-PRIORITY SWITCH(config)#**no lacp system-priority**
Description	The system priority range is 1 to 65535, the default value 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.

- Configuring LACP Interface Priority

Command	SWITCH(config-if)#**lacp port-priority** PORT-PRIORITY SWITCH(config-if)#**no lacp port-priority**
Description	The interface priority range is 1 to 65535, the default value is 32768.

- Configuring LACP Timeout Mode

Command	SWITCH(config-if)#**lacp timeout {long | short}** SWITCH(config-if)#**no lacp timeout**
Description	In long mode, the interval for sending LACP protocol packets is 30S, and the timeout is 90S. In short mode, the interval for sending LACP protocol packets is 1S, and the timeout is 3S. Default is in long mode.

- Configuring Load-balance Method

Command	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**} SWITCH(config)#**no port-channel load-balance**
Description	Configure an Channel load-balancing method. The default is src-mac. Select one of these load-distribution methods: • dst-ip: Load distribution is based on the destination IP address. dst-mac: Load distribution is based on the destination MAC address of the incoming packet. Dist-port: Load distribution is based on the destination L4-port of the incoming packet src-dst-ip: Load distribution is based on the source-and-destination IP address. src-dst-mac: Load distribution is based on the source-and-destination MAC address. src-dst-port: Load distribution is based on the source-and-destination L4-port of the incoming packet. src-ip: Load distribution is based on the source IP address. src-mac: Load distribution is based on the source-MAC address of the incoming packet.

5.4. Examples

Example 1: This example shows how to assign the ports to a channel, and set load-balance method.

- Assign the gigabitEthernet0/5, gigabitEthernet0/6 to PO 1, set load-balance 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
```

5.5. Display information

- Display Channels Configuration and Status

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

Interface po3
  Type: static
  Member:
    gigabitEthernet0/18     link down     Disable

Interface po8
  Type: LACP
  Member:
    gigabitEthernet0/19     link up       Enable
    gigabitEthernet0/17     link up       Enable
```

```
SWITCH#show port-channel 8
Interface po8
  Type: LACP
  Member:
    gigabitEthernet0/19     link up       Enable
    gigabitEthernet0/17     link up       Enable

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

- Display LACP Summary

```
SWITCH#show lacp summary
% Aggregator po8 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

SWITCH#show lacp detail
% Aggregator po8 1008
% Aggregator Type: Layer2
%  Mac address: 74:b9:eb:ee:25:46
%  Admin Key: 0008 - Oper Key 0008
%  Actor LAG ID- 0x8000,74-b9-eb-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

SWITCH#show lacp 8
% Aggregator po8 1008 Admin Key: 0008 - Oper Key 0008
% Partner LAG ID: 0x8000,00-01-a0-00-10-10,0x0032
% Partner Oper Key 0050

SWITCH#show lacp sys-id
% System 8000,74-b9-eb-ee-25-46

SWITCH#show lacp port gigabitEthernet0/19
% LACP link info: gigabitEthernet0/19 - 19
% LAG ID: 0x8000,74-b9-eb-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: 0x0000-00:00:00:00:0000
% 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
```

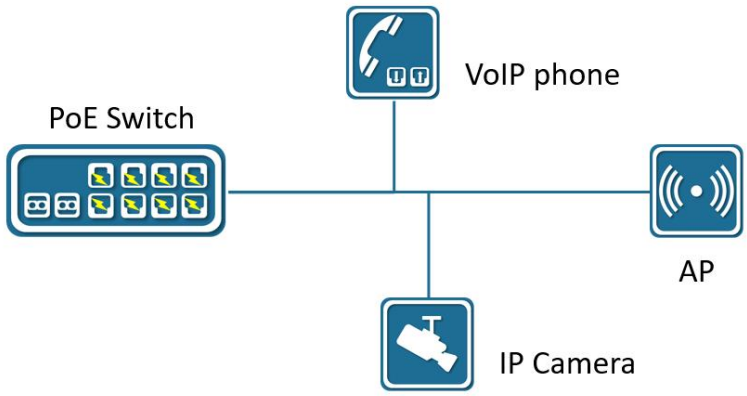
- Display Only One Channel Information

```
        SWITCH#show int po8
        Interface po8
          Hardware is AGG  Current HW addr: 74b9.ebee.2546
          Logical:(not set)
          Port Mode is access
          interface configure:
            medium-fiber mtu 1526 speed-auto duplex-auto flowcontrol-off autonego-
off
          interface status:
            link-up bandwidth-2g
          Aggregate Members:(LACP)
            gigabitEthernet0/19     link up       Enable
            gigabitEthernet0/17     link up       Enable
          input packets:
            Good Octets Rx          : 18986
            Good Packets Rx         : 104
            Broadcast Packets Rx    : 0
            Multicast Packets Rx    : 104
          ouput packets:
            Good Octets Tx          : 38529
            Good Packets Tx         : 359
            Broadcast Packet Tx     : 4
            Multicast Packet Tx     : 355
          un-normal packets:
            Drop Events             : 0
            Undersized Pkts Recvd   : 0
            Oversized Pkts Recvd    : 0
           Bad CRC                 : 0
```

6. Configuring PoE

6.1. Overview of PoE

Power over Ethernet (PoE) is a technology that transmits both electrical power and network data over an ethernet cable. With PoE, each Ethernet interface of LAN switches can supply power to devices like VoIP phones, IP cameras or security cameras, and wireless access points (AP), As shown in the figure below.



PoE powersupply diagram

The PoE device like LAN switches that are supplying power is called Power Sourcing Equipment (PSE). The power that is supplying is in Direct Current (DC) form.

PoE (Power over Ethernet) Standards:

PoE : IEEE 802.3af standard that supplies up to 15 watts of DC power from PSE and 12.95 watts from PD due to losses on an ethernet cable. It uses two pairs of wires like CAT3 or CAT5 cables as a medium.

PoE+: IEEE 802.3at standard that supplies power up to 30 watts of DC power from PSE and 25.5 watts from PD due to losses on an ethernet cable. It is also using two pairs of wires like CAT5 or higher as a medium.

UPoE(Universal PoE): IEEE 802.3bt standard that supplies power up to 60 watts of DC power from PSE and 51 watts from PD due to losses on an ethernet cable. It uses four pairs of wire as a medium.

UPoE+(Universal PoE +): IEEE 802.3bt standard that supplies power up to 100 watts of DC power from PSE and 71.3 watts from PD due to losses on an ethernet cable. It is also using four pairs of ethernet cabling as a medium.

6.2. Configuring

6.2.1. Enabling Port Powersupply

Command	SWITCH (config-if)#**poe enable** SWITCH (config-if)#**no poe enable**
Description	Default port power supply enabled.

6.2.2. Configuring Port Priority

Users can configure the interface power supply priority of the PoE switch. The priority from high to low is: high, meidum, and low. When the overall power of the PoE switch is insufficient, the ports with lower

priority will be powered off first.

The port priorities of the same priority are arranged in the order of port numbers, and the priority of ports with smaller port numbers is higher. For example, the priority of port gi0/1 is higher than that of port gi0/2. Ports with the same priority and newly inserted ports will not affect the power supply of PDs that are already powered. Ports with different priorities are not affected by this feature, and ports with high priority can preempt ports with low priority.

Command	SWITCH (config-if)#**poe priority (low | medium | high)** SWITCH (config-if)#**no poe priority**
Description	Set port power supply priority. The port default priority is low.

6.2.3. Configuring Port PD Description

Command	SWITCH (config-if)#**poe pd-description** DESC SWITCH (config-if)#**no poe pd-description**
Description	Configure the PD description of the interface. The parameter is a string, up to 32 characters supported.

6.2.4. Configuring Port Max Power

Users can limit the maximum output power of the port by configuring the maximum power of the port. When the power supplied of the port exceeds the maximum power value, the port will be powered off and the port state turn to be abnormal.

Command	SWITCH (config-if)#**poe max-power** VALUE SWITCH (config-if)#**no poe max-power**
Description	Set the maximum power of the port in watts. For AF/AT ports, the maximum port power range is 1-30. For BT ports, the maximum port power range is 1-90.

6.2.5. Enabling Port Legacy

Command	SWITCH (config-if))#**poe legacy** SWITCH (config-if))#**no poe legacy**
Description	Configuring a port to enable and disable compatibility mode. Using this command on a port that is not connected to a PD device may cause the peer device to be powered on and burned by mistake. Please ensure that the port is connected to a PD device when using this command.

6.2.6. Configuring Port Pd-detect Mode

The pd-detect function is to solve the situation that the PD load equipment receives power normally, but the actual work is abnormal. When an abnormal PD load is detected, the port stops external power supply, and the load is powered on again in about 10 seconds. There are two ways of pd-detect

By-flow: Port flow detection. For power supply ports, if there is no data interaction for a long time, the load status is considered abnormal. Specific time user configurable.

By-ping: The device actively sends a ping request. If the load responds normally, the status is considered normal. If there is no response for many times, the load status is considered abnormal.

Command	SWITCH (config)#**poe pd-detect mode** (**by-flow | by-ping** IPADDR) SWITCH (config))#**no poe pd-detect mode**

Description	Configure to enable and disable the port pd-detect function, and configure the detection mode. By-flow: flow-based load detection. By-ping: load detection based on ping requests. IPADD: In by-ping mode, the IP address of the PD load.

- Configuring Port Pd-detect Parameters

After the pd-detect function is enabled on the port, it will detect immediately. Therefore, if the detection interval is configured as 60 seconds and the number of detections is 5 times, the fifth detection will be completed in about 240 seconds.

Command	SWITCH (config)#**poe pd-detect parameter interval** VALUE **times** VALUE SWITCH (config))#**no poe pd-detect parameter**
Description	Configuring Port PD Self-Detection Parameters. Interval VALUE: detection interval, range 5-60 seconds, default 60 seconds. Times VALUE: detection times, range 3-30 times, default 5 times.

6.2.7. Enabling Port Force On

For some load devices, the power supply is unstable. The forced power supply mode of the port can be configured to maintain the stable power supply of the port to the load.

To configure the port to force power supply, you need to disable the port power supply enablement first.

Command	SWITCH (config-if)#**poe force on** SWITCH (config-if)#**no poe force on**
Description	Configure Port Forced Power Supply. The default port force power supply is closed.

6.2.8. Configuring the External Powersupply

Command	SWITCH(config)#**poe powersupply** POWER SWITCH(config)#**no poe powersupply**
Description	The default power calculation method: the product of the number of PoE power supply ports and the single port 15.4W. POWER: range 0-999.9, unit W. If the configured power is less than the current device power consumption, power off the PD device on the port with the lower priority, and the port priority is a higher priority with a smaller port ID.

6.2.9. Configuring Reserved Power

Considering that the power consumption of the PD device fluctuates, there is a risk of damage to the device due to the overload of the PoE switch. The switch provides a command to set the reserved power of the PoE system to protect the PoE switch from having power "rich" all the time, and avoid this phenomenon from happening.

Command	SWITCH (config)#**poe power-reserved VALUE** SWITCH (config))#**no poe power-reserved**
Description	Set the percentage of reserved power to the total system power, ranging from 0% to 50%. The system's reserved power defaults to 0%.

6.2.10. Configuring Power Alarm Level

When the system power consumption is greater than the alarm waterline power, the system outputs

alarm log.

Command	SWITCH (config)#**poe power-alarm VALUE** SWITCH (config))#**no poe power-alarm**
Description	Configure the power alarm threshold of the system, the range is 50-99, the unit is percentage, the default is off, not supported.

6.3. Examples

6.3.1. Case For Port Pd-detect

Port gi0/1 is connected to the camera load. If the port does not capture packet traffic within 5 minutes, it is considered that the camera load is working abnormally, and the camera needs to be restarted to return to normal.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#poe enable
SWITCH(config-if)#poe pd-detect mode by-flow
SWITCH(config-if)#poe pd-detect parameter interval 60 times 6
```

6.3.2. Case For Port Force On

Port gi0/1 is connected to the AP load, and the port is powered off at irregular intervals, and then powered on again.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no poe enable
SWITCH(config-if)#poe force on
```

6.3.3. Case For Port Priority

The system power is insufficient. It is necessary to ensure that the loads of ports gi0/1 and gi0/2 are powered on every time the device is powered off and restarted.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#poe priority high
SWITCH(config-if)#exit
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#poe priority high
```

6.4. Display Information

6.4.1. Display Power Supply Information

```
SWITCH#show poe powersupply
  Power supply                : 123.2W
  Power reserved              :  0%
  Power available:            : 123.2W
  Power consume            : 44.1W
  Power management     : energy-saving
  Disconnect mode         : DC
  Powered ports              : 2
  Power alarm:               : --
```

The meaning of the displayed information:

Power supply	The total power of the power supply, in W, with one decimal place reserved.
Power reserved	System reserve power percentage.
Power available	The available power of the system, in W, with one decimal place reserved.
Power consume	The actual power consumption of the system, in W, with one decimal place reserved.
Power management	Power management mode, currently only supports energy-saving mode.
Disconnect mode	Disconnection detection mode, currently only supports DC detection.
Powered ports	Number of power-on ports.
Power alarm	System alarm power percentage.

6.4.2. Display All Port Information

```
SWITCH#show poe interfaces
Interface   enable  status  reason      class  icut(mA) power(W)
-------------------------------------------------------------------
GiE0/1      YES     OFF     short       4      --       --
GiE0/2      YES     OFF     --          -      --       --
GiE0/3      YES     OFF     --          -      --       --
GiE0/4      YES     OFF     --          -      --       --
GiE0/5      YES     OFF     --          -      --       --
GiE0/6      YES     ON      --          4      270.2    14.0
GiE0/7      YES     OFF     --          -      --       --
GiE0/8      YES     OFF     --          -      --       --
```

The meaning of the displayed information:

Interface	Port name, abbreviated.
Enable	Whether the port enables external power supply, YES or NO.
Status	Port power supply status, ON or OFF.
Reason	The reason why the port is not powered on normally: Power management: Insufficient power. unknown：unknown hardware problem.
Class	PD classification registration.
Icut	Current value, unit mA, keep one decimal place.
Power	Power value, unit W, keep one decimal place.

6.4.3. Display Single Port Information

```
SWITCH#show poe interface gigabitEthernet0/1
  Description            :  --
  Enabled                :  YES
  Status                 :  ON
  Reason:                :  --
  Class                  :  4
  Icut                   :  260.5
  Power                  :  14.2
  Max-power              :  --
  Priority               :  low
  Legacy:                :  Disabled
  Pd-detect mode         :  --
  Pd-detect interval     :  60
  Pd-detect times        :  5
```

The meaning of the displayed information

Description	POE port descriptor information.
Enabled	Whether the port enables external power supply, YES or NO.
Status	Port power supply status, ON or OFF.
Reason	The reason why the port is not powered on normally: Power management: Insufficient power. unknown：unknown hardware problem.
Class	PD classification registration.
Icut	Current value, unit mA, keep one decimal place.
Power	Power value, unit W, keep one decimal place.
Max-power	Port maximum power supply, unit W.
Priority	Port power supply priority, Low, Medium, High.
Legacy	Whether to enable non-standard detection, Enabled, Disabled.
Pd-detect mode	PD self-detection mode, By-flow, By-ping, --. For example: By-ping (192.168.3.4).
Pd-detect interval	PD detection interval.
Pd-detect times	PD detection times.

7. Log Management

7.1. Log Management Overview

During the operation of the device, various status changes will occur, such as link status UP, DOWN, etc., and some events such as processing exceptions will also be encountered.

The syslog provides a series of services. When the status changes or an event occurs, fixed-format messages will be automatically generated, and these messages will be recorded on the device log file. It can be displayed on the console port and remote login terminal, and can also be sent to 1-3 groups of log servers on the network for administrators to analyze network conditions and locate problems.

In order to facilitate administrators to read and manage log messages, these log messages can be classified according to the priority of the log information.

7.2. Configuring

7.2.1. Configure Console Log Level

Command	SWITCH(config)# **logging console** {| <0-7>} SWITCH(config)# **no logging console**
Description	Configure console log output level Default level is 6 When executing the no command, the log will not be output on the console. Execute logging console, no level parameters, configured as default level 6

7.2.2. Configure Terminal Log Level

- Configure Terminal Log Level

Command	SWITCH(config) **#logging monitor** {| < 0-7>} SWITCH(config)# **no logging monitor**
Description	Configure terminal log output level Default level is 6 When executing the no command, the log will not be output Execute logging monitor, no level parameters, configured to the default level 6

- Enable Terminal Output Log

Command	SWITCH# **terminal monitor** SWITCH# **terminal no monitor**
Description	Enable log output on the terminal By default, the terminal does not output log When executing the no command, the terminal does not output log

7.2.3. Configure Remote Server

- Configure Remote Server

Command	SWITCH(config)# **logging server {| second	third} {**A.B.C.D **| ipv6** XX::XX } **udp-port** <1-65535> SWITCH(config)# **no logging server {| second	third}**

Description	Configure remote server Supports up to 3 remote server configurations Support remote server UDP protocol port configuration, range <1-65535> When no UDP protocol port parameters are configured, the default port number is 514

- Configure the Log Level Sent to the Remote Server

Command	SWITCH(config) **#logging trap** {**|** < 0-7>} SWITCH(config)# **no logging trap**
Description	Configure the level of logs sent to the server Default level is 6 When executing the no command, no logs will be sent to the server. Execute logging trap , no level parameters, configured as default level 6

- Configure the Rate Limit for Sending Server Logs

Command	SWITCH(config) **#logging rate-limit interval** <1-30> **burst** <1-1000> SWITCH(config)#no **logging rate-limit**
Description	Configure the rate at which the device sends logs to the remote server Interval is the time range, the default is 6, the range is <1-30>, the unit is seconds burst is the maximum number of logs that can be sent within the time range, the default is 60, the range is <1-1000> By default, up to 60 sys logs can be sent to the server every 6 seconds

7.2.4. Configure the Logging Buffer

Command	SWITCH(config) **#logging buffer** <64-4096> SWITCH(config)**#no logging buffer**
Description	Configure log storage entries, log storage starts from device startup Default number of storage entries is 1024 The range is <64-4096>

7.2.5. Clear Log

Command	SWITCH# **clear logging**
Description	Clear syslog

7.3. Examples

Case 1 : The device sent syslog to the remote server, the device IP is 1 92.168.1.240 , the remote server IP is 1 92.168.1.33 ,UDP port number is 10514.

Configure the remote server on the device:

```
SWITCH(config)# logging server 192.168.1.33 udp-port 10514
```

The device generates syslog information:

```
*1970 Jan 01 14:19:34 SWITCH %HAL-4: Interface gigabitEthernet0/1 changed
```

```
state to down
```

Monitor syslog information on the remote server:

```
       LOCAL7.warn: *1970 Jan 1 14:19:34 SWITCH %HAL-4: Interface
gigabitEthernet0/1 changed state to down
```

7.4. Display Information

- Display Logs Stored in Device

Command	SWITCH# **show logging**
Description	Show all syslog stored in device

- Display Logs Stored in Device of Last entries

Command	SWITCH# **show logging last** <1 4096>
Description	Show last specific number of logs stored in device

- Display Log Configuration Information

Command	SWITCH# **show logging summary**
Description	Display log configuration information

```
       SWITCH#show logging summary
       Summary of logging configuration:
           Logging console         : 6
           Logging monitor         : 6
           Logging trap            : 6
           Logging buffer          : 1024

           Server:
               Ip address          : 192.168.1.33
               Udp port            : 10514

           Server second           : Disabled

           Server third            : Disabled

           Rate-limit:
               Interval            : 1 seconds
              Burst                : 2
```

Field	Illustrate
Logging console	Log console output control <0-7>: Indicates the log level Disabled: Indicates no console output
Logging monitor	Log terminal line output control <0-7>: Indicates the log level Disabled: Indicates that it is not output in terminal line
Logging trap	Log trap remote server output control

	<0-7>: Indicates the log level Disabled: Indicates not sending to the remote server
Logging buffer	Log storage entries, log storage starts from device startup <64-4096>: Indicate max log storage entries
Server Server second Server third	Server, currently supports 3 servers
Ip address Ipv6 address	Ipv4, ipv6 address information
Udp port	UDP port information
Rate-limit	Speed limit for sending logs to remote server
Interval	Speed limit effective time range
Burst	Speed limit value within interval time

8. Configuring VLAN

8.1. Overview of VLAN

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a switch supporting fallback bridging.

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

Access： An access port can belong to one VLAN and is manually assigned to that VLAN.

Trunk： A trunk port is a member of all VLANs by default, but membership can be limited by configuring the allowed-VLAN list. A trunk port have a native vlan, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

Hybrid： A hybrid port is a member of all VLANs by default, but membership can be limited by configuring the allowed-VLAN list. A hybrid port allow users to configure traffic of a vlan forwards tagged or untagged. A trunk port has a hybrid vlan, The hybrid VLAN is VLAN 1 by default.

8.2. Configuring

- Creating VLAN

Command	SWITCH(config)#vlan (<vlan-id> | <vlan-range>)
	SWITCH(config)#no vlan (<vlan-id> | <vlan-range>)

Description	Create a VLAN, vlan-id 1-4094, vlan-range example: 2-10.

- Configuring the Interface as an Access Port

Command	SWITCH(config)#**interface** IFNAME SWITCH(config-if)#**switchport mode access**
Description	Configure the interface port mode access.

Command	SWITCH(config-if)#**switchport access vlan** VLANID SWITCH(config-if)#**no switchport access vlan**
Description	Specify the default VLAN of the interface, which is used if the interface is access mode. Default vlan is 1.

- Configuring the Interface as a Trunk Port

Command	SWITCH(config)#**interface** IFNAME SWITCH(config-if)#**switchport mode trunk**
Description	Configure the interface port mode trunk.

Command	SWITCH(config-if)#**switchport trunk allowed vlan** { **all** | VLAN_LIST | **none**}

	SWITCH(config-if)#**no switchport trunk allowed vlan** VLAN_LIST
Description	Configure the list of VLANs allowed on the trunk, which is used if the interface is trunk mode. All: Adds all VLANs in available in the VLAN table, New VLANs added to the VLAN table are added automatically. None: Removes all VLANs. VLAN_LIST: It will manually set the Allowed VLAN list, if it belongs to ALL, the Allowed VLAN list will be cleared first, and then the new VLAN list will be added; vlan-list parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. 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 automatically deleted. All VLANs are allowed by default.

Command	SWITCH(config-if)#**switchport trunk native vlan** VLANID SWITCH(config-if)#**no switchport trunk native vlan**
Description	Configure the VLAN that is sending and receiving untagged traffic on the trunk port. For VLANID, the range is 1 to 4094. Native VLAN has nothing to do with whether the Allowed VLAN contains this VLAN, or even whether the VLAN is created. Default vlan is 1.

Note:

✦ The default VLAN ID of the trunk port of the local device must be the same as the default VLAN ID of the trunk port of the connected device, otherwise the packets of the default VLAN will not be transmitted correctly.

- Configure the Interface as a Hybrid Port

Command	SWITCH(config)#**interface** IFNAME SWITCH(config-if)#**switchport mode hybrid**
Description	Configure the interface port mode hybrid.

Command	SWITCH(config-if)#**switchport hybrid allowed vlan** { **all** | VLAN_LIST | **none**} SWITCH(config-if)#**no switchport hybrid allowed vlan** VLAN_LIST
Description	Configure the list of VLANs allowed on the trunk, which is used if the interface is hybrid mode. All: Adds all VLANs in available in the VLAN table, New VLANs added to the VLAN table are added automatically. None: Removes all VLANs. VLAN_LIST: It will manually set the Allowed VLAN list, If it belongs to ALL , the Allowed VLAN list will be cleared first, and then the new VLAN list will be added; vlan-list parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. 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 automatically deleted. All VLANs are allowed by default.

Command	SWITCH(config-if)#**switchport hybrid vlan** VLANID SWITCH(config-if)#**no switchport hybrid vlan**

Description	Configure the default VLAN that is sending and receiving untagged traffic on the hybrid port. For VLANID, the range is 1 to 4094. Native VLAN has nothing to do with whether the Allowed VLAN contains this VLAN, or even whether the VLAN is created. Default vlan is 1.

Command	SWITCH(config-if)#**switchport hybrid untagged vlan** VLAN_LIST SWITCH(config-if)#**no switchport hybrid untagged vlan** VLAN_LIST
Description	Configure the list of untagged VLANs, which is used if the interface is hybrid mode. The default VLAN must be untagged output, therefore, it is not maintained by the untagged VLAN list. By default the untagged VLAN list is empty. 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.

Note

✦ The default VLAN ID of the hybrid port of the local device must be the same as the default VLAN ID of the hybrid port of the connected device, otherwise the packets of the default VLAN will not be transmitted correctly.

8.3. Display Information

Displays the VLAN table, includes VLAN VID, VLAN status, VLAN member ports, and VLAN configuration information.

- Display VLAN Information

```
VLAN ID  Name         State   H/W Status  Member ports
                                          (u)-Untagged, (t)-Tagged
======= ============ ======= =========== ============================
1       default      ACTIVE  Up          gigabitEthernet0/2(u)
                                             gigabitEthernet0/3(u)
```

9. Configuring QINQ

9.1. Overview of QINQ

QINQ technology also known as Stacked VLAN. The standard is derived from IEEE 802.1ad, which means that the public network VLAN Tag of a service provider network is encapsulated before the user packet enters the service provider network, and the private network user VLAN Tag in the user packet is regarded as data, so that the packet carries Two-layer VLAN tag traversal of service provider network.

In the metropolitan area network, a large number of VLANs are required to isolate users. The 4094 VLANs supported by the IEEE 802.1Q protocol are far from meeting the requirements. Through the double-layer Tag encapsulation of QINQ technology, in the service provider network, the packets are only transmitted according to the unique outer VLAN Tag allocated on the public network, so that the VLANs of different private network users can be reused, and the number of VLAN tags available to users is expanded. At the same time, it 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 is for stacking VLANs, and VLAN Mapping is for VLAN mapping.

9.1.1. VLAN Stacking

VLAN Stacking: From the user network to the provider network, a single-layer tag becomes a double-layer tag, and the C-Tag remains in the packet as an inner-layer tag; reverse, from a double-layer tag to a single-layer tag.

VLAN Stacking QINQ is divided into three categories:

- Type A: Basic QINQ, which is enabled and disabled based on the interface. When an interface with basic QINQ enabled receives a packet, it is treated as an un-tagged packet. On the basis of the original packet, a VLAN tag of the default VLAN of the port is added.
- Type B: Flexible QINQ based on C-tag, according to the C-VLAN Tag on the user side, according to the configured mapping policy, an S-VLAN tag is added to the original packet. There are two optional configuration methods for this type of QINQ, and only one of them can be selected. One way is to configure the mapping relationship between C-VLAN and S-VLAN directly on the interface; the other way is to configure VLAN VPN globally (which includes the mapping relationship between C-VLAN and S-VLAN), and then associate the VPN on the interface. When using the same mapping policy for multiple interfaces, generally choose the latter configuration method. For this type of QINQ, if the packets received by the interface are un-tagged, the C-tag is the default VLAN Tag of the interface.
- Class C: ACL-based flexible QINQ, adding outer tags according to the configured traffic policy. The configuration of this type of QINQ is placed in the "QOS" module. For details, please refer to the "Configuring QOS" chapter. The policy pair between Policy-map and Class-map: "nest vlan <1-4094>" is used to configure ACL-based Flexible QINQ.

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

9.1.2. VLAN Mapping

VLAN Mapping: From the user network to the provider network, it is still a single-layer Tag, but the C-Tag becomes S-Tag; in reverse, from S-Tag to C-Tag.

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. VLAN Mapping is configured by configuring VLAN VPN globally, and then associating VPN on interface. VLAN Mapping only takes effect on tag packets, which is very different from the QINQ function.

The following points should be noted when configuring QINQ and VLAN Mapping.

VLAN Mapping takes effect only for tagged packets. Upstream, original packets must carry tags to implement CVLAN-to-SVLAN mapping; for downstream, the VLAN output rule on downlink interfaces must be tag output to implement SVLAN-to-SVLAN mapping. Mapping of CVLANs.

Note

Only physical interfaces support the configuration of QINQ and VLAN Mapping, but aggregated interfaces do not

When using the QINQ function or the VLAN Mapping function, it needs to be used in conjunction with the VLAN configuration. In the input and output directions, the filtering function of the VLAN, and the rules for whether the VLAN carries tags are all subject to the VLAN configuration. Specific requirements are as follows:

- Both CVLAN and SVLAN need to be added to the allow list of the downlink interface (connected to the Customer network), otherwise the flow will be filtered.
- The SVLAN needs to be added to the allow list of the uplink interface (connected to the provider network), otherwise the flow will be filtered.
- For QINQ, on the downlink interface, SVLAN should be configured with untag output, so as to strip the outer tag of QINQ downstream.
- For VLAN-Map, since it only takes effect for untag packets, for downlink interfaces, 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, but not both.

VLAN Mapping only supports 1:1 mapping. Therefore, if there are VLAN VPNs with N:1 mapping, they cannot be associated with the interface as the VPN of VLAN mapping. Similarly, if the VPN has been associated with the interface as the VLAN mapping, the mapping relationship Cannot change to N:1

The mapping relationship of VLAN Mapping must be consistent globally. 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 CVLANs and SVLANs. The specific constraints are as follows.

- If VLAN Mapping is used together with basic QINQ, the basic QINQ will take effect and VLAN Mapping will be 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 CVLAN to match the mapping policy of flexible QINQ, the final packet will take effect with flexible QINQ, adding SVLAN as external Layer TAG, the inner layer TAG remains unchanged (not the VLAN mapped by VLAN Mapping).
- Due to the above constraints, when two applications are enabled on the same interface, it is necessary to pay attention that the VLANs controlled by the two do not overlap. Invalid.

For Type B QINQs, you can either choose to configure the mapping policy directly under the interface, or choose to associate with VPN, but cannot be configured at the same time.

9.2. Configuring

- Creating VLAN VPN

Command	SWITCH(config)#**vlan-vpn** VPN-NAME SWITCH(config)#**no vlan-vpn** VPN-NAME
Description	There can be multiple VPNs in the system, and each VPN maintains the mapping relationship between independent CVLANs and SVLANs. A VPN will only actually take effect when applied to an interface. A VPN can be applied to VLAN Stacking (QINQ) or VLAN Mapping, but only one of the two can be selected.

- Adding VPN Mapping Relations

Command	SWITCH(config-vlan-vpn)#**cvlan** VLAN_LIST **svlan** VLANID SWITCH(config-vlan-vpn)#**no cvlan** VLAN_LIST SWITCH(config-vlan-vpn)#**no cvlan**
Description	The valid range of VLAN_LIST and VLANID is <1,4094>, VLAN_LIST supports standard multi-vlan representation method ("-" and "," and combination of both). no cvlan without any parameters, clear all the mapping relationships in the VPN.

- Configuring Port-based QINQ

Command	SWITCH(config-if)#**switchport vlan-stacking basic** SWITCH(config-if)#**no switchport vlan-stacking basic**
Description	After basic QINQ is enabled, all incoming packets from this interface match the QINQ rules, and the mapped SVLAN is the default VLAN ID of the interface.

- Configuring Mapping Relationship of QINQ on the interface

Command	SWITCH(config-if)#**switchport vlan-stacking cvlan** VLAN_LIST **svlan** VLANID SWITCH(config-if)#**no switchport vlan-stacking cvlan** VLAN_LIST SWITCH(config-if)#**no switchport vlan-stacking cvlan**
Description	Similar to the mapping relationship configuration under VPN. Only when the interface is not associated with a VPN, can the mapping relationship be configured directly.

- Attaching QINQ VPN on the Interface

Command	SWITCH(config-if)#**switchport vlan-stacking vpn** VPN-NAME SWITCH(config-if)#**no switchport vlan-stacking vpn**
Description	An interface can only be associated with one VPN. The VPN association configuration can be performed only when the interface is not configured with a mapping relationship.

- Clearing QINQ Configuration on the Interface

Command	SWITCH(config-if)#**no switchport vlan-stacking**
Description	Equivalent to three commands: no switchport vlan-stacking basic no switchport vlan-stacking cvlan no switchport vlan-stacking vpn

- Attaching VLAN Mapping VPN on the Interface

Command	SWITCH(config-if)#**switchport vlan-mapping vpn** VPN-NAME SWITCH(config-if)#**no switchport vlan-mapping**
Description	VLAN mapping configured on different interfaces must be associated with the same VPN. And the mapping relationship in the corresponding VPN must be 1:1.

9.3. Examples

Example 1: This example shows how to configure L2 VPN service.

Service Provider provides VPN for Enterprise A and Enterprise B:

- Enterprise A and enterprise B belong to different VLANs on the public network, and communicate through their own public network VLANs.
- 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 encapsulates a layer of VLAN Tag of Native VLAN to user data packets. In the public network, user data packets are transmitted in the native VLAN, which does not affect the use of VLANs in different enterprise user networks, and implements a simple Layer 2 VPN.

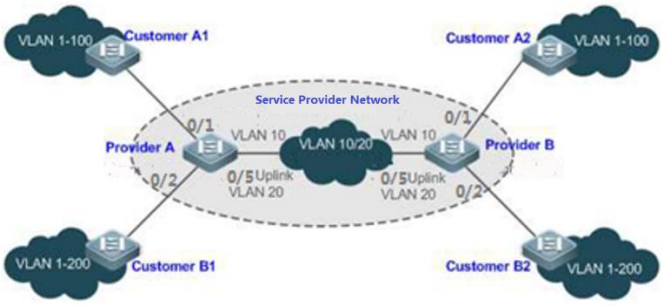


Illustration:

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

ProviderA and ProviderB are completely symmetrical and have exactly the same configuration:

- Configuring VLAN

```
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
```

- Configuring Base QINQ

```
SWITCH(config)#interface gigabitEthernet0/1-2
SWITCH(config-if)#switchport vlan-stacking basic
SWITCH(config-if)#exit
```

Example 2: This example shows how to Implement Layer 2 VPN and service flow management based on Flexible QINQ.

Basic QinQ can only encapsulate user data packets in the outer tag of a native VLAN, that is, the encapsulation of the outer tag depends on the native VLAN of the tunnel port. Flexible QinQ provides flexible encapsulation of external tags (S-Tags) of service providers (ISPs) according to the tags of user packets (ie C-Tags), so as to flexibly implement VPN transparent transmission and service flow QoS policies.

- Broadband Internet access and IPTV services are an important part of the services carried by the MAN. The MAN service provider network divides VLANs for different service flows to differentiate management, and provides QoS policy settings for these VLANs. You can use QinQ based on C-Tag on the edge device of the service provider to encapsulate the relevant VLAN of the user's business flow, and use the QoS policy of the service provider network for guaranteed transmission while transparent transmission.
- Unified VLAN planning is implemented between enterprise branches, and 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 can also use the service provider network. The QOS strategy of the company gives priority to ensuring the data transmission of important services.

As shown in the figure below, the client devices in the metropolitan area network are aggregated through the corridor switches in the community, and broadband Internet access and IPTV services are differentiated by assigning different VLANs to enjoy different QoS service policies.

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

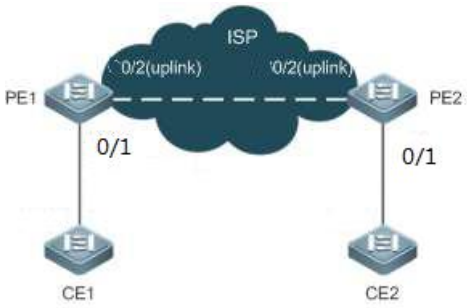


Illustration:

- CE1 and CE2 are edge devices that connect to the user's network, and PE1 and PE2 are edge devices that the provider serves on the network.
- VLAN 1-100 and VLAN 101-200 on CE1 and CE2 devices are the broadband Internet service flow for users, and the IPTV service flow for users.
- PE1 and PE2 devices package different s-tags for vlans of different businesses to distinguish different business data. VLAN 1-100 package VLAN100, vlan101-200 package VLAN200.

PE1 and PE2 are configured exactly the same:

- Configuring VLAN

```
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
```

- Configuring Flexible QINQ

```
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
SWITCH(config-if)#exit
```

Example 3: This example shows how to Implement Layer 2 VPN and service flow management based on VLAN Mapping.

Similar to Case 2, the broadband Internet access service and the IPTV service of the user are distinguished. For example, the broadband Internet access service is VLAN2, and the IPTV service is VLAN3. In the ISP network, VLAN200 and VLAN300 are respectively 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 uplink interface is gigabitEthernet0/11.

PE1 and PE2 are configured exactly the same:

- Configuring VLAN

```
SWITCH(config)#vlan2-3,200,300
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
```

- Configuring VLAN Mapping

```
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
```

9.4. Display Information

- Display a VPN Information

```
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
```

2）Display all VPN Information

```
SWITCH#show vlan-vpn
------------------------------------------------------------
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
------------------------------------------------------------
VLAN VPN: test-map1
Class: vlan-mapping
Mapping attributes:
 cvlan 100 svlan 1
 cvlan 200 svlan 2
 cvlan 800 svlan 8
 cvlan 900 svlan 9
Applied interfaces:
 gigabitEthernet0/18
 gigabitEthernet0/19
------------------------------------------------------------
VLAN VPN: test1
Class: unkown
Mapping attributes:
 cvlan 800 svlan 8
 cvlan 900 svlan 9
Applied interfaces:
```

```
        empty!
```

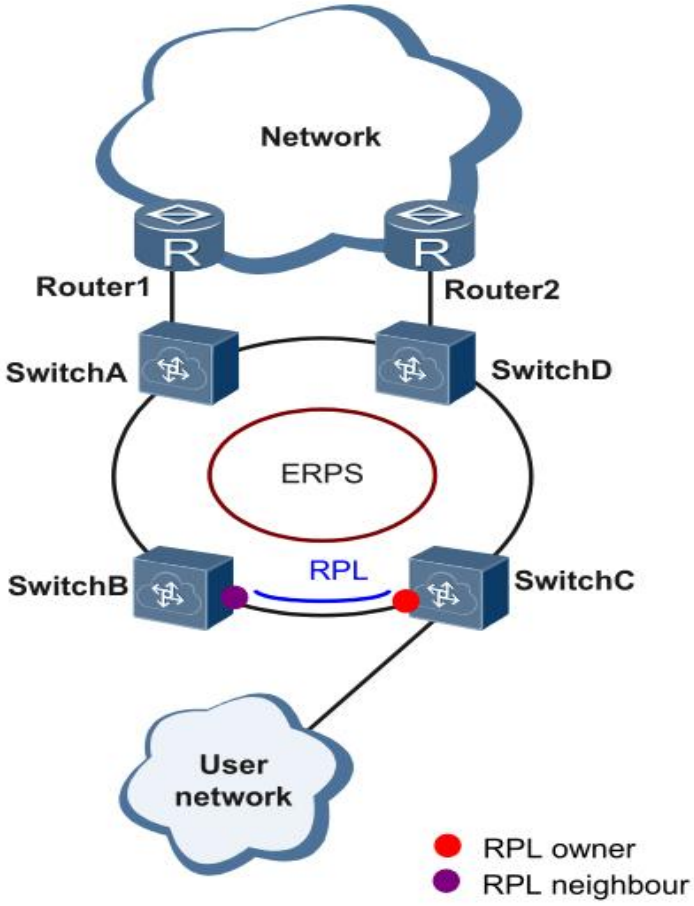
10. Configuring ERPS

10.1. Overview of ERPS

ERPS (Ethernet Ring Protection Switching) was developed by ITU, also known as G.8032.It is a link layer protocol specifically applied to Ethernet. It can prevent the broadcast storm caused by the data loop when the Ethernet ring network is complete, and can quickly restore the communication between each node on the ring network when a link on the Ethernet ring is disconnected.

At present, the technology to solve the Layer 2 network loop problem is STP.STP is more mature to use, but its convergence time is longer (seconds).ERPS is a link layer protocol that is specially applied to Ethernet and has a faster rate than STP for convergence, up to 50ms.

ERPS typical scenario：



10.2. Introduction to ERPS Rationale

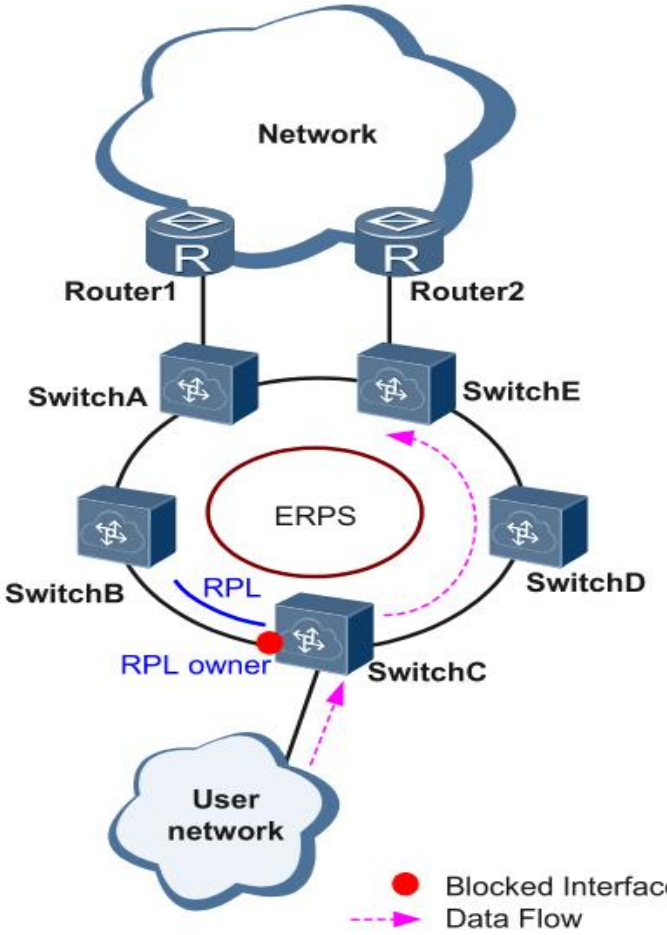
ERPS is a standard ring network protocol dedicated to the Ethernet link layer, with the ERPS ring as the basic unit. Only two ports on each layer 2 switch can be added to the same ERPS ring. In the ERPS, in order to prevent network loop, a break-down mechanism can be launched, blocking the RPL owner port and eliminating the ring route. When the ring connection fails, the equipment running the ERPS protocol

can quickly forward the blocked port, make the link protection replacement, and restore link communication between various nodes on the ring network. This section mainly presents the rationale for the implementation of ERPS under the basic network based on the normal ->link failure->link recovery process (including protection switch operations).

Link OK

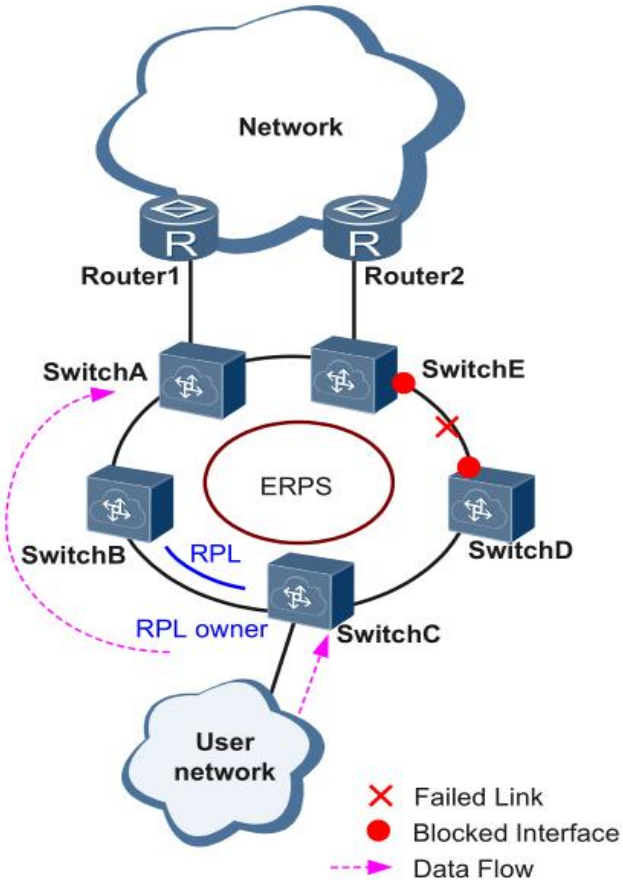
As shown in the diagram below, the equipment on the ring consisting of SwitchA~SwitchE is in good condition.

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



Link Failure

As shown in the diagram, when the link between SwitchD and SwitchE fails, the ERPS protocol starts the protection switching mechanism, blocks the ports on both ends of the faulty link, and then forward the RPL owner port, and the two ports resume user traffic. receiving and sending, thus ensuring uninterrupted traffic.



Link Restore

After the link returns to normal, if the ERPS ring is configured in revert mode, the device where the RPL owner port resides will block the traffic on the RPL link again, and the faulty link will be used again to transmit user traffic.

10.3. Configuring

- Creating Ring

Command	SWITCH(config)#**erps ring** <1-255> **east-interface** IFNAME **west-interface** IFNAME SWITCH(config)#**no erps ring** <1-255>
Description	Create/delete ERPS ring. The ERPS ring is made up of the same set of VLAN and interconnected layer 2 switch, which 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 for the ERPS ring.

- Creating ERPS Instance

Command	SWITCH(config)#**erps instance** NAME SWITCH(config)#**no erps instance** NAME
Description	Create/remove ERPS instances; Create an instance to go into instance configuration mode. For the layer 2 switch operating an ERPS protocol, VLAN transmitting ERPS and data articles must be mapped into a protective instance so that ERPS protocol can be forwarded or blocked in accordance with their blocking principles. Otherwise, user traffic could cause broadcast storms in a ring network that could make the network unavailable.

- Associating ERPS Instances and Rings

Command	SWITCH(config-erps-inst)#**ring** <1-255>
Description	Configure the corresponding relationships between ERPS instances and rings.

- Configuring ERPS Instance Level

Command	SWITCH(config-erps-inst)#**level** <0-7>
Description	Configure ERPS instance level.

- Configuring RPL Roles in ERPS Instance

Command	SWITCH(config-erps-inst)#**rpl-role** NAME
Description	Configure the ERPS instance RPL role; An ERPS ring has only one RPL owner port, which is determined by user configuration. The RPL owner port is blocked from forwarding user traffic to prevent loops in the ERPS ring.

- Configuring Raps VLAN for Instance

Command	SWITCH(config-erps-inst)#**vlan** <1-4094> **raps-channel** SWITCH(config-erps-inst)#**no raps-channel**
Description	Configuration/delete raps VLAN for ERPS instances; Each ERPS ring must be configured with a raps VLAN.Different ERPS rings cannot use the same raps VLAN ID.

- Configuring MST Instance

Command	SWITCH(config-erps-inst)#**protected-mst-instance** <0-255>
Description	Configure MST Instance; The relationship between VLAN and Instance can be configured in MST mode, after STP mode be set to MSTP, refer to STP configuration for more details; by default, all VLANs belong to Instance 0; the default value is 0. Note: Multi-instance is currently not supported in intersecting rings!

- Configuring Intersecting Sub-ring Block Port

Command	SWITCH(config-erps-inst)#**sub-ring block (east-interface | west-interface)**
Description	Configure the ERPS instance as a sub-ring instance and specify a sub-ring block port.

- Configuring Sub-ring Virtual Channels and Non-virtual Channels

Command	SWITCH(config-erps-inst)#**virtual-channel attached-to-instance** NAME SWITCH(config-erps-inst)# **non-virtual-channel**
Description	Configure the type of ERPS intersecting sub-ring: virtual channel and associated main ring; or non-virtual channel type. Note: The position displayed by this command in show running-config must be after the displayed position of the associated instance. Normally only need to ensure that the sub-ring ID and instance name are larger than the main ring ID and instance name.

- Configuring ERPS Revert Mode

Command	SWITCH(config-erps-inst)#**revertive | non-revertive**
Description	Configure ERPS revertive/non-revertive.

- Configuring ERPS Timer Parameters

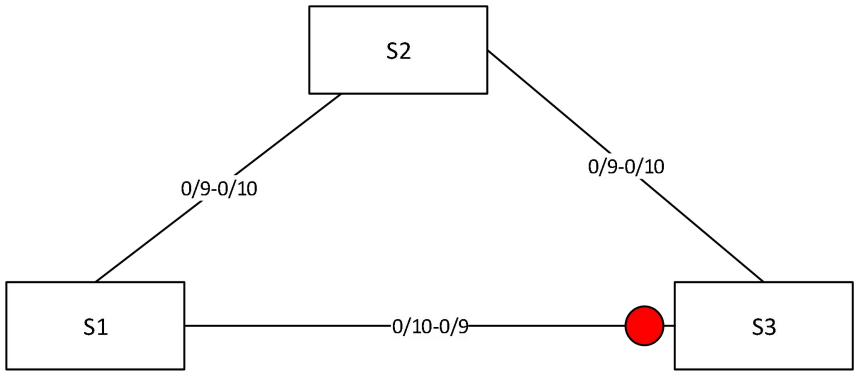
Command	SWITCH(config-erps-inst)# (**wtr-timer** (<1-12> | **default**) | **holdoff-timer** (<0-100> | **default**) | **guard-timer** (<1-200> | **default**))
Description	Configure ERPS timer parameters. <1-12>: in minutes; revert time after recovery, default is 5 minutes. <0-100>: in 100 milliseconds; hold time before port forwarding, the default is 0, direct forwarding without delay. <1-200>: in 10 milliseconds; protection window when state changes, avoid receiving messages from previous state leading to protocol errors, default is 50: 500 ms. **guard-timer** parameters limit network size. It is conservatively recommended that when there are more than 300 nodes in the ring network, directly configure this parameter to the maximum value to avoid the failure of old packets to be discarded due to the large network size; no special configuration is required for nodes within 300 nodes.

- Configuring ERPS Logging

Command	SWITCH(config)# **erps logging** SWITCH(config)# **no erps logging**
Description	Configure ERPS logging.

10.4. Examples

1. Single-ring case requirements: As shown in the figure, the configuration blocks the direct links of S1 and S2 by default, and restores the link in time to ensure the availability of the network in case of failure. Where the data VLANs are 1, 2 and 3.



S1/S2:

- Enter global configuration mode, create ERPS and set related parameters, command reference list below:

Create vlan 2,3;vlan 1 default exists

```
SWITCH(config)#vlan 2,3
```

Change the interface mode to trunk. By default, trunk mode will add all data vlans and management vlans to the interface for forwarding.

```
SWITCH(config)#interface gigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
```

Create ERPS ring 1

```
SWITCH(config)#erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
```

Create ERPS instance 1, associated with ring 1, and associated details configuration

```
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
```

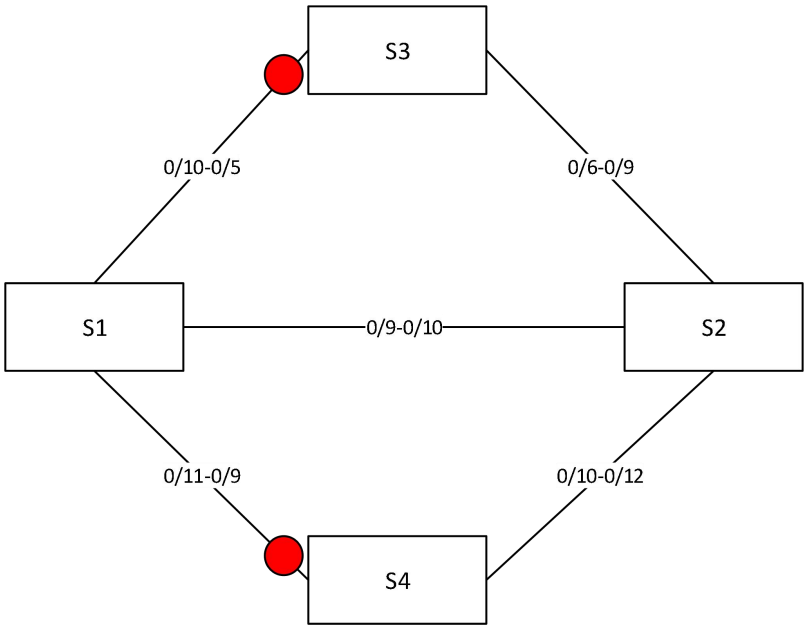
S3:

- Enter global configuration mode, create ERPS and set related parameters, command reference list below:

```
SWITCH(config)#Vlan 2,3
SWITCH(config)#interface gigabitEthernet0/9,gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
SWITCH(config)#Erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role owner east
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

2. Intersection ring case requirements

As shown in the following topology, S1, S2, S3, and S4 form intersecting rings, and the data vlans are 1, 2, 3, and 4. It is required to achieve fast convergence when a single point of failure occurs in each ring; a maximum of two faults can occur in the network Points (different rings), without user disconnection, to achieve optimal reliability.



Typical configuration examples:

S1:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/11
```

```
Erps instance 2
 ring 2
  sub-ring block east-interface
  vlan 1100 raps-channel
  virtual-channel attached-to-instance 1
```

S2:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/12 west gigabitEthernet0/10
Erps instance 2
 ring 2
  sub-ring block east-interface
  vlan 1100 raps-channel
  virtual-channel attached-to-instance 1
```

S3:

```
Vlan 2,3,4
interface gigabitEthernet0/5-6
switchport mode trunk
Erps ring 1 east gigabitEthernet0/5 west gigabitEthernet0/6
Erps instance 1
 ring 1
 rpl-role owner east
 vlan 1000 raps-channel
```

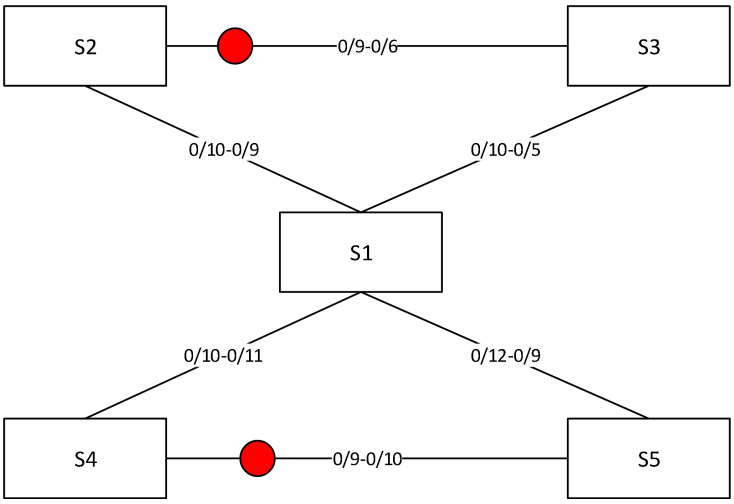
S4:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 2
 ring 2
 rpl-role owner east
 vlan 1100 raps-channel
```

3. Tangent ring case requirements

The topology diagram is shown below. S1 is located in the central computer room, which can be supervised and maintained by the administrator in real time, and has high reliability; S2-S5 are distributed in various deployment points, in order to improve the reliability of the network and avoid the occurrence of single-link external connection The single-point failure risk is avoided, and the single-machine failure risk that may occur in a dual-link external connection is avoided, and the dual-link external connection is used to form a ring network.

It is required that each ring network can converge quickly when a single point of failure occurs to avoid user network interruption.



Typical configuration examples:

S1:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/11 west gigabitEthernet0/12
Erps instance 2
 ring 2
  vlan 1100 raps-channel
```

S2:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 rpl-role owner east
 vlan 1000 raps-channel
```

S3:

```
Vlan 2,3,4
interface gigabitEthernet0/5-6
switchport mode trunk
Erps ring 1 east gigabitEthernet0/5 west gigabitEthernet0/6
Erps instance 1
 ring 1
 vlan 1000 raps-channel
```

S4:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
```

```
Erps instance 2
 ring 2
 rpl-role owner east
 rpl-role owner east
```

S5:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 2
 ring 2
 vlan 1100 raps-channel
```

10.5. Display Information

- Show ERPS Ring Information

```
SWITCH#show erps ring 1

Ring     : 1
==========
Bridge   : 1
East     : gigabitEthernet0/23
West     : gigabitEthernet0/24
ERP Inst :1, 2,
SWITCH#
```

- Show ERPS Instances

```
SWITCH#
SWITCH#show erps instance 1
Name                  : 1
Protected MST Instance: 0
Protected VLANs       : 1
State                 : ERPS_ST_IDLE
Last Priority         : RAPS-NR-RB
Phy Ring              : 1
Role                  : NON-OWNER
East Link             : Link_Unblocked(up)(78-A9-12-12-13-12, 1)
West Link             : Link_Unblocked(up)(78-A9-12-12-13-12, 1)
TCN Propagation       : Disabled
Attached              : -
Attached To           : -
Virtual ID            : -:-
-----------------------------------------------------
     Channel         |       Interface
 (LEVL, VID, RID)    | (east,ver) ,   (west,ver)
=====================================================
 (0, 1000,    1)     | (gigabitEthernet0/23, V=1), (gigabitEthernet0/24,
V=1)
=====================================================
Wait-To-Restore       : 5 mins
Hold Off Timer        : 0 secs
Guard Timer           : 500 ms
Wait-To-Block         : 5500 ms
```

```
        Protection Type        : Revertive
        SWITCH#
```

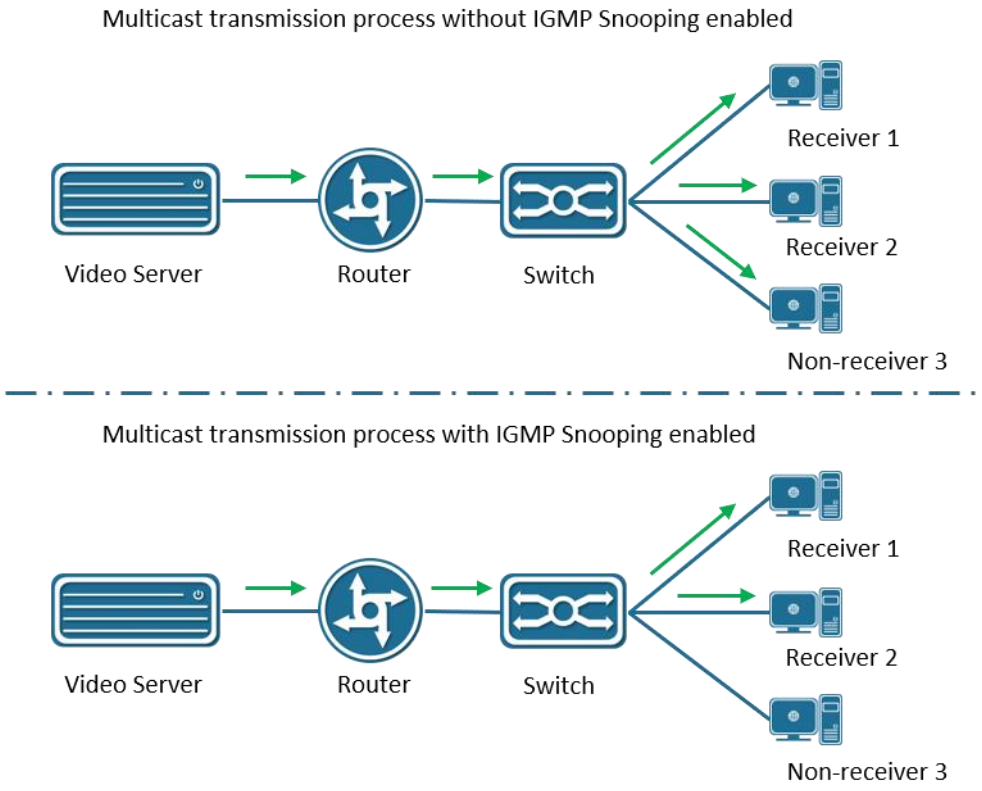
11. Configuring IGMP Snooping

11.1. Overview of IGMP Snooping

IGMP Snooping is a short term for Internet Group Management Protocol Snooping, a mechanism running on a layer 2 device for managing and controlling multicast groups.

A Layer 2 device running IGMP Snooping analyzes the received IGMP packets, establishes a mapping relationship between ports and MAC multicast addresses, and forwards multicast data according to the 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, the multicast data of the known multicast group will not be broadcast at Layer 2, but at Layer 2.

As shown in the figure below, when the Layer 2 multicast device does not run IGMP Snooping, the IP multicast packets are broadcast in the VLAN; when the Layer 2 multicast device runs IGMP Snooping, the IP multicast packets are only sent to the group members recipient.



11.2. Configuring

- Enabling IGMP Snooping

Command	SWITCH(config)# **igmp snooping** SWITCH(config)# **no igmp snooping**
Description	Enable/disable IGMP Snooping function; disabled by default. Global configuration mode.

- Configuring IGMP Snooping Upstream Ports

Command	SWITCH(config-if)# **igmp snooping mrouter interface** IFNAME

	SWITCH(config-if)# **no igmp snooping mrouter interface** IFNAME
Description	Configure/delete IGMP Snooping upstream port; optional configuration. SVI interface mode.

- Configuring IGMP Snooping Static Groups

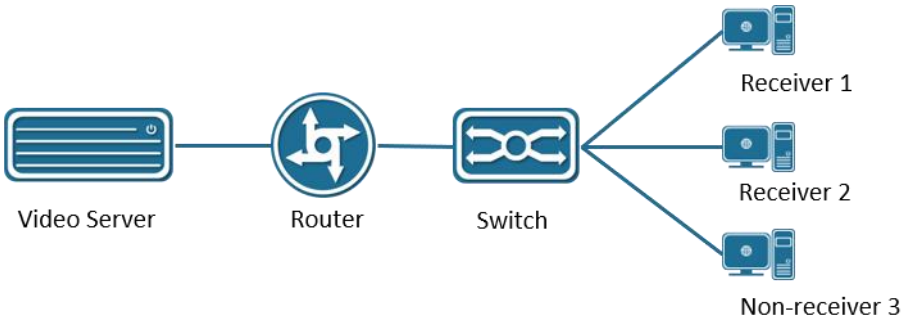
Command	SWITCH(config-if)# **igmp snooping static-group** IPADDR **source** IPADDR **interface** IFNAME SWITCH(config-if)# **no igmp snooping static-group** IPADDR **source** IPADDR **interface** IFNAME
Description	Configure/delete IGMP Snooping static group; optional configuration. SVI interface mode.

- Configuring IGMP Snooping Fast Leave

Command	SWITCH(config-if)# **igmp snooping fast-leave** SWITCH(config-if)# **no igmp snooping fast-leave**
Description	Configure/delete IGMP Snooping fast leave function; optional configuration. SVI interface mode.

11.3. Examples

Simplified topology:



Basic configuration /roles: (top down)

server:

During the test, VLC is used as the multicast server to provide the multicast service: udp://225.0.0.1:1234, the server IP is 3.3.3.10

router:

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

Enable multicast routing

```
ip multicast-routing
```

Configure the uplink port , connect to the server, here is simply to select the PIM dense mode, the actual network scale is large, and the multicast use is less, it is recommended to use the sparse mode

```
interface GigabitEthernet 0/23
 no switchport
 no ip proxy- arp
 ip pim dense-mode
```

```
ip address 3.3.3.3 255.255.255.0
```

Configure the downlink port. The PIM dense mode is simply selected here. The actual network scale is large and the multicast usage is small. It is recommended to use the sparse mode

```
interface VLAN 1
no ip proxy- arp
 ip pim dense-mode
ip address 2.2.2.1 255.255.255.0
```

SWITCH:

Multicast can be enabled

```
igmp snooping
```

Client:

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

11.4. Display Information

- View IGMP Snooping Multicast Groups

```
SWITCH#show igmp snooping groups
```

- Viewing IGMP Snooping Interface Information

```
SWITCH#show igmp snooping interface {ifname}
Example:
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
```

- Viewing IGMP Snooping Routing Port Information

```
SWITCH#show igmp snooping mrouter vlan1
Example:
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) -- --
```

- Viewing IGMP Snooping Interface Statistics

```
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
```

12. Configuring Spanning Tree Protocol

12.1. Overview of Spanning Tree Protocol

Spanning Tree Protocol is a Layer 2 management protocol that eliminates Layer 2 loops by selectively blocking redundant links in the network, and 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, Spanning Tree Protocol) to RSTP (Rapid Spanning Tree Protocol, Rapid Spanning Tree Protocol), to the latest MSTP (Multiple Spanning Tree Protocol).

Comparison of three spanning tree protocols:

Spanning Tree Protocol	Features	Application Scenario
STP	Form a loop-free tree, resolve broadcast storms and implement redundant backup. Slow convergence.	There is no need to distinguish user or service traffic, all VLANs share a spanning tree.
RSTP	Form a loop-free tree, resolve broadcast storms and implement redundant backup. Convergence is fast.	
MSTP	Form a loop-free tree, resolve broadcast storms and implement redundant backup. Convergence is fast. Multiple spanning trees implement load balancing among VLANs, and traffic of different VLANs is forwarded according to different paths.	It is necessary to distinguish user or service traffic and implement load balancing. Different VLANs forward traffic through different spanning trees, and each spanning tree is independent of each other.

12.1.1. STP

12.1.1.1. Requirement Background

STP is a protocol for eliminating loops in local area networks. Devices running this protocol discover loops in the network by exchanging information with each other, and appropriately block certain ports to eliminate loops. Due to the continuous growth of LAN scale, Spanning Tree Protocol has become one of the most important LAN protocols.

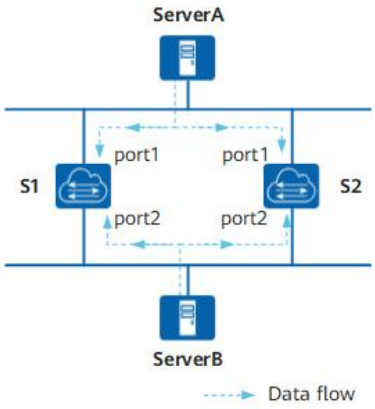


Figure2-1 Schematic diagram of typical local area network

In the network shown in Figure2-1, the following two situations will occur:

1. Network unavailable due to broadcast storm.

The loop generates a broadcast storm, which can make the network unavailable. Assume that the STP protocol is not enabled on the switch device. If ServerA sends a broadcast request, then the broadcast packet will be received by the port port1 of the other two switching devices, and broadcast from the port port2 respectively, and then the port port2 will receive another switching device. The broadcast packets are forwarded from the ports port1 of the two switching devices respectively. Repeatedly, the entire network resources will be exhausted and the network will be paralyzed and unavailable.

2. MAC address table flapping caused MAC address table entries to be destroyed.

Even unicast packets may cause confusion in the MAC address table entries of the switching device, thus destroying the MAC address table of the switching device.

Assuming that there is no broadcast storm in the network shown, ServerA sends a unicast packet to ServerB. If ServerB is temporarily removed from the network at this time, then the MAC address entry about ServerB on the switching device will also be changed. been deleted. At this time, the unicast packet sent by ServerA to ServerB will be received by port 1 of switching device S1. Since there is no corresponding MAC address forwarding entry on S1, the unicast packet will be forwarded to port 2. Then the port port2 of the switching device S2 receives the unicast message sent from the peer port2 port, and then sends it out from port1. At the same time, the port port1 of the switching device S2 will also receive the unicast message sent by ServerA to ServerB, and then send it out from port2. So repeatedly, on the two switching devices, since the unicast packets from host A are continuously received from ports port1 and port2, the switching device will constantly modify its own MAC address entries. , thus causing the MAC address table to jitter. If this goes on, the MAC address entry will eventually be destroyed.

12.1.1.2. Basic Concepts

- One Root Bridge

For an STP network, there is only one root bridge in the entire network, which is the logical center of the entire network, but not necessarily the physical center. The root bridge changes dynamically according to changes in the network topology.

After the network converges, the root bridge will generate and send configuration BPDUs at certain time intervals. Other devices will only process the packets and communicate the topology change records to ensure topology stability.

- Two metrics

The generation calculation of spanning tree has two basic metrics: ID and path cost.

ID

ID is divided into: BID (Bridge ID) and PID (Port ID).

BID: Bridge ID

The IEEE 802.1D standard stipulates that the BID is composed of the bridge priority (Bridge Priority) and the bridge MAC address. BID bridge priority occupies the upper 16 bits, and the remaining lower 48 bits are the MAC address.

In an STP network, the device with the smallest bridge ID will be elected as the root bridge.

PID: Port ID

PID consists of two parts, the upper 4 bits are the port priority, and the lower 12 bits are the port number. PID is only useful for selecting the designated port in some cases.

Path cost

Path Cost is a port variable and a reference value used by the STP protocol to select links. The STP protocol selects the 'stronger' link by calculating the path cost, blocks the redundant links, and prunes the network into a loop-free tree network structure.

In an STP network, the path cost from a port to the root bridge is the accumulation of the path costs of the outgoing ports on the bridges it passes through. This value is called the Root Path Cost.

- Three-element election

From ring network topology to tree structure, there are generally three elements: root bridge, root port and designated port. The following three elements are introduced in combination with Figure2- 2.

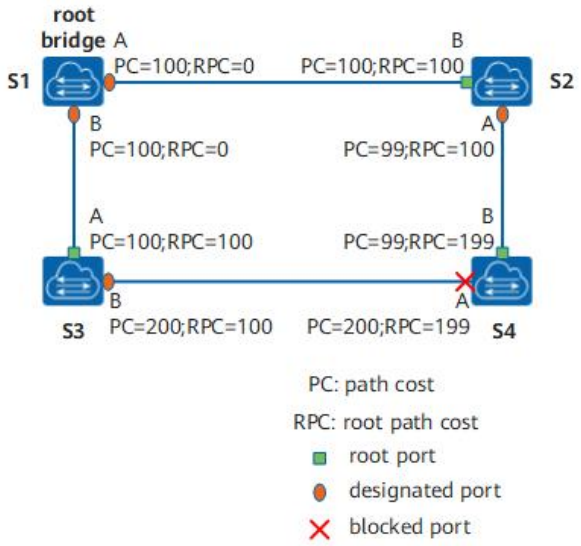


Figure2- 2 STP network structure

Root Bridge RB

The root bridge is the bridge with the smallest bridge ID, and the smallest BID is selected by configuring the BPDU protocol packets interactively.

Root Port RP

The so-called root port is the port with the least path cost to the root bridge. The root port is responsible for forwarding data to the root bridge. The selection criteria of this port are determined based on the cost of the root path. Among all STP-enabled ports on a device, the one with the lowest root path cost is the root port. Obviously, there is only one root port on a device running the STP protocol, and there is no root port on the root bridge.

Designated Port (Designated Port)

See Table2- 1 for the description of the designated bridge and designated port.

Table2- 1 Meaning of Designated Bridge and Designated Port

Classification	Specify bridge	Designated port
Device	A device directly connected to this machine and responsible for forwarding configuration messages to this machine	The designated bridge's port that forwards configuration BPDUs to the device
LAN	The device responsible for	The designated bridge's port that

Classification	Specify bridge	Designated port
	forwarding configuration messages to this network segment	forwards configuration BPDUs to the LAN

As shown in , AP1, AP2, BP1, BP2, CP1, and CP2 represent the ports of devices S1, S2, and S3, respectively.

S1 forwards configuration messages to S2 through port AP1, then the designated bridge of S2 is S1, and the designated port is port AP1 of S1.

There are two devices connected to the local area network LAN: S2 and S3. If S2 is responsible for forwarding configuration messages to the LAN, the designated bridge of the LAN is S2, and the designated port is the BP2 of S2.

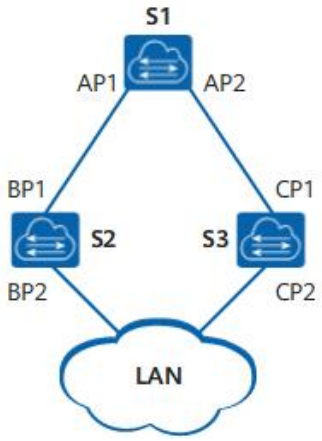


Figure2-3 Designated Bridge and Designated Port Diagram

Once the root bridge, root port, and designated port are elected successfully, the entire tree topology is established. After the topology is stable, only the root port and the designated port forward traffic, and other non-root and non-designated ports are in the blocking state. They only receive STP protocol packets and do not forward user traffic.

- Four comparison principles

STP election has four comparison principles to form a message priority vector: < root bridge ID, root path cost, sending device BID, sending port PID>.

The main information of this port carried in the configuration BPDU is shown in Table2-2.

Table2-2 Four Important Information Fields

Field Content	Brief Description
Root Bridge ID	There is exactly one root per STP network.
Root path cost	The distance from the port sending the configuration BPDU to the root bridge determines the path cost to the root bridge.
Sender BID	The BID of the device that sent the configuration BPDU.
PID	PID of the port that issued the configuration BPDU.

Other devices in the STP network will compare the fields described in table after receiving the configuration BPDU message. The four basic comparison principles are as follows:

Minimum BID: used to elect the root bridge. Select the smallest BID according to the root bridge ID field between devices running the STP protocol.

Minimum root path cost: used to select root ports on non-root bridges. On the root bridge, the root path cost from each port to the root bridge is 0.

Minimum sender BID: When a device running the STP protocol wants to select a root port among two or more ports with the same root path cost, it is calculated by the STP protocol, and the received configuration message will be selected. The port with the smaller sender's BID. As shown in Figure2-2, assuming that the BID of S2 is smaller than the BID of S3, if the root path costs in the BPDUs received by ports A and B of S4 are equal, then port B will become the root port .

Minimum PID: When the root path cost is the same, the port with the smallest PID is not blocked, but the port with the larger PID value is blocked. The PID only works in the case shown in Figure2-4, the PID of port A of S1 is smaller than the PID of port B, because in the BPDUs received on the two ports, the root path overhead, sending exchange The device BIDs are the same, so the basis for eliminating the loop is only the PID.

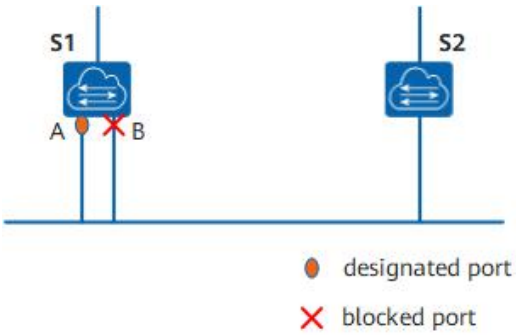


Figure2-4 Topology applied to PID for comparison

- Five Port States

The port status on the device running the STP protocol is shown in Table2-3.

Table2-3 STP Port Status

Port Status	Purpose	Description
Forwarding	The port both forwards user traffic and processes BPDUs.	Only the root port or the designated port can enter the Forwarding state.
Learning	The device will build a MAC address table based on the received user traffic, but will not forward user traffic.	Transition state, add Learning state to prevent temporary loops.
Listening	Determine the port role. The root bridge, root port and designated port will be elected.	Transition state.
Blocking	The port only receives and processes BPDUs and does not forward user traffic.	The final state of the blocked port.
Disabled	The port not only does not process BPDUs, but also does not forward user traffic.	The port status is Down.

The port state migration mechanism is shown in .

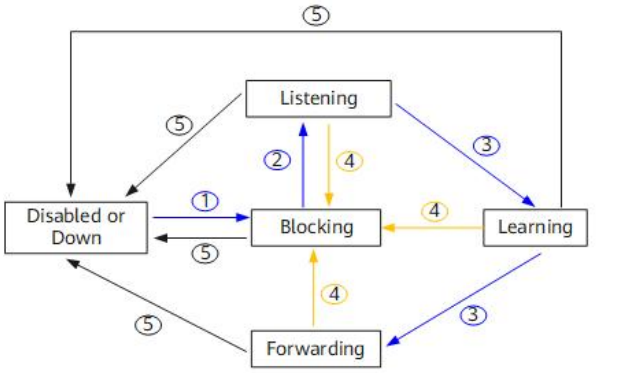


Figure2-5 STP port state transition diagram

For STP, the following 3 parameters affect port status and port convergence.

1. Hello Time

The time interval at which the device running the STP protocol sends the configuration message BPDU, which is used by the device to detect whether the link is faulty. The device will send hello packets to surrounding devices every Hello Time to confirm whether the link is faulty.

When the network topology is stable, the modification of this timer will only take effect after the root bridge is modified. The new root bridge will populate the appropriate fields in outgoing BPDUs to pass the timer modification information to other non-root bridges. But when the topology changes, the sending of TCN BPDUs is not managed by this timer.

2. Forward Delay

Delay time for device state transition. A link failure will cause the network to recalculate the spanning tree, and the structure of the spanning tree will change accordingly. However, the new configuration message obtained by recalculation cannot immediately spread to the entire network. If the newly selected root port and designated port start data forwarding immediately, it may cause a temporary loop. For this reason, STP adopts a state transition mechanism. The newly selected root port and designated port can enter the forwarding state after 2 times of the Forward Delay. Configuration messages are propagated throughout the network, preventing temporary loops.

Forward Delay Timer refers to the respective durations of a port in the Listening and Learning states. The default is 15 seconds. The Listening state lasts for 15 seconds, followed by the Learning state for another 15 seconds. Ports in these two states do not forward user traffic, which is exactly what STP is used to avoid temporary loops.

3. Max Age

The aging time of BPDU packets of the port can be manually changed by commands on the root bridge. Max Age can be guaranteed to be consistent in the entire network by configuring the transmission of BPDU packets. After the non-root bridge device in the network running the STP protocol receives the

configuration BPDU message, the Message Age and Max Age in the message will be compared:

If Message Age is less than or equal to Max Age, the non-root bridge device continues to forward configuration BPDUs.

If Message Age is greater than Max Age, the configuration BPDU will be aged out. The non-root bridge device directly discards the configuration BPDU. It can be considered that the network diameter is too large and the root bridge connection fails.

If the configuration BPDU is sent by the root bridge, the Message Age is 0. Otherwise, Message Age is the total time from the root bridge to the BPDU received by the current bridge, including transmission delay, etc. In the actual implementation, when BPDU packets pass through a bridge, the Message Age is increased by 1.

12.1.1.3. Message Format

Information such as bridge ID, path cost, and port ID were introduced in the previous chapters, all of which are transmitted via BPDU protocol packets.

The configuration BPDU is a heartbeat message. As long as the port is enabled with STP, the configuration BPDU will be sent from the designated port at the interval specified by the Hello Time timer. TCN BPDUs are sent when the device detects that the network topology has changed.

BPDUs are encapsulated in Ethernet data frames, the destination MAC is multicast MAC: 01-80-C2-00-00-00, the Length/Type field is the MAC data length, followed by LLC header, LLC is followed by the BPDU header. The Ethernet data frame format is shown in Figure2-6.

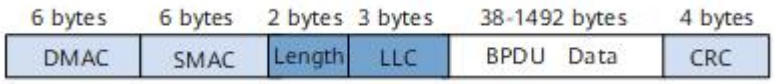


Figure2-6 Ethernet Data Frame Format

- Configuring BPDU

Most commonly referred to as BPDUs refer to configuration BPDUs.

During initialization, each bridge actively sends configuration BPDUs. But after the network topology is stable, only the root bridge actively sends configuration BPDUs, and other bridges trigger to send their own configuration BPDUs after receiving configuration BPDUs from upstream. The length of the configuration BPDU must be at least 35 bytes, including parameters such as bridge ID, path cost, and port ID. Only when at least one of the sender's BID or port PID is different from the receiving port of the bridge, the BPDU will be processed, otherwise it will be discarded. This avoids processing BPDUs with the same port information.

The configuration BPDU will be generated in the following 3 cases:

1. As long as the port is enabled with STP, the configuration BPDU will be sent from the designated port at the interval specified by the Hello Time timer.
2. When the root port receives a configuration BPDU, the device where the root port is located will copy a configuration BPDU to each of its designated ports.
3. When the designated port receives a configuration BPDU that is worse than its own, it will immediately send its own BPDU to the downstream device.

The basic format of the configuration BPDU message is shown in Table2-4.

Table2-4 BPDU basic format

Field	bytes	Description
Protocol Identifier	2	Always 0.
Protocol Version Identifier	1	Always 0.
BPDU Type	1	Current BPDU type: 0x00: Configure BPDU. 0x80: TCN BPDU.
Flags	1	Network topology change flag: Lowest bit = TC (Topology Change) flag. Highest bit=TCA (Topology Change Acknowledgment, Topology Change Acknowledgment) flag.
Root Identifier	8	The BID of the current root bridge.
Root Path Cost	4	The total cost of this port to the root bridge.
Bridge Identifier	8	BID of this switching device.
Port Identifier	2	Port ID for sending this BPDU.
Message Age	2	The message age of this BPDU. If the configuration BPDU is sent by the root bridge, the Message Age is 0. Otherwise, Message Age is the total time from the root bridge to the BPDU received by the current bridge, including transmission delay, etc. In the actual implementation, when BPDU packets pass through a bridge, the Message Age is increased by 1.
Max Age	2	Message aging age.
Hello Time	2	The time interval between sending two adjacent BPDUs.
Forward Delay	2	Controls the duration of the Listening and Learning states.

The flag field is shown in Figure2-7, only the highest and lowest bits are used in STP.

Figure2-7 Flags field format

- TCN BPDU

TCN BPDU content is relatively simple, only the first 3 fields listed in Table2-4: protocol number, version and type. The type field is a fixed value of 0x80, and the length is only 4 bytes.

TCN BPDU refers to sending a topology change notification to the upstream when the downstream topology changes, until the root node. TCN BPDU will be generated in the following two cases:

1. The port status changes to Forwarding status.
2. The designated port receives the TCN BPDU, copies the TCN BPDU and sends it to the root bridge.

12.1.1.4. Topology Calculation

After all devices in the network enable the STP protocol, each device considers itself to be the root bridge. At this point, each device only sends and receives configuration BPDUs without forwarding user traffic, and all ports are in the Listening state. After all devices exchange configuration BPDUs, they perform election work to elect the root bridge, root port and designated port.

BPDU interaction process

As shown in Figure2-8, the quadruple marked with <> represents the root bridge ID (S1_MAC and S2_MAC represent the BIDs of two devices in the figure), the accumulated root path cost, An ordered group consisting of sender BID and sending port PID. The configuration BPDU will be sent at the interval specified by the Hello Timer.

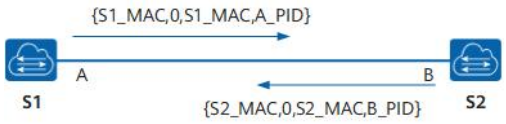


Figure2-8 Initial Information Interaction

Basic process of STP algorithm implementation

- Initial state

Because each bridge thinks it is the root bridge, in the BPDU sent by each port, the root bridge field uses its own BID, and the Root Path Cost field is accumulated to the root bridge. Overhead, the sender BID is its own BID, and the port PID is the port ID of the port that sent the BPDU.

- Select root bridge

When the network is initialized, all STP devices in the network consider themselves to be the 'root bridge', and the root bridge ID is its own device ID. By exchanging configuration messages, devices compare root bridge IDs, and the device with the smallest root bridge ID in the network is selected as the root bridge.

- Select root port and designated port

The selection process of root port and designated port is shown in Table2-5.

Table2-5 Root port and designated port selection process

Step	Process
1	The non-root bridge device will set the port that receives the optimal configuration message (the selection process of the optimal configuration message is shown in Table2-6) as the root port
2	The device calculates a designated port configuration message for each port according to the configuration message of the root port and the path cost of the root port: Replace the root bridge ID with the root bridge ID of the configuration message of the root port; The root path cost is replaced by the root path cost of the root port configuration message plus the path cost corresponding to the root port; Replace the sender's BID with the ID of its own device; Replace the sending port PID with the own port ID.
3	The device compares the calculated configuration message with the role-pending port's own configuration message: If the calculated configuration message is better, the port is determined to be the designated port, and its configuration message is also replaced by the calculated configuration message and sent out periodically; If the port's own configuration message is better, the port's configuration message will

Step	Process
	not be updated and the port will be blocked. This port will no longer forward data, and will only receive and not send configuration messages.

Table2- 6 Optimal configuration message selection process

Step	Process
1	Each port compares the received configuration message with its own configuration message: If the received configuration message has a lower priority, it will be discarded directly, and its own configuration message will not be processed; If the received configuration message has a higher priority, replace the content of the configuration message with the content of the configuration message.
2	The device compares the configuration messages of all ports and selects the optimal configuration message.

STP algorithm implementation example

Once the root bridge, root port and designated port are elected successfully, the whole tree topology is established. The following describes the specific process of implementing the STP algorithm with an example.

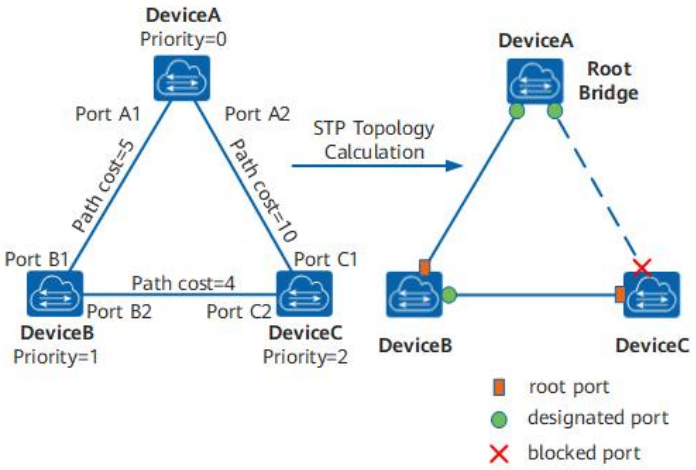


Figure2- 9 STP algorithm implementation process networking diagram and calculated topology

As shown in the figure, the priorities of DeviceA, DeviceB, and DeviceC are 0, 1, and 2, respectively. The path cost of the links between DeviceA and DeviceB, between DeviceA and DeviceC, and between DeviceB and DeviceC 5, 10 and 4 respectively.

Initial state of each device

The initial state of each device is shown in the table below.

Table2- 7 Initial state of each device

Device	Port Name	Port configuration message < Root bridge ID, cumulative root path cost, sender BID, sender port PID>
DeviceA	Port A1	<0,0,0,Port A1>
	Port A2	<0,0,0,Port A2>
DeviceB	Port B1	<1,0,1,Port B1>
	Port B2	<1,0,1,Port B2>

Device	Port Name	Port configuration message < Root bridge ID, cumulative root path cost, sender BID, sender port PID>
DeviceC	Port C1	<2,0,2,Port C1>
	Port C2	<2,0,2,Port C2>

Comparison process and results of each device

The comparison process and results of each device are shown in the table below.

Table2- 8 STP topology calculation process and results

Device	Comparison process	Configuration message of port after comparison
DeviceA	Port A1 received the configuration message of Port B1 <1, 0, 1, Port B1>, and found that its configuration message < 0, 0, 0, Port A1> was better, so it throw away. Port A2 receives the configuration message <2, 0, 2, Port C1> of Port C1, and finds that its configuration message < 0, 0, 0, Port A2> is better, so it throw away. DeviceA finds that both the root bridge and the designated bridge in the configuration messages of its ports are itself, so it thinks that it is the root bridge, and the configuration messages of each port do not make any changes, and then periodically send out Send configuration message.	Port A1: <0, 0, 0, Port A1> Port A2: <0, 0, 0, Port A2>
DeviceB	Port B1 receives the configuration message of Port A1 <0,0,0,Port A1>, and finds that it is better than its own configuration message <1,0,1,Port B1>, so Update your own configuration message. Port B2 receives the configuration message of Port C2 <2, 0, 2, Port C2>, and finds that its configuration message < 1, 0, 1, Port B2> is better, so it throw away.	Port B1: <0, 0, 0, Port A1> Port B2: <1, 0, 1, Port B2>
	DeviceB compares the configuration messages of its own ports and finds that the configuration messages of Port B1 are optimal, so this port is determined as the root port, and its configuration messages remain unchanged. DeviceB calculates the configuration message <0, 5, 1, Port B2> of the designated port for Port B2 according to the configuration message and path cost of the root port, and then matches the configuration message of Port B2 itself < 1, 0, 1, and Port B2> are compared, and it is found that the calculated configuration message is better, so Port B2 is determined as the designated port, and its configuration message is also replaced with the calculated configuration message and sent out periodically. .	Root port B1: <0, 0, 0, Port A1> Designated port B2: <0, 5, 1, Port B2>
DeviceC	Port C1 receives the configuration message of Port A2 <0,0,0,Port A2>, and finds that it is better than its own configuration message <2,0,2,Port C1>, so Update your own configuration message. Port C2 receives the configuration message <1, 0, 1, Port B2> before the update of Port B2, and finds that it is better than its own configuration message < 2, 0, 2, Port C2> , so update your own configuration message.	Port C1 :<0, 0, 0, Port A2> Port C2: <1, 0, 1, Port B2>

Device	Comparison process	Configuration message of port after comparison
	DeviceC compares the configuration messages of its own ports and finds that the configuration messages of Port C1 are optimal, so the port is determined as the root port, and its configuration messages remain unchanged. DeviceC calculates the configuration message <0, 10, 2, Port C2> of the designated port for Port C2 according to the configuration message and path cost of the root port, and then matches the configuration message of Port C2 itself < 1, 0, 1, Port B2> compare and find that the calculated configuration message is better, so Port C2 is determined as the designated port, and its configuration message is also replaced with the calculated configuration message.	Root port C1: <0, 0, 0, Port A2> Designated port C2: <0, 10, 2, Port C2>
	Port C2 received the updated configuration message <0, 5, 1, Port B2> from Port B2, and found that it is better than its own configuration message <0, 10, 2, Port C2> , so update your own configuration message. Port C1 receives the configuration message <0, 0, 0, Port A2> periodically sent by Port A2, and finds that it is the same as its own configuration message, so it discards it.	Port C1 :<0, 0, 0, Port A2> Port C2: <0, 5, 1, Port B2>
	DeviceC compares the root path cost 10 of Port C1 (the root path cost 0 in the received configuration message + the path cost 10 of the link where the port is located) and the root path cost 9 of Port C2 (received The root path cost in the configuration message is 5 + the path cost of the link where this port is located 4). It is found that the latter is smaller, so the configuration message of Port C2 is better, so Port C2 is determined as the root port, and its configuration message remains unchanged. DeviceC calculates the configuration message <0, 9, 2, Port C1> of the designated port for Port C1 according to the configuration message and path cost of the root port, and then matches the configuration message of Port C1 itself < 0, 0, 0, Port A2> compared, and found that its own configuration message is better, so Port C1 is blocked, and its configuration message remains unchanged. From now on, Port C1 will no longer forward data until a new situation that triggers spanning tree calculation occurs, such as the link between DeviceB and DeviceC is down.	Blocking port C1: <0, 0, 0, Port A2> Root port C2: <0, 5, 1, Port B2>

After the topology is stable, the root bridge still sends configuration BPDUs according to the interval specified by the Hello Timer. Non-root bridge devices receive configuration BPDUs from the root port and forward them through the designated port. If it receives a configuration BPDU with a higher priority than itself, the non-root bridge device will update the configuration BPDU information stored on its corresponding port according to the information carried in the received configuration BPDU.

STP topology change

The STP topology change processing process is shown in the figure below.

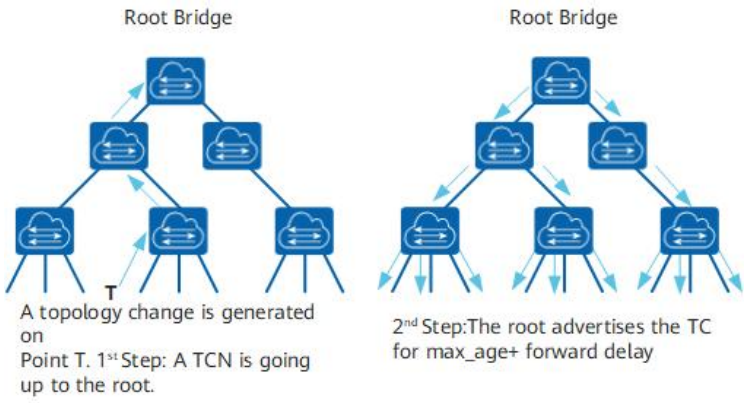


Figure 2- 10 TCN sending and TC flooding

After the network topology changes, the downstream device will continuously send TCN BPDUs to the upstream device.

After the upstream device receives the TCN BPDU message from the downstream device, only the designated port processes the TCN BPDU message. Other ports may also receive TCN BPDUs, but will not process them.

The upstream device will set the TCA bit of the Flags in the configuration BPDU message to 1, and then send it to the downstream device to tell the downstream device to stop sending TCN BPDU messages.

The upstream device copies a TCN BPDU and sends it to the root bridge.

Repeat steps 1, 2, 3, and 4 until the root bridge receives a TCN BPDU.

The root bridge sets the TC and TCA bits of the Flags in the configuration BPDU message to 1 and sends it to notify the downstream device to delete the bridge MAC address entry directly.

12.1.2. RSTP

12.1.2.1. Requirement Background

The 802.1w standard released by the IEEE in 2001 defines the Rapid Spanning Tree Protocol (RSTP), which is based on the STP protocol and makes more detailed modifications and additions to the original STP protocol.

STP deficiencies

Although the STP protocol can solve the loop problem, the slow convergence of the network topology affects the quality of user communication. If the topology in the network changes frequently, the network will also lose connectivity frequently, resulting in frequent interruption of user communication, which is unbearable for users.

The disadvantages of STP are as follows:

STP does not distinguish port status and port role in detail, which is not conducive to beginners' learning and deployment.

The quality of a network protocol often depends on whether the protocol distinguishes each situation carefully.

From the user's point of view, there is no difference between the Listening, Learning and Blocking states, and they also do not forward user traffic.

From the perspective of usage and configuration, the most essential difference between ports is not the state of the port, but the role the port plays.

The root port and the designated port can both be in the Listening state or both in the Forwarding state.

The STP algorithm is a passive algorithm. It relies on the timer to wait to determine the topology change,

and the convergence speed is slow.

The STP algorithm requires that in a stable topology, the root bridge actively sends out configuration BPDUs, and other devices process them and spread them throughout the STP network. This is also one of the main reasons for slow topology convergence.

RSTP improves STP

According to the insufficiency of STP, RSTP deletes 3 port states, adds 2 new port roles, and fully decouples port attributes according to state and role; in addition, RSTP also adds some corresponding Enhanced features and protection measures to achieve network stability and rapid convergence, simplifies the understanding and deployment of Spanning Tree Protocol by adding port roles.

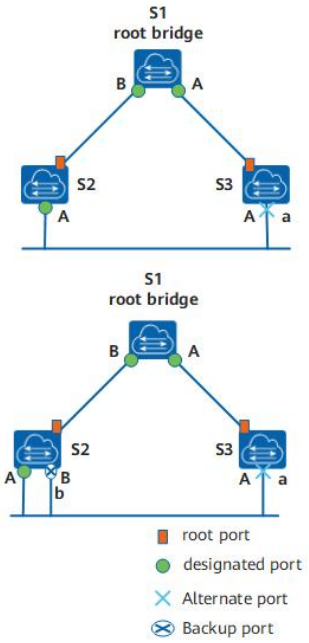


Figure2- 11 Port Role Schematic

As shown in the figure above, there are four types of RSTP port roles: root port, designated port, alternate port and backup port.

The functions of the root port and the designated port are the same as those defined in the STP protocol.

The description of the alternate port and the backup port is as follows:

From the perspective of configuring BPDU sending:

Alternate port is a port that is blocked due to learning configuration BPDUs sent by other bridges.

The backup port is the port that is blocked due to learning the configuration BPDUs sent by itself.

From a user traffic perspective:

The Alternate port provides an alternate switchable path from the designated bridge to the root, acting as a backup port for the root port.

The Backup port acts as a backup of the designated port, providing another backup path from the root bridge to the corresponding network segment.

The process of assigning roles to all ports in an RSTP network is the process of topology convergence.

Repartition of port state

RSTP state specification reduces the original 5 states to 3. Divided according to whether the port forwards user traffic and learns the MAC address:

If the user traffic is not forwarded and the MAC address is not learned, the port state is Discarding state.

If the user traffic is not forwarded but the MAC address is learned, the port state is the Learning state.

If both user traffic is forwarded and the MAC address is learned, the port state is the Forwarding state.

As shown in Table2-9, the new port state is compared with the port state specified by STP. Port status and port role are not necessarily related. The table shows the port status that various port roles can have.

Table2-9 STP and RSTP Port Status Role Correspondence Table

STP port status	RSTP port status	The role of the port in the topology
Forwarding	Forwarding	Include root port, designated port
Learning	Learning	Include root port, designated port
Listening	Discarding	Include root port, designated port
Blocking	Discarding	Include Alternate port, Backup port
Disabled	Discarding	Include Disable port

The change of the configuration BPDU format makes full use of the Flag field in the STP protocol message and clarifies the port role.

In addition to ensuring that the format of the BPDU is basically the same as the STP format, RSTP has made some minor changes:

Type field, the configuration BPDU type is no longer 0 but 2, so the device running STP will discard the RSTP configuration BPDU when it receives it.

Flags field, using the original reserved middle 6 bits, so the changed configuration BPDU is called RST BPDU, as shown in the following figure.

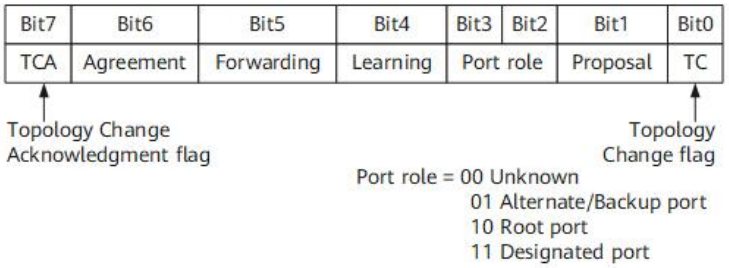


Figure2-12 RSTP Flag field format

- The processing of configuration BPDUs has changed

■ Transmission frequency of configuration BPDUs

After the topology is stable, the root bridge sends configuration BPDUs at the interval specified by the Hello Timer. Other non-root bridge devices will trigger configuration BPDUs after receiving the configuration BPDUs sent by the upstream device. This method makes the calculation of the STP protocol complicated and slow. RSTP has been improved, that is, after the topology is stable, no matter whether the non-root bridge device receives the configuration BPDU from the root bridge or not, the non-root bridge device still follows the interval specified by Hello Timer. Sending a configuration BPDU, this behavior is entirely autonomous for each device.

■ Shorter BPDU timeout

If a port does not receive a configuration BPDU from an upstream device within 3 consecutive Hello Time, the device considers that the negotiation with this neighbor has failed. Instead of waiting for a Max Age like STP.

■ Process inferior BPDUs

When a port receives an RST BPDU from an upstream designated bridge, the port will compare its own stored RST BPDU with the received RST BPDU.

If the priority of the RST BPDU stored by the port is higher than that of the received RST BPDU, the port will directly discard the received RST BPDU and immediately respond to its own stored RST BPDU. When the upstream device receives the RST BPDU responded by the downstream device, the upstream device will immediately update its stored RST BPDU according to the corresponding fields in the received RST BPDU.

Therefore, RSTP processing inferior BPDUs no longer relies on any timer to solve topology convergence through timeout, thus speeding up topology convergence.

- fast convergence

■ Proposal/Agreement mechanism

After a port is elected as the designated port, in STP, the port will wait at least one Forward Delay (Learning) time before transitioning to the Forwarding state. In RSTP, this port will first enter the Discarding state, and then quickly enter the Forward state through the Proposal/Agreement mechanism. This mechanism must be used on point-to-point full-duplex links.

Proposal/Agreement mechanism is referred to as P/A mechanism.

■ Root port fast switching mechanism

If a root port in the network fails, the optimal alternate port in the network will become the root port and enter the Forwarding state. Because there must be a designated port on the network segment connected through this alternate port that can lead to the root bridge.

Introduction of edge ports

In RSTP, if a designated port is located at the edge of the entire network, that is, it is no longer connected to other switching devices, but directly connected to terminal devices. This port is called an edge port.

The edge port does not receive and process configuration BPDUs, and does not participate in RSTP operations. It can go to the Forwarding state directly from Disable without experiencing delay, just like disabling STP on the port. But once the edge port receives the configuration BPDU, it loses the edge port attributes, becomes a normal STP port, and recalculates the spanning tree, which causes network flapping.

- protection function

The protection functions provided by RSTP are shown in the table below.

Table2- 10 Protection function

Protection function	Scene	Principle
BPDU Protection	On switching devices, the ports directly connected to non-switching devices such as user terminals (such as PCs) or file servers are usually configured as edge ports. Normally, edge ports will not receive RST BPDUs. If someone forges an RST BPDU to maliciously attack a switching device, when an edge port receives an RST BPDU, the switching device will	After the BPDU protection function is enabled on the switching device, if the edge port receives an RST BPDU, the edge port will be error-down, but the edge port attributes will remain unchanged, and the network management system will be notified at the same time.

Protection function	Scene	Principle
	automatically set the edge port as a non-edge port and recalculate the spanning tree, causing network flapping .	
Root Protection	Due to the misconfiguration of the maintenance personnel or the malicious attacks in the network, the legitimate root bridges in the network may receive RST BPDUs with higher priority, so that the legitimate root bridges lose their root status, thus causing the network topology Incorrect change of structure. This illegal topology change will cause traffic that should have passed through the high-speed link to be pulled to the low-speed link, causing network congestion.	For the designated port with root protection function enabled, its port role can only remain as designated port. Once a designated port with the root protection function enabled receives a RST BPDU with a higher priority, the port state will enter the Discarding state and will no longer forward packets. After a period of time (usually twice the Forward Delay), if the port has not received RST BPDUs with higher priority, the port will automatically return to the normal Forwarding state. Description: Root protection can only be configured on designated ports.

12.1.2.2. Technical Principles

Proposal/Agreement mechanism

The purpose is to make a designated port enter the Forwarding state as soon as possible. As shown in the figure below, a new link has been added between the root bridge S1 and S2. In the current state, the other ports p2 of S2 are alternate ports, p3 is the designated port and is in the forwarding state, and p4 is the edge port.

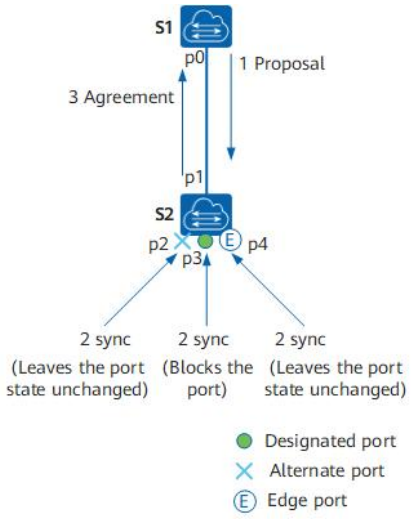


Figure2- 13 Proposal/Agreement Process Diagram

After the new link is successfully connected, the P/A mechanism negotiation process is as follows:

1. Both ports p0 and p1 will immediately become designated ports and send RST BPDUs.
2. The p1 port of S2 received a better RST BPDU, and immediately realized that it would become the root port, not the designated port, and stopped sending RST BPDUs.
3. P0 of S1 enters the Discarding state, so the proposal is set to 1 in the sent RST BPDU.

4. S2 receives the RST BPDU with proposal sent by the root bridge, and starts to set all its own ports into the sync variable.
5. p2 has been blocked and the state remains unchanged; p4 is an edge port and does not participate in the operation; so only the non-edge designated port p3 needs to be blocked.
6. After both p2 and p3 enter the Discarding state, the synced variable of the port is set, and the synced of the root port p1 is also set, so the response RST BPDU with the Agreement bit set is returned to S1. This RST BPDU carries the same information as the BPDU sent by the root bridge just now, except that the Agreement bit is set (the Proposal bit is cleared).
7. When S1 determines that this is a response to the proposal just sent, port p0 immediately enters the Forwarding state.

The downstream device continues the P/A negotiation process.

In fact, for STP, the selection of the designated port can be completed very quickly. The main speed bottleneck is: in order to avoid loops, it is necessary to wait long enough to make the port status of the entire network all determined, that is Says that all ports must wait for at least one Forward Delay before forwarding. The main purpose of RSTP is to eliminate this bottleneck by blocking its own non-root ports to ensure that there will be no loops. Using the P/A mechanism speeds up the upstream port's transition to the Forwarding state.

RSTP topology change processing

There is only one criterion for detecting topology changes in RSTP: a non-edge port migrates to the Forwarding state.

Once a topology change is detected, the following processing will be performed:

Start a TC While Timer for all non-edge designated ports of this switching device. The timer value is twice the Hello Time.

During this time, clear the MAC addresses learned on all ports.

At the same time, a RST BPDU is sent out from the non-edge port, with TC set. Once the TC While Timer times out, stop sending RST BPDUs.

After receiving the RST BPDU, other switching devices clear all ports to learn the MAC address, except the port that received the RST BPDU. Then also start the TC While Timer for all non-edge designated ports and root ports, and repeat the above process.

In this way, a flood of RST BPDUs will occur in the network.

RSTP and STP interoperability

RSTP can interoperate with STP, but the advantages of RSTP such as fast convergence will be lost at this time.

When a network segment has both STP and RSTP switching devices, the STP switching device will ignore RSTP BPDUs. The switching device running RSTP receives the configuration BPDU sent by the switching device running STP on a port, and after two Hello Time times, it switches its port to STP working mode and sends the configuration BPDU , thus enabling interoperability.

12.1.3. MSTP

12.1.3.1. Requirement Background

RSTP has been improved on the basis of STP to achieve rapid network topology convergence. But RSTP and STP still have the same defect: because all VLANs in the LAN share a spanning tree, load

balancing of data traffic between VLANs cannot be achieved, and the link will not carry any traffic after it is blocked. traffic, resulting in wasted bandwidth, and may also cause some VLAN packets to fail to be forwarded.

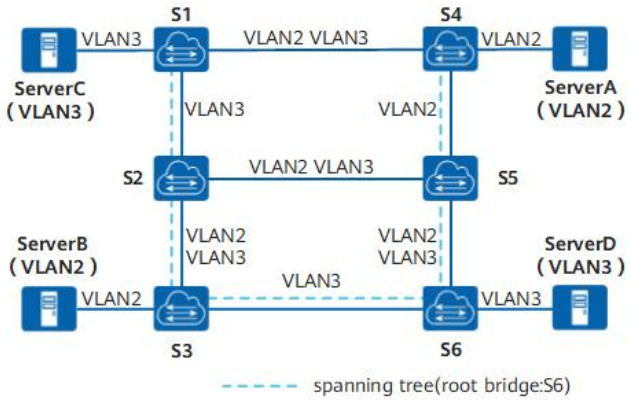


Figure2- 14 STP/RSTP defect diagram

In the network shown above, STP or RSTP is applied in the local area network. The spanning tree structure is represented by a dotted line in the figure, and S6 is the root switching device. The links between S2 and S5 and between S1 and S4 are blocked. Except for the links marked 'VLAN2' or 'VLAN3' in the figure, the corresponding VLAN packets are allowed to pass through. The packets of VLAN2 and VLAN3 are not allowed to pass through.

ServerA and ServerB belong to VLAN2, because the link between S2 and S5 is blocked, and the link between S3 and S6 does not allow packets from VLAN2 to pass, so ServerA and ServerB cannot communicate with each other. communicate with each other.

In order to make up for the shortcomings of STP and RSTP, the 802.1S standard released by IEEE in 2002 defines MSTP. MSTP is compatible with STP and RSTP, which can not only converge quickly, but also provide multiple redundant paths for data forwarding to achieve load balancing of VLAN data during data forwarding.

A switching network is divided into multiple regions through MSTP, and multiple spanning trees are formed in each region, and the spanning trees are independent of each other. Each spanning tree is called a Multiple Spanning Tree Instance (MSTI), and each region is called an MST Region (MST Region: Multiple Spanning Tree Region).

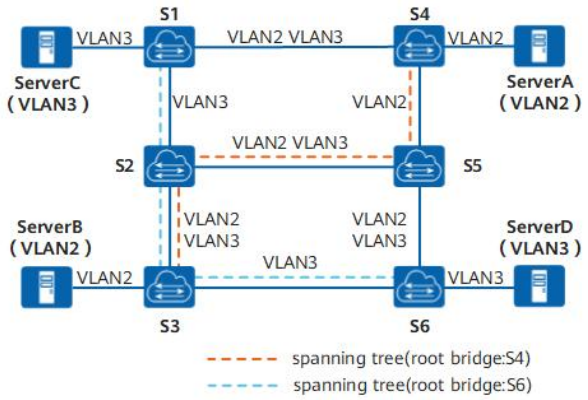


Figure2- 15 Multiple spanning trees in the MST region

As shown in the figure above, MSTP connects VLAN and MSTI by setting the VLAN mapping table (that is, the correspondence table between VLAN and MSTI). Each VLAN can only correspond to one MSTI, that is, the data of the same VLAN can only be transmitted in one MSTI, and one MSTI may correspond

to multiple VLANs.

After calculation, two spanning trees are finally generated:

MSTI1 uses S4 as the root switching device to forward packets of VLAN2.

MSTI2 uses S6 as the root switching device to forward packets of VLAN3.

In this way, all VLANs can communicate with each other, and packets of different VLANs are forwarded along different paths, realizing load balancing.

12.1.3.2. Basic Concepts

MSTP Network

As shown in the figure below, the MSTP network contains one or more MST regions (MST Regions), and each MST Region contains one or more MSTIs. MSTI is composed of switching equipment running STP/RSTP/MSTP. MSTI is a tree network formed by all switching equipment running STP/RSTP/MSTP after MSTP protocol calculation.

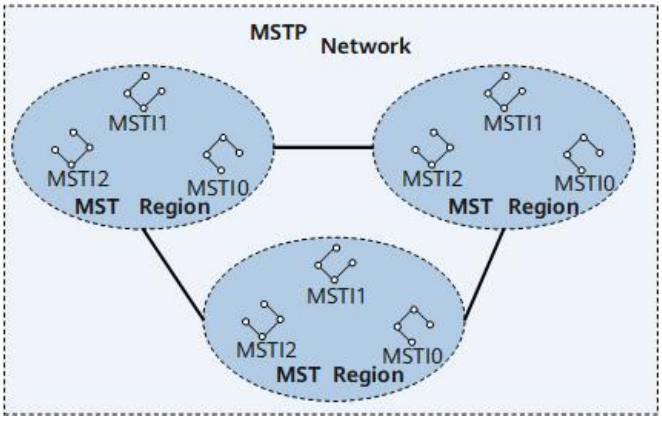


Figure2- 16 MSTP Network Diagram

MST Region

The MST region is a Multiple Spanning Tree Region, which consists of multiple switching devices in the switching network and the network segments between them. Devices in the same MST region have the following characteristics:

- MSTP is enabled.
- Has the same region name.
- Has the same VLAN to Spanning Tree instance mapping configuration.
- Has the same MSTP revision level configuration.

A LAN can have multiple MST regions, and the MST regions are physically connected directly or indirectly. Users can divide multiple switching devices into the same MST region through MSTP configuration commands.

As shown in the figure below, MST Region D0 consists of switching devices S1, S2, S3 and S4, and there are 3 MSTIs in the region.

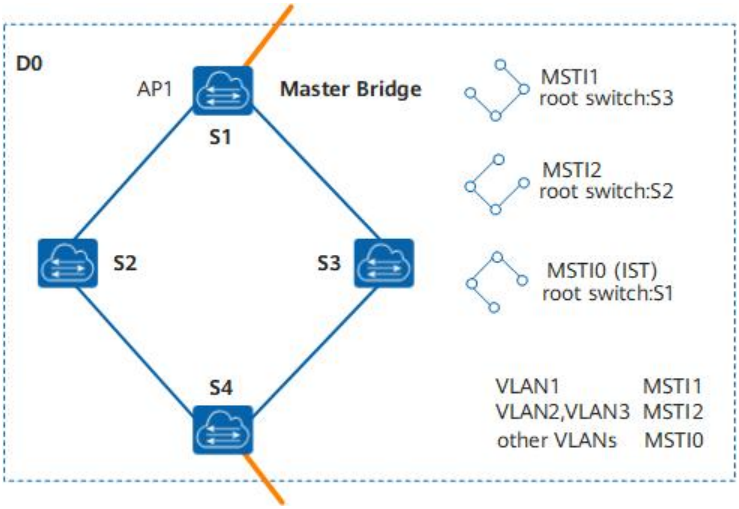


Figure2- 17 Basic Concept Diagram of MST Region

VLAN mapping table

VLAN mapping table is an attribute of MST region, which describes the mapping relationship between VLAN and MSTI.

As shown in the figure above, the VLAN mapping table of MST region D0 is:

VLAN1 maps to MSTI1

VLAN2 and VLAN3 are mapped to MSTI2

The rest of the VLANs are mapped to MSTI0

Regional Root

Regional Root is divided into IST (Internal Spanning Tree) regional root and MSTI regional root.

The IST regional root is shown in Figure2- 19. In B0, C0 and D0, the switching device closest to the total root (CIST Root) in the IST spanning tree is the IST regional root.

Multiple spanning trees can be generated in one MST region, and each spanning tree is called an MSTI. The MSTI regional root is the root of each multiple spanning tree instance. As shown in Figure2- 18, different MSTIs in the region have their own regional root.

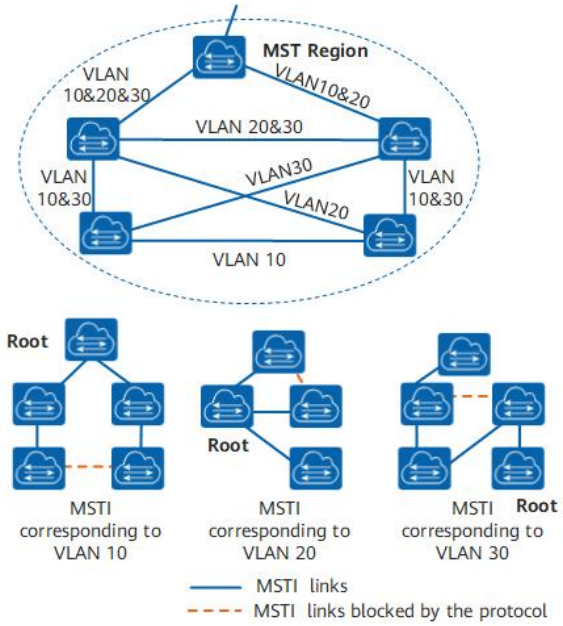


Figure2- 18 MSTI basic concept diagram

MSTIs are independent of each other, and MSTIs can correspond to one or more VLANs. But a VLAN can only correspond to one MSTI.

Master Bridge

The Master Bridge, also known as the IST Master, is the switching device closest to the root in the region. S1 as in

Figure2- 17.

If the master root is in the MST region, then the master root is the master bridge for this region.

CIST Root

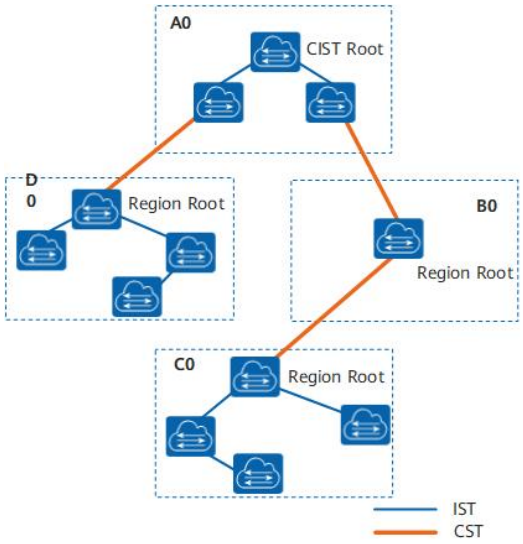


Figure2- 19 MSTP network basic concept diagram

As shown above, the total root is the root bridge of CIST (Common and Internal Spanning Tree). The total root is a device in area A0.

CST

Common Spanning Tree (CST) is a spanning tree that connects all MST regions in a switched network.

If each MST region is regarded as a node, the CST is a spanning tree calculated and generated by these nodes through the STP or RSTP protocol.

As shown in Figure2- 19, thicker lines connect fields to form CST.

IST

Internal Spanning Tree IST (Internal Spanning Tree) is a spanning tree in each MST region.

IST is a special MSTI, the ID of MSTI is 0, usually called MSTI0.

IST is a fragment of CIST in the MST region.

As shown in Figure2- 19, the thinner lines in the region connect all switching devices in the region to form the IST.

CIST

Common and Internal Spanning Tree CIST is calculated and generated by STP or RSTP protocol, connecting all switching devices in a single spanning tree in a switching network.

As shown in Figure2- 19, the IST plus CST of all MST regions constitutes a complete spanning tree, namely CIST.

SST

There are two cases of forming a single spanning tree SST (Single Spanning Tree):

A switching device running STP or RSTP can only belong to one spanning tree.

There is only one switching device in the MST region, and this switching device constitutes a single spanning tree.

As shown in Figure2-19, the switching device in B0 is a single spanning tree.

Port role

MSTP adds 2 new ports based on RSTP. MSTP has 7 port roles: root port, designated port, alternate port, backup port, edge port, master port and regional edge port.

The functions of root port, designated port, alternate port, backup port and edge port are the same as those defined in RSTP protocol. All port roles defined in MSTP are shown in the following table.

Table2-11 Port Role

Port Role	Description
Root port	On a non-root bridge, the port closest to the root bridge is the root port of this switch. The root switch device has no root port. The root port is responsible for forwarding data to the root of the tree. As shown in Figure2-20, S1 is the root bridge, CP1 is the root port of S3, and BP1 is the root port of S2.
Designated port	For a switching device, its designated port is the port that forwards BPDUs to downstream switching devices. As shown in Figure2-20, AP2 and AP3 are designated ports of S1, and CP2 is designated port of S3.
Alternate port	From the perspective of sending configuration BPDUs, the alternate port is a port that is blocked by learning configuration BPDUs sent by other bridges. From a user traffic perspective, the Alternate port provides another switchable path from the designated bridge to the root, acting as a backup port to the root port. As shown in Figure2-20, BP2 is an alternate port.
Backup port	From the perspective of sending configuration BPDUs, the Backup port is a port that is blocked by learning the configuration BPDUs sent by itself. From the perspective of user traffic, the Backup port acts as a backup of the designated port, providing another backup path from the root node to the leaf node. As shown in Figure2-20, CP3 is the backup port.
Master port	The master port is the port on the shortest path among all paths connecting the MST region to the general root. It is the port on the switching device that connects the MST region to the general root. The master port is the only way for packets in the region to go to the master root. The master port is a special regional edge port. The role of the master port on the CIST is the root port, and the role of the master port on other instances is the master port. As shown in Figure2-21, the switching devices S1, S2, S3, S4 and the links between them constitute an MST region, and the port AP1 of the S1 switching device is in all ports in the region to the total root The path cost is the least, so AP1 is the master port.
Regional Edge Port	A regional edge port is a port located at the edge of an MST region and connected to other MST regions or SSTs. When performing MSTP calculations, the role of the regional edge port on the MSTI is the same as the role of the CIST instance. That is, if the role of the edge port on the CIST instance is the Master port (the port on the shortest path among all paths connecting the region and the general root), then its role on all MSTIs in the region is also the Master port. As shown in Figure2-21, AP1, DP1 and DP2 in the MST region are directly connected to other regions, and they are all regional edge ports in this MST region. The role of regional edge ports on spanning tree instances is the same as on CIST. For example, in Figure2-21, AP1 is the regional edge port, and its role in the CIST is the master port, then the role of AP1 in all spanning tree instances in the MST region is the master port.

Port Role	Description
Edge Port	If the designated port is located at the edge of the entire region and is no longer connected to any switching device, this port is called an edge port. Edge ports are generally connected directly to user terminal equipment. After the MSTP function is enabled on a port, the automatic edge port detection function will be enabled by default. When the port does not receive BPDUs within (2 × Hello Timer + 1) seconds, the port will be automatically set to Edge port, otherwise set to non-edge port.

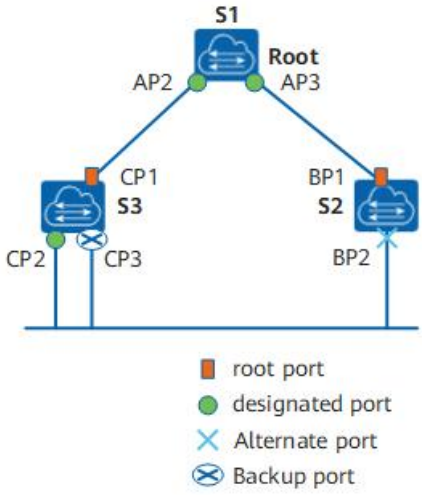


Figure2- 20 Root Port, Designated Port, Alternate Port and Backup Port Schematic

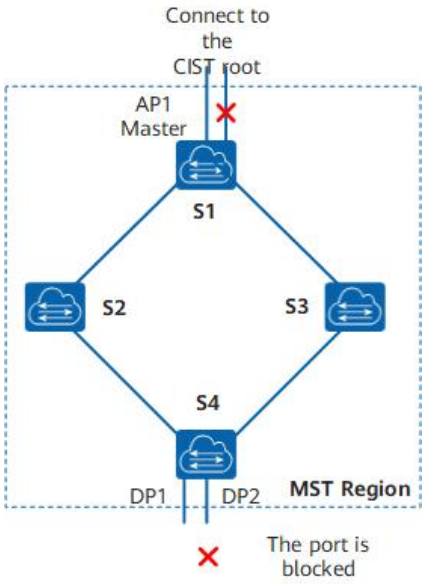


Figure2- 21 Master Port and Regional Edge Port Diagram

MSTP port status

The port state defined by MSTP is the same as that defined in the RSTP protocol, as shown in the following table.

Table2- 12 Port Status

Port Status	Description
Forwarding	In this state, the port both forwards user traffic and receives/sends BPDUs.
Learning	This is a transitional state. Under Learning, the switching device will build a MAC

Port Status	Description
	address table according to the received user traffic, but will not forward the user traffic, so it is called the learning state. The port in the Learning state receives/sends BPDUs and does not forward user traffic.
Discarding	The port in Discarding state only receives BPDU packets.

Port status and port role are not necessarily related. The following table shows the port status that various port roles can have.

Table2- 13 Port Status and Port Role Correspondence Table

Port Status	Root Port/Master Port	Designated port	Regional Edge Port	Alternate port	Backup port
Forwarding	Yes	Yes	Yes	No	No
Learning	Yes	Yes	Yes	No	No
Discarding	Yes	Yes	Yes	Yes	Yes

Yes: indicates the port support status. No: indicates that the port is not supported.

12.1.3.3. Message Format

MSTP uses Multiple Spanning Tree Bridge Protocol Data Unit (MST BPDU) as the basis for spanning tree calculation. MST BPDUs are used to calculate spanning tree topology, maintain network topology, and communicate topology change records.

The difference between configuration BPDUs defined in STP, RST BPDUs defined in RSTP, MST BPDUs defined in MSTP, and TCN BPDUs is shown in the following table.

Table2- 14 Four BPDU Difference Comparison

Version	Type	Name
0	0x00	Configuration BPDU
0	0x80	TCN BPDU
2	0x02	RST BPDU
3	0x02	MST BPDU

MSTP message format

The structure of the MST BPDU is shown in the figure below.

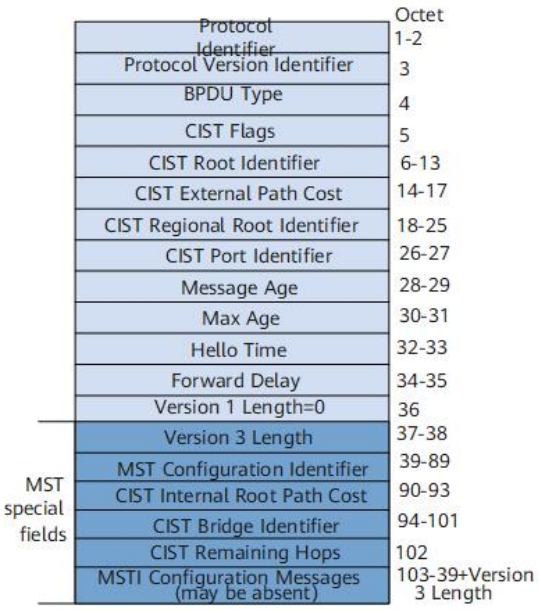


Figure2- 22 MST BPDU structure

Whether it is an intra-region MST BPDU or an inter-region MST BPDU, the first 36 bytes are the same as the RST BPDU.

Starting from the 37th byte is an MSTP-specific field. The last MSTI configuration information field consists of several MSTI configuration information groups concatenated.

The main information in the MST BPDU is shown in the table below.

Table2- 15 Main information description in MST BPDU

Field Content	bytes	Description
Protocol Identifier	2	Protocol identifier.
Protocol Version Identifier	1	Protocol version identifier, STP is 0, RSTP is 2, MSTP is 3.
BPDU Type	1	BPDU type: 0x00: Configuration BPDU of STP 0x80: STP TCN BPDU (Topology Change Notification BPDU) 0x02: RST BPDU (Rapid Spanning-Tree BPDU) or MST BPDU (Multiple Spanning-Tree BPDU)
CIST Flags	1	CIST flag field.
CIST Root Identifier	8	CIST 's total root exchange device ID.
CIST External Path Cost	4	The CIST external path cost refers to the cumulative path cost from the MST region to which this switching device belongs to the MST region to which the CIST root switching device belongs. CIST external path cost is calculated based on link bandwidth.
CIST Regional Root Identifier	8	Indicates the ID of the regional root switching device on the CIST, that is, the IST master ID. If the root is in this region, the CIST Regional Root Identifier is the same as the CIST Root Identifier.

Field Content	bytes	Description
CIST Port Identifier	2	The designated port ID of this port in IST.
Message Age	2	BPDU lifetime.
Max Age	2	The maximum lifetime of a BPDU packet. If the timeout expires, the link to the root switching device is considered to be faulty.
Hello Time	2	Hello timer, the default is 2 seconds.
Forward Delay	2	Forward Delay timer, the default is 15 seconds.
Version 1 Length	1	Version1 BPDU length, the value is fixed to 0.
Version 3 Length	2	Version3 length of BPDU.
MST Configuration Identifier	51	MST configuration identifier, indicating the label information of the MST region, including 4 fields.
CIST Internal Root Path Cost	4	CIST internal path cost refers to the cumulative path cost from this port to the IST Master switching device. CIST internal path cost is calculated based on link bandwidth.
CIST Bridge Identifier	8	Indicates the ID of the designated switching device on the CIST.
Indicates the remaining hops of the BPDU in the CIST.	1	The remaining hops of the BPDU in the CIST.
MSTI Configuration Messages(may be absent)	16	MSTI configuration information. The configuration information of each MSTI occupies 16 bytes. If there are n MSTIs, it occupies n×16 bytes.

The maximum number of BPDUs that the port can send within each Hello Time is configurable

Hello Time is used by the Spanning Tree Protocol to periodically send configuration messages to maintain the stability of the spanning tree. If the switching device does not receive a BPDU within a period of time, it will recalculate the spanning tree due to message timeout.

When a switching device becomes the root switching device, the switching device will send BPDUs at the interval of the set value. The non-root switching device adopts the Hello Time value set by the root switching device.

12.1.3.4. Topology Calculation

MSTP rationale

MSTP can divide the entire Layer 2 network into multiple MST regions, and CST is generated between each region through calculation. In the region, multiple spanning trees are generated by calculation, and each spanning tree is called a multiple spanning tree instance. where instance 0 is called IST, and the other multiple spanning tree instances are MSTI. MSTP, like STP, uses configuration messages to

calculate spanning tree, but the configuration messages carry the configuration information of MSTP on the device.

priority vector

Both MSTI and CIST are calculated from priority vectors, which are included in the MST BPDU. The switching devices exchange MST BPDUs with each other to generate MSTI and CIST.

- Introduction to Priority Vectors

The priority vector participating in the CIST calculation is:

< Root Switch ID, External Path Cost, Regional Root ID, Internal Path Cost, Designated Switch ID, Designated Port ID, Receive Port ID >

The priority vector participating in MSTI calculation is:

< Regional Root ID, internal path cost, designated switching device ID, designated port ID, receiving port ID >

The priority of the vectors in parentheses decreases from left to right.

The following table explains each priority vector.

Table2-16 Vector Description

Vector Name	Description
Root Switch Device ID	The root switch ID is used to select the root switch in CIST. Root Switch ID = Priority(16bits) + MAC(48bits). Where Priority is the priority of MSTI0.
External Path Cost (ERPC)	Path cost from the regional root of CIST to the total root. The external path cost stored on all switching devices in the MST region is the same. If the CIST root switching device is in the region, the external path cost stored on all switching devices in the region is 0.
Regional Root ID	Regional Root ID is used to select the regional root in MSTI. Regional Root ID = Priority(16bits) + MAC(48bits). Where Priority is the priority of MSTI0.
Internal Path Cost (IRPC)	The path cost of this bridge to reach the regional root. The internal path cost stored by the regional edge port is greater than the internal path cost stored by the non-regional edge port.
Specify switch device ID	The designated switching device of the CIST or MSTI instance is the nearest upstream bridge from this bridge to the regional root. If this bridge is the general root or regional root, specify the switching device as itself.
Specify port ID	Specify the port on the switching device that is connected to the root port on this device. Port ID = Priority(4 digits) + Port number(12 digits). The port priority must be an integer multiple of 16.
Receive port ID	The port that received the BPDU. Port ID = Priority(4 digits) + Port number(12 digits). The port priority must be an integer multiple of 16.

- Comparison Principle

Comparing the same vector, the vector with the smallest value has the highest priority.

The priority vector comparison principle is as follows.

First, compare the root swap device ID.

If the root switch device ID is the same, then compare the external path cost.

If the external path cost is the same, then compare the regional root ID.

If the regional root ID is still the same, compare the internal path costs.

If the internal path is still the same, then compare the designated switch ID.

If the designated switch device ID is still the same, then compare the designated port ID.

If the designated port ID is still the same, then compare the receiving port ID.

If the configuration message contained in the BPDU received by the port is better than the configuration message saved on the port, the configuration message originally saved on the port is replaced by the newly received configuration message. The port also updates the global configuration message saved by the switching device. On the contrary, the newly received BPDU is discarded.

- Calculation of CIST

After comparing the configuration messages, select a switching device with the highest priority in the entire network as the root of the CIST. MSTP generates IST through calculation in each MST region; at the same time, MSTP treats each MST region as a single switching device, and generates CST between MST regions through calculation. CST and IST constitute the CIST of the entire switching device network.

- Calculation of MSTI

In the MST region, MSTP generates different spanning tree instances for different VLANs according to the mapping relationship between VLANs and spanning tree instances. Each spanning tree is calculated independently, and the calculation process is similar to that of STP.

Characteristics of MSTI:

Each MSTI calculates its own spanning tree independently and does not interfere with each other.

The spanning tree calculation method of each MSTI is basically the same as that of STP.

The spanning tree for each MSTI can have different roots and different topologies.

Each MSTI sends BPDUs within its own spanning tree.

The topology of each MSTI is determined by command configuration.

The spanning tree parameters can be different for each port on different MSTIs.

Each port can have different roles and states on different MSTIs.

In a network running MSTP protocol, a VLAN packet will be forwarded along the following path:

In the MST region, forward along its corresponding MSTI.

Forwarding along CST between MST regions.

- MSTP handling of topology changes

MSTP topology change processing is similar to RSTP topology change processing, please refer to RSTP topology change processing.

12.1.3.5. Fast Convergence

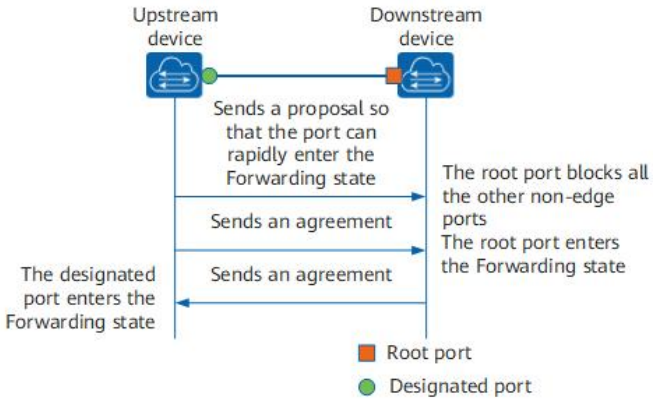


Figure2- 23 P/A of MSTP Mechanism

As shown in the figure above, in MSTP, the P/A mechanism works as follows:

The upstream device sends a Proposal message requesting fast migration. After the downstream device receives it, it sets the port connected to the upstream device as the root port, and blocks all non-edge ports.

The upstream device continues to send Agreement packets. After the downstream device receives it, the root port changes to the Forwarding state.

The downstream device responds to the Agreement message. After the upstream device receives it, it sets the port connected to the downstream device as the designated port, and the designated port enters the Forwarding state.

12.1.4. Standard Specification

The protocol specifications related to spanning tree are:

- IEEE 802.1D: Media Access Control (MAC) Bridges
- IEEE 802.1w:Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration
- IEEE 802.1s: Virtual Bridged Local Area Networks—Amendment 3: Multiple Spanning Trees

12.2. Configuring

12.2.1. Default Configuration

Parameters	Default
Working mode	RSTP mode
Status	Global disabled, enabled on all ports
Device priority	32768
Port Priority	128
Calculation method of path cost	Dot1t, the IEEE 802.1t standard
Forward Delay Time	1500 centiseconds (15 seconds)
Hello Time	200 centiseconds (2 seconds)
Max Age Time	2000 centiseconds (20 seconds)

12.2.2. Configure STP Mode and Status

- Configure STP Mode

Command	SWITCH(config)#**spanning-tree mode** <**stp	rstp	mstp**>
Description	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 disabled by default and needs to be re-enabled. Global configuration mode.

- Enable Spanning Tree Protocol

Command	SWITCH(config)#**spanning-tree enable** SWITCH(config)#**no spanning-tree enable**

Description	Enable/disable STP function; default disabled. Global configuration mode.

12.2.3. Configure STP Election Parameters

- Configure Device Priority

Command	SWITCH(config)#**spanning-tree priority** <0-61440> SWITCH(config)#**no spanning-tree priority** SWITCH(config)#**spanning-tree instance** <1-63> **priority** <0-61440> SWITCH(config)**#no spanning-tree instance** <1-63> **priority**
Description	Configure/delete STP system priority; default 32768. Optional configuration. Global configuration mode.

- Configure Port Priority

Command	SWITCH(config-if)#**spanning-tree priority** <0-240> SWITCH(config-if)#**spanning-tree instance** <1-63> **priority** <0-240>
Description	Configure port STP priority; default 128. Optional configuration. Interface configuration mode.

- Configure Port Path Cost

Command	SWITCH(config-if)#**spanning-tree path-cost** <1-200000000> SWITCH(config-if)#**no spanning-tree path-cost**
Description	Configure/reset path cost of port; optional configuration. Interface configuration mode.

12.2.4. Configure Topology Convergence Parameters

- Configure Hello Time

Command	SWITCH(config)#**spanning-tree hello-time** <1-10> SWITCH(config)#**no spanning-tree hello-time**
Description	Configure/reset the BPDU packet period, in seconds; the default is 2s. Optional configuration. Global configuration mode.

- Configure Forward-Delay Time

Command	SWITCH(config)#**spanning-tree forward-time** <4-30> SWITCH(config)#**no spanning-tree forward-time**
Description	Config/reset STP port forwarding state delay time, in seconds; default is 15s. Optional configuration. Global configuration mode.

- Configure Max-Age Time

Command	SWITCH(config)#**spanning-tree max-age** <6-40> SWITCH(config)#**no spanning-tree max-age**
Description	Configure/reset the lifetime of BPDU packets, in seconds; the default is 20s. Optional configuration. 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 – 1.0 seconds), otherwise it may lead to topology instability. The longest path of the STP/RSTP network is affected by this parameter. The default longest path is 20 devices. When there are more than 20 devices, the configuration needs to be modified (forward-delay 21s, max-age 40s can be configured) , the maximum support for the longest path is 40.

	Global configuration mode.

- Configure Max-Hops

Command	SWITCH(config)#**spanning-tree max-hops** <1-40> SWITCH(config)#**no spanning-tree max-hops**
Description	Configure/reset the maximum hop count for BPDU packets; the default is 20. Optional configuration. The longest path of the MSTP network is affected by this parameter. When there are more than 20 devices, the configuration needs to be modified, and the maximum is 40. MSTP is compatible with the max-age function, you need to adjust the max-age parameter at the same time, refer to the corresponding command. Global configuration mode.

12.2.5. Configure Edge Port

- Configure Edge Port

Command	SWITCH(config-if)#**spanning-tree <edgeport | autoedge>** SWITCH(config-if)#**no spanning-tree <edgeport | autoedge>**
Description	Configure/delete the port Edge Port; if configured as edgeport, it means that the device directly connected to the port is not a bridge device and can be forwarded quickly; if configured as autoedge, it means that the port automatically identifies whether it is an edge port according to BPDU; it is disabled by default; Select configuration. Interface configuration mode.

- Open Portfast

Command	SWITCH(config-if)#**spanning-tree portfast** SWITCH(config-if)#**no spanning-tree portfast**
Description	Configure/delete port portfast; the port will be forwarded directly after opening portfast. But the Port Fast Operational State will be disabled due to the receipt of BPDUs, so that it can normally participate in the STP algorithm and forwarding; it is disabled by default; optional configuration. Interface configuration mode.

12.2.6. Configure MST Parameters

- Enter MST Configuration Mode

Command	SWITCH(config)#**spanning-tree mst configuration**
Description	Enter MST configuration mode. Global configuration mode.

- Configure MST VLAN Instance

Command	SWITCH(config-mst)# **instance** <1-63> **vlan** VLANID SWITCH(config-mst)# **no instance** <1-63> **vlan** VLANID
Description	Configure/delete the association between MST instance and VLAN; optional configuration. MST configuration mode.

- Configure MST Region Name

Command	SWITCH(config-mst)#**region** NAME SWITCH(config-mst)#**no region** NAME
Description	Configure/delete MST area name; optional configuration. MST configuration mode.

- Configure MST Version

Command	SWITCH(config-mst)#**revision** <0-65535>
Description	Configure/delete the MST version number, the default is 0; optional configuration. MST configuration mode.

- Configure MSTI Port

Command	SWITCH(config-if)# **spanning-tree instance** <1-63> SWITCH(config-if)# **no spanning-tree instance** <1-63>
Description	Configure/delete port-instance association; optional configuration. By default, when configuring the instance and VLAN relationship, the system will automatically generate port and instance relationship data based on the VLAN and port relationship, and no manual configuration is required. After the instance configuration is ready, if the relationship between ports and VLANs is manually modified, such as adding/exiting all VLANs of an instance to ports, you need to manually maintain the relationship between ports and instances through this command. When there are major configuration changes, it is recommended to automatically generate port and instance data by reconfiguring the instance-VLAN relationship or restarting the device. MST configuration mode.

12.2.7. Configuration Protection Function

- Configure Root Guard

Command	SWITCH(config-if)# **spanning-tree guard root** SWITCH(config-if)#**no spanning-tree guard root**
Description	Configure/delete port root guard; when the root guard function is enabled on an interface, the port role on all instances is forced to be the designated port. Once the port receives configuration information with a higher priority, the root guard The function will put the interface into the blocked state; default closed; optional configuration. Interface configuration mode.

- Configure BPDU Guard

Command	SWITCH(config)#**spanning-tree portfast bpdu-guard** SWITCH(config)#**no spanning-tree portfast bpdu-guard** SWITCH(config-if)#**spanning-tree portfast** SWITCH(config-if)#**no spanning-tree portfast** or: SWITCH(config-if)#**spanning-tree bpdu-guard enable** SWITCH(config-if)#**spanning-tree bpdu-guard disable**
Description	Configure/delete BPDU Guard; after the port has BPDU Guard enabled, if a BPDU is received on the port, it will enter the Error-disabled (blocked) state; optional configuration. Interface configuration mode.

- Configure BPDU Filter

Command	SWITCH(config)#**spanning-tree portfast bpdu-filter** SWITCH(config)#**no spanning-tree portfast bpdu-filter** SWITCH(config-if)#**spanning-tree portfast** SWITCH(config-if)#**no spanning-tree portfast** or: SWITCH(config-if)#**spanning-tree bpdu-filter enable** SWITCH(config-if)#**spanning-tree bpdu-filter disable**
Description	Configure/delete BPDU Filter; after the port opens BPDU Filter, it neither sends BPDU nor receives BPDU message; optional configuration. Interface configuration mode.

- Configure TC Notification

Command	SWITCH(config-if)#**spanning-tree restricted-tcn** SWITCH(config-if)#**no spanning-tree restricted-tcn** SWITCH(config-if)#**spanning-tree instance** <1-63> **restricted-tcn** SWITCH(config-if)#**no spanning-tree instance** <1-63> **restricted-tcn**
Description	Configure/reset the topology change notification limit. After configuration, the port will not forward TC BPDUs, nor refresh the address table; optional configuration. Interface configuration mode.

- Configure Error Port Recover Time

Command	SWITCH(config)#**spanning-tree errdisable-timeout enable** SWITCH(config)#**no spanning-tree errdisable-timeout enable** SWITCH(config)#**spanning-tree errdisable-timeout interval** <10-1000000> SWITCH(config)#**no spanning-tree errdisable-timeout interval**
Description	Configure/reset error port timeout feature. By default, the error port timeout function is not enabled, that is, the error port will never timeout and automatically recover, and must be recovered manually. The timeout unit is seconds, the default is 300 seconds; Optional configuration. Global configuration mode.

12.2.8. Other Optional Configuration

- Configure Transmit-Holdcount

Command	SWITCH(config)#**spanning-tree transmit-holdcount** <1-10> SWITCH(config)#**no spanning-tree transmit-holdcount**
Description	Configure/reset the maximum number of BPDUs sent per second; default is 6. Optional configuration. Global configuration mode.

- Configure Link-Type

Command	SWITCH(config-if)#**spanning-tree link-type <auto | point-to-point | shared>** SWITCH(config-if)#**no spanning-tree link-type**
Description	Configure/reset link type, default is auto. Optional configuration. auto: Automatic setting mode based on the duplex capability of link negotiation, full duplex is point-to-point connection. point-to-point: Enable fast forwarding. shared: Fast Forwarding is disabled. Interface configuration mode.

- Configure Protocol Migration Processing

Command	SWITCH#**clear spanning-tree detected protocols**
Description	Force version checking on all ports. Execution mode.

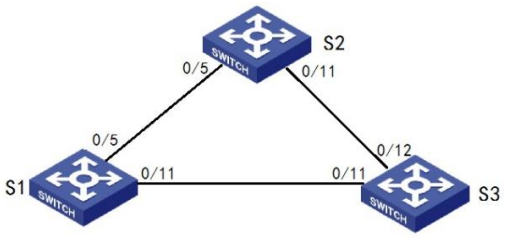
- Configure Logging

Command	SWITCH(config)#**spanning-tree logging** SWITCH(config)#**no spanning-tree logging**
Description	Configure logging. Global configuration mode.

12.3. Examples

12.3.1. Example for Configuring RSTP

Simplified topology:



User P1 goes under S1, P2 goes under S2, P3{ 5> followed by S3;

Requirement description:

When the network is not faulty, the communication between users (ping)is ok

When the network has a single chain failure, the communication between users is still ok

Typical configuration:

S1/S2/S3:

- Enter global configuration mode, configure to use rstp mode, enable stp switch:

Use rstp mode

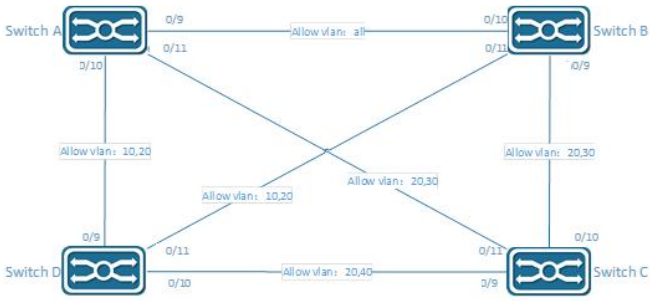
```
spanning-tree mode rstp
```

Enable stp switch

```
spanning-tree enable
```

12.3.2. Example for Configuring MSTP

Simplified topology:



Requirement description:

Users in the same VLAN communicate normally when the network is normal

Improve network reliability through redundant links; for example, for VLAN 10 20, a single link failure between Switch ABDs does not affect the communication of users under it.

Configuration plan:

The devices belong to the same region, the default ‘Default’ region is used here, no additional configuration is required

VLAN 20 is a shared vlan and is directly assigned to CST

Instance	VLAN
0	20
1	10
3	30
4	40

Typical configuration:

Switch A :

Configure VLAN and port

```
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
```

Configure MSTP instance

```
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
```

Enable MSTP

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

Switch B:

Configure VLAN and port

```
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
```

Configure MSTP instance

```
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
```

Enable MSTP

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

Switch C:

Configure VLAN and port

```
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
```

Configure MSTP instance

```
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
```

Enable MSTP

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

Switch D:

Configure VLAN and port

```
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
```

Configure MSTP instance

```
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
```

Enable MSTP

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

12.4. Display Information

- View STP status

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

- View MSTP instance status

```
SWITCH# show spanning-tree mst instance <1-63>
```

13. Configuring MAC Address

13.1. Overview of MAC Address

The MAC address table contains address information that the switch uses to forward traffic between ports. The switch sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the switch forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded.

The MAC address table includes these types of addresses:

Dynamic address: a source MAC address that the switch learns and then ages when it is not in use.

Static address: a manually entered unicast address that does not age and that is not lost when the switch resets.

Filter address: Also a static MAC address, but drop the packet with the specified source or destination unicast filter address.

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN.

Dynamic addresses are source MAC addresses that the switch learns and then ages when they are not in use. You can change the aging time setting for all VLANs or for a specified VLAN. Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being learned.

13.2. Configuring

- Changing MAC Address Aging Time

Command	SWITCH(config)#**mac-address-table aging-time** <0-600> SWITCH(config)#**no mac-address-table aging-time**
Description	Set the length of time that a dynamic entry remains in the MAC address table. The range is 1 to 600 seconds. The default is 300 seconds. You can also enter 0, which disables aging.

- Adding Static MAC Address Entries

Command	SWITCH(config)#**mac-address-table static** MAC_ADDR **vlan** VLANID **interface** IFNAME SWITCH(config)#**no mac-address-table static** MAC_ADDR **vlan** VLANID **interface** IFNAME
Description	Add a static address to the MAC address table. MAC_ADDR: specify the destination MAC unicast address to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface. VLANID: specify the VLAN for which the packet with the specified MAC address is received, Valid VLAN IDs are 1 to 4094. IFNAME: specify the interface to which the received packet is forwarded, Valid interfaces include physical ports or port channels.

- Adding Filter MAC Address Entries

Command	SWITCH(config)#**mac-address-table filter** MAC_ADDR **vlan** VLANID SWITCH(config)#**no mac-address-table filter** MAC_ADDR **vlan** VLANID
Description	Add a filter address to the MAC address table. VLANID: specify the VLAN for which the packet with the specified MAC address is received, Valid VLAN IDs are 1 to 4094. IFNAME: specify the interface to which the received packet is dropped, Valid interfaces include physical ports or port channels.

- Clearing Dynamic MAC Address Entries

Command	SWITCH#**clear mac-address-table dynamic** SWITCH#**clear mac-address-table dynamic vlan** VLANID SWITCH#**clear mac-address-table dynamic interface** IFNAME
Description	Clear Dynamic Mac Address Entries. Support all, based on vlan or based on interface options.

- Enable/disable Port MAC Address Learning

Mainly used in the following scenarios:

When the network is relatively stable and the MAC addresses of the packets are relatively fixed, the device does not need to continue to learn the MAC addresses of all other packets. At this time, by applying a flow policy, the MAC address learning function is disabled for all traffic classifications under the policy, which can not only save the cost of MAC address entries, but also improve the operation efficiency of the device.

Some illegal users sometimes attack the network by changing the MAC address frequently. At this time, by applying the flow policy, and disabling the MAC address learning function for all traffic classifications under the policy, the device MAC address table caused by such attacks can be avoided. Item overflow problem to protect device performance from being affected.

Command	SWITCH(config-if)#**mac-address-table learning disable action** (**forward** | **drop**) SWITCH(config-if)#**no mac-address-table learning disable**
Description	This command supports physical ports and AP ports, but does not support AP member ports. Disabling the port MAC address learning function. forward: If there is a matching entry in the MAC address table, the packet is forwarded according to the MAC table; if there is no matching entry, the packet is broadcast. discard: If there is a matching entry in the MAC address table, the packet is forwarded according to the MAC table; if there is no matching entry, the packet is discarded. The default port MAC address learning is enabled.

- Port MAC Address Learning Limit

In order to control the number of access users or prevent the MAC address table from being attacked, you can limit the number of MAC addresses that the switch module is allowed to learn, so as to control the number of access users to improve network security.

Command	SWITCH(config-if)#**mac-address-table limit maximum** MAXINUM **action** (**forward** | **drop**) SWITCH(config-if)#**no mac-address-table limit**
Description	This command supports physical ports and AP ports, but does not support AP member ports. Configuring the function of limiting the number of learned MAC addresses on a port. MAXINUM: range <1-32767> forward: After the number of MAC address entries reaches the limit, the packets whose source MAC address is the new MAC address continue to be forwarded, but the MAC address entry is not recorded.

	discard: After the number of MAC address entries reaches the limit, the packets whose source MAC address is the new MAC address will be discarded.

- Enable/disable VLAN MAC Address Learning

To improve the security of the device, network administrators can specify certain VLANs to only allow packets from certain MAC addresses to pass through. After the MAC address learning function is disabled, the device will no longer learn a new MAC address from this VLAN, so it will not be able to communicate through this VLAN, which enhances the stability and security of the network.

When the MAC address learning function is enabled, it receives Ethernet frames from peripheral devices, parses out the source MAC address, and adds a new entry to the MAC address entry. Later, when the switching module receives the Ethernet frame destined for the destination MAC address, it can directly query the MAC address entry to obtain the correct sending interface, avoiding broadcast.

Command	SWITCH(config)#**mac-address-table learning disable vlan** VLAN-LIST **action** (**forward** | **drop**) SWITCH(config)#**no mac-address-table learning disable vlan** VLAN-LIST
Description	Disabling the VLAN MAC address learning function. VLAN-LIST: Support single vlan or range mode, for example: 10 or 10-20. forward: If there is a matching entry in the MAC address table, the packet is forwarded according to the MAC table; if there is no matching entry, the packet is broadcast. discard: If there is a matching entry in the MAC address table, the packet is forwarded according to the MAC table; if there is no matching entry, the packet is discarded. The default port MAC address learning is enabled.

- Limit the Number of Learned Addresses on VLAN

In order to control the number of access users or prevent the MAC address table from being attacked, you can limit the number of MAC addresses that the switch module allows to learn in the VLAN, so as to control the number of access users to improve network security.

Command	SWITCH(config-if)#**mac-address-table limit vlan** VLAN-LIST **maximum** MAXINUM **action** (**forward** | **drop**) SWITCH(config-if)#**no mac-address-table limit vlan** VLAN-LIST
Description	Configuring the function of limiting the number of learned VLAN MAC addresses. VLAN-LIST: Support single vlan or range mode, for example: 10 or 10-20. MAXINUM: range <1-32767>. forward: After the number of MAC address entries reaches the limit, the packets whose source MAC address is the new MAC address continue to be forwarded, but the MAC address entry is not recorded. discard: After the number of MAC address entries reaches the limit, the packets whose source MAC address is the new MAC address will be discarded.

- Turn On/off the Flipping Function

MAC address flapping means that the MAC address learned by one interface on the device is also learned on another interface in the same VLAN, and the MAC address entry learned later overwrites the original entry.

MAC address flapping may be caused by the following reasons：

The network cable of the switch module in the network is incorrectly connected or configured incorrectly to form a ring network, resulting in MAC address drift.

Some illegal users in the network conduct MAC address attacks.

Configuring the MAC address flapping detection function can detect whether all the MAC addresses on the device are flapping. If drift occurs, the drift event will be recorded, and maintenance personnel can locate the fault according to the alarm information.

Command	SWITCH(config)#**mac-address-table flapping detect**

	SWITCH(config)#**no mac-address-table flapping detect**
Description	Configure and enable the MAC address flapping function, which is disabled by default.

- Flapping Detected to Trigger Shutdown

After an interface is configured with a MAC address flapping action, if the system detects that the MAC learned by the interface is flapping, it will shut down the interface.

Whether the port shutdown action is executed depends on whether the Mac-address-table-flapping option of the errdisable module is selected. It is enabled by default.

Command	SWITCH(config)#**mac-address-table flapping detect action shutdown** SWITCH(config)#**no mac-address-table flapping detect action**
Description	Configure and enable the MAC address flapping function, which is disabled by default.

- Configure The Number Of Migrations Triggered By Flipping

MAC address migration may be caused by normal unplugging or plugging, or it may be caused by other abnormal reasons such as loops. If the number of MAC address migration exceeds the configured value, it is considered that a flapping event has occurred.

Command	SWITCH(config)#**mac-address-table flapping detect times** VALUE SWITCH(config)#**no mac-address-table flapping detect times**
Description	Configure the number of migrations triggered by flipping. VALUE：<1 50>，default value is 5

- Clear the Flapping Record Information

Command	SWITCH#**clear mac-address-table flapping**
Description	Clear the flapping record information.

13.3. Examples

Example 1：This example shows how to change MAC Address aging time to 60 seconds.

Step1: Enter configuration mode：

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Step2: Change MAC Address aging time to 60 seconds.

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

Example 2: This example shows how to add a static MAC Address entry.

Step1: Enter configuration mode：

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Step2: Add a static MAC Address entry.

```
SWITCH(config)#mac-address-table static 000E.C6C1.C8AB vlan 1 interface
gigabitEthernet0/1
```

Example 3: This example shows how to add a filter MAC Address entry.

Step1: Enter configuration mode：

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Step2: Add a filter MAC Address entry

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

Example 4: This example shows how to clear dynamic MAC Address entries.

Step1: Clear MAC Address entries by interface.

```
SWITCH#clear mac-address-table dynamic interface gigabitEthernet0/1
```

13.4. Display Information

- Display MAC Address Table Entries

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

- Display MAC Address Table Statistics

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

- Display MAC Address Learning Configuration Information

```
SWITCH#show mac-address-table learning

Interface               Status          Action
--------------------------------------------------
GiE0/4                  Disabled        Forward
Vlan 3-6                Disabled        Drop
Vlan 9-10               Disabled        Drop
```

- Display MAC Address Limit Configuration Information

```
SWITCH#show mac-address-table limit

Interface               Limit           Action
--------------------------------------------------
GiE0/5                  1000            Drop
Vlan 20-25              100             forward
```

- Display MAC Address Flapping Information

```
SWITCH#show mac-address-table flapping

Mac-address-table Flapping Configurations:
------------------------------------------------------------
Mac-address-table flapping detect   :  Disabled
Mac-address-table flapping times    :  5
Mac-address-table flapping action   :  none
------------------------------------------------------------

Mac-address-table Flapping entries  :  0
```

14. Configuring LLDP

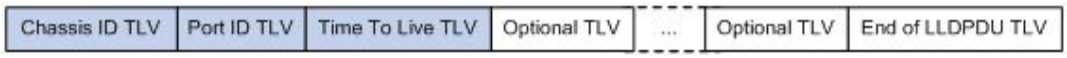
14.1. Overview of LLDP

LLDP (Link Layer Discovery Protocol) provides a standard link layer discovery method, enabling devices of different manufacturers to discover each other in the network and exchange their system and configuration information. LLDP encapsulates the information of the local device (including main capabilities, management address, device identification, interface identification, etc.) in LLDPDU (Link Layer Discovery Protocol Data Unit) It is released to the neighbors directly connected to itself. After receiving the information, the neighbors save it in the form of standard MIB up for the network management system to query and judge the communication status of the link.

LLDPDU

LLDPDU is a data unit encapsulated in the data part of an LLDP message. Before forming an LLDPDU, the device first encapsulates the local information into a TLV format, and then combines several TLVs into one LLDPDU and encapsulates it in the data part of the LLDP packet for transmission.

Figure 1 LLDPDU encapsulation format



As shown in Figure 1, the blue Chassis ID TLV, Port ID TLV, and Time To Live TLV must be carried by each LLDPDU, and the remaining TLVs are optional. Each LLDPDU can carry up to 32 TLVs.

TLV

TLV is the unit that makes up LLDPDU, and each TLV represents a piece of information. The TLVs that LLDP can encapsulate include basic TLVs, 802.1 organization-defined TLVs, 802.3 organization-defined TLVs, and LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery, Link Layer Discovery Protocol Media Endpoint Discovery) TLVs.

Basic TLV

Basic TLVs are a set of TLVs that are the basis for network device management. 802.1 organization-defined TLVs, 802.3 organization-defined TLVs, and LLDP-MED TLVs are TLVs defined by standards organizations or other organizations to enhance the management of network devices. Need to choose whether to send in LLDPDU.

Among the basic TLVs, there are several TLVs that are mandatory for implementing the LLDP function, that is, they must be published in the LLDPDU, as shown in Table 1.

Table 1 Basic TLV

TLV name	instruction	Must be published
Chassis ID	Bridge MAC address of the sending device	Yes

TLV name	instruction	Must be published
Port ID	Identifies the port of the sender of the LLDPDU. If LLDP-MED TLV is carried in LLDPDU, its content is the MAC address of the port; otherwise, its content is the name of the port	Yes
Time To Live	The survival time of this device information on the neighbor device	Yes
End of LLDPDU	The end identifier of the LLDPDU, which is the last TLV of the LLDPDU	no
Port Description	Description of the port	no
System Name	the name of the device	no
System Description	description of the system	no
System Capabilities	The main functions of the system and the function items that have been turned on	no
Management Address	Management address, as well as the interface number and OID (Object Identifier) corresponding to the address	no

802.1 Organization-Defined TLV

The content of TLV defined by IEEE 802.1 organization is shown in Table2.

Currently, the devices do not support sending Protocol Identity TLV and VID Usage Digest TLV, but can receive these two types of TLVs.

Layer 3 Ethernet interfaces only support Link Aggregation TLVs.

Table2 IEEE 802.1Organization defined TLV

TLV name	instruction
Port VLAN ID (PVID)	Port VLAN ID
Port and protocol VLAN ID (PPVID)	Port Protocol VLAN ID
VLAN Name	The name of the VLAN to which the port belongs
Protocol Identity	The type of protocol supported by the port
DCBX	Data Center Bridging Exchange Protocol
EVB module	(Not currently supported) Edge Virtual Bridging module, including EVB TLV and CDCP (S-Channel Discovery and Configuration Protocol, S-Channel Discovery and Configuration Protocol) TLV. For the detailed introduction of these two TLVs, please refer to "EVB Configuration Guide"
Link Aggregation	Whether the port supports link aggregation and whether link aggregation is enabled

TLV name	instruction
Management VID	management VLAN
VID Usage Digest	Data containing a summary of VLAN ID usage
ETS Configuration	Enhanced Transmission Selection configuration
ETS Recommendations	Enhanced transfer selection recommendation
PFC	Priority-based Flow Control
APP	Application Protocol
QCN	(Not currently supported) Quantized Congestion Notification

802.3 Organization-Defined TLV

The content of TLV defined by Table3.

The Power Stateful Control TLV was defined in the IEEE P802.3at D1.0 version, and later versions no longer support this TLV. The device will only send this type of TLV after receiving the Power Stateful Control TLV.

Table3 IEEE 802.3Organization defined TLV

TLV name	instruction
MAC/PHY Configuration/Status	The rate and duplex status supported by the port, whether it supports port rate auto-negotiation, whether the auto-negotiation function is enabled, and the current rate and duplex status
Link Aggregation	Whether the port supports link aggregation and whether link aggregation is enabled
Power Via MDI	The power supply capability of the port, including the type of PoE (Power over Ethernet) (including PSE (Power Sourcing Equipment) and PD (Powered Device)), the remote power supply mode of the PoE port, Whether PSE power supply is supported, whether PSE power supply is enabled, whether the power supply mode is controllable, power supply type, power source, power priority, PD requested power value, and PSE allocated power value
Maximum Frame Size	Maximum frame length supported by the port
Power Stateful Control	Power status control of ports, including the type of power used by the PSE/PD, the priority of supplying/receiving power, and the power supplied/received
Energy-Efficient Ethernet	Energy Efficient Ethernet

management address

The management address is an address for the network management system to identify and manage network devices. The management address can clearly identify a device, which facilitates the drawing of

network topology and facilitates network management. The management address is encapsulated in the Management Address TLV of the LLDP packet and advertised.

LLDP Mode

Under the specified type of LLDP proxy, LLDP has the following four working modes:

- TxRx: Both send and receive LLDP packets.
- Tx: Only sends and does not receive LLDP packets.
- Rx: only receives and does not send LLDP packets.
- Disable: Neither sends nor receives LLDP packets.

When the LLDP working mode of the port changes, the port will initialize the protocol state machine. To prevent the port from continuously performing initialization operations due to frequent changes in the working mode of the port, you can configure the port initialization delay time.

Protocol Specification

The protocol specifications related to LLDP are:

- IEEE 802.1AB-2005: Station and Media Access Control Connectivity Discovery.
- IEEE 802.1AB 2009: Station and Media Access Control Connectivity Discovery.
- ANSI/TIA-1057: Link Layer Discovery Protocol for Media Endpoint Devices.
- IEEE Std 802.1Qaz-2011: Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes.

14.2. Configuring

14.2.1. Configuring Switch and Operating Mode

- Enabling/disabling the LLDP Function Globally

Command	SWITCH(config)# **lldp run** SWITCH(config)# **no lldp run**
Description	Global configuration mode. Enable/disable LLDP function. required.

- Entering LLDP Interface Proxy Configuration Mode

Command	SWITCH(config-if)# **lldp -agent** SWITCH(lldp-agent)# **exit**
Description	Interface configuration mode. Enter the LLDP interface proxy configuration mode. Optional.

- Configuring the Working Mode of an LLDP Interface

Command	SWITCH(lldp-agent)# **lldp enable** { **rxonly** | **txonly** | **txrx** } SWITCH(lldp-agent)# **lldp disable**
Description	LLDP interface proxy configuration mode. Configure the working mode of the LLDP interface. Optional.

14.2.2. Configuring Optional Basic Parameter

- Configuring System Name

Command	SWITCH(config)# **lldp system-name** NAME SWITCH(config)# **no lldp system-name**
Description	Global configuration mode. Configure/reset the system name. Optional.

- Configuring System Descriptor

Command	SWITCH(config)# **lldp system-description** LINE SWITCH(config)# **no lldp system-description**
Description	Global configuration mode. Configure /reset system descriptors. Optional.

- Configuring the Device Locally-assigned

Command	SWITCH(config)# **lldp chassis locally-assigned** NAME SWITCH(config)# **no lldp chassis locally-assigned**
Description	Global configuration mode. Configure/reset the device locally-assigned . Optional.

- Configuring Interface Locally-assigned

Command	SWITCH(config-if)# **lldp locally-assigned** NAME SWITCH(config-if)# **no lldp locally-assigned**
Description	Interface configuration mode. Configure/reset the interface locally-assigned . Optional.

- Configuring Interface Proxy Cable Identification

Command	SWITCH(config-if)# **lldp agt-circuit-id** VALUE SWITCH(config-if)# **no lldp agt-circuit-id**
Description	Interface configuration mode. Configuration/reset interfaceagt-circuit-id.can be used as a value for port-id-tlv. Optional.

- Configuring Interface Port Descriptor

Command	SWITCH(config-if)# **lldp port-description** LINE SWITCH(config-if)# **no lldp port-description**
Description	Interface configuration mode. Configure/reset interface port descriptors. Optional.

- Configuring the Device ID Type of LLDP Interface

Command	SWITCH(lldp-agent)# **lldp chassis-id-tlv** { **if-alias | if-name | ip-address | locally-assigned | mac-address** } SWITCH(lldp-agent)# **no lldp chassis-id-tlv**
Description	LLDP interface proxy configuration mode. Configure the device identification type of the LLDP interface. Optional.

- Configuring the Management Address Type of LLDP Interface

Command	SWITCH(lldp-agent)# **lldp management-address-tlv** { **ip-address | mac-address** } SWITCH(lldp-agent)# **no lldp management-address-tlv**
Description	LLDP interface proxy configuration mode. Configure the management address type of the LLDP interface. Optional.

- Configuring the Port ID Type of LLDP Interface

Command	SWITCH(lldp-agent)# **lldp port-id-tlv** { **agt-circuit-id | if-alias | if-name | ip-address | locally-assigned | mac-address** } SWITCH(lldp-agent)# **no lldp port-id-tlv**
Description	LLDP interface proxy configuration mode. Configure the port ID type of the LLDP interface. Optional.

14.2.3. Configuring Optional State Machine Parameter

- Configuring the MsgTxHold Parameter of an LLDP Interface

Command	SWITCH(lldp-agent)# **lldp msg-tx-hold** <1-100> SWITCH(lldp-agent)# **no lldp msg-tx-hold**
Description	LLDP interface proxy configuration mode. This variable is used as a multiplier for msgTxInterval to determine the value of txTTL carried in LLDP frames transmitted by the LLDP proxy.The default msgTxHold is 4. Administrators can change this value to any value in the range 1 to 100.TTL= msgTxInterval * msgTxHold + 1 . Optional.

- Configuring the TxFastInit Parameter of the LLDP Interface

Command	SWITCH(lldp-agent)# **lldp tx-fast-init** <1-8> SWITCH(lldp-agent)# **no lldp tx-fast-init**
Description	LLDP interface proxy configuration mode. This variable is used as the initial value of the txFast variable. This value determines the number of LLDPDUs transmitted during the fast transmission period.The default value of txFastInit is 4. Administrators can change this value to any value between 1 and 8. Optional.

- Configuring the TxCredit Parameter of the LLDP Interface

Command	SWITCH(lldp-agent)# **lldp tx-max-credit** <1-8> SWITCH(lldp-agent)# **no lldp tx-max-credit**
Description	LLDP interface proxy configuration mode. Configure the maximum value of txCredit.The default value is 5. Administrators can change this value to any value in the range 1 to 10. Optional.

- Configuring the msgFastTx Parameter of the LLDP Interface

Command	SWITCH(lldp-agent)# **lldp timer msg-fast-tx** <1-3600>

	SWITCH(lldp-agent)# **no lldp timer msg-fast-tx**
Description	LLDP interface proxy configuration mode. This variable defines the time interval of the timer interval between two transfers in a fast transfer period (i.e. txFast is not zero). The default value for msgFastTx is 1; administrators can change this value to any value between 1 and 3600. Optional.

- Configuring the MsgTxInterval Parameter of the LLDP Interface

Command	SWITCH(lldp-agent)# **lldp timer msg-tx-interval** <5-3600> SWITCH(lldp-agent)# **no lldp timer msg-tx-interval**
Description	LLDP interface proxy configuration mode. This variable defines the timer interval between normal transfers (i.e. txFast is zero). The default value for msgTxInterval is 30 s; admin can change this value to any value between5and 300. Optional.

- Configuring the ReinitDelay Parameter of an LLDP Interface

Command	SWITCH(lldp-agent)# **lldp timer reinit-delay** <1-10> SWITCH(lldp-agent)# **no lldp timer reinit-delay**
Description	LLDP interface proxy configuration mode. This parameter represents the amount of delay between when adminStatus becomes "disabled" and when reinitialization is attempted. The default value of reinitDelay is 2 s. Optional.

14.2.4. Configuring Send Tlv List

- Configuring Tlv Selection for LLDP Interfaces

Command	SWITCH(lldp-agent)# [**no**] **lldp tlv-select basic-mgmt** { management-address | port-description | system-capabilities | system-description | system-name} SWITCH(lldp-agent)# [**no**] **lldp tlv-select ieee-8021-org-specific** { link-agg | mgmt-vid | port-ptcl-vlanid | port-vlanid | ptcl-identity | vid-digest | vlan-name } SWITCH(lldp-agent)# [**no**] **lldp tlv-select ieee-802 3 -org-specific** { mac-phy | max-mtu-size }
Description	LLDP interface proxy configuration mode. tlvs can be selected with multiple commands. Optional. Note: When there are many VLAN configurations on the device, the VLAN-related tlv may cause the packet length to exceed the MTU, resulting in packet sending errors. It is necessary to configure not to send this type of tlv.

14.3. Examples

14.3.1. LLDP Basic Function Configuration Example

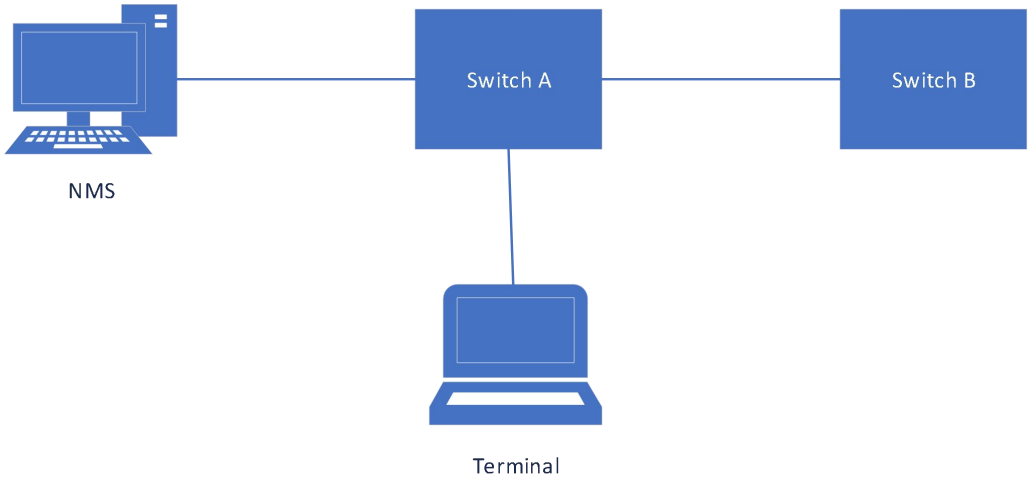
Requirements

NMS (Network Management System, network management system) is connected to Switch A, and Switch A is connected to the Terminal device and Switch B respectively.

By configuring the LLDP function on Switch A and Switch B, the NMS can judge the communication status of the link between Switch A and the terminal device, and between Switch A and Switch B.

Network diagram

Figure2 LLDP basic function configuration network diagram



Typical configuration example

Switch A/B:

```
Lldp run
```

14.4. Display Information

- Display the Status of the LLDP Interface

```
#show lldp interface gigabitEthernet0/2

Agent Mode : Nearest bridge
Enable (tx/rx): Y/Y
Message fast transmit time:1
Message transmission interval: 30
Reinitialisation delay: 2
MED Enabled:Y
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 4608
Total entries aged: 0
Total frames received: 150
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0
```

- Show LLDP Interface Neighbors

```
#show lldp interface gigabitEthernet0/2 neighbor
Nearest bridge Neighbors
Interface Name : gigabitEthernet0/2
System Name :
System Description :
Port Description :
TTL: 3601
System Capabilities : Routing
Mandatory TLVs :
CHASSIS ID TYPE :
Chassis MAC Address: 000e.c6c1.3841
PORT ID TYPE :
Port MAC Address: 000e.c6c1.3841
8021 ORIGIN SPECIFIC TLV
```

```
    Port Vlan id :0
    PP Vlan id :0
    Remote Protocols Advertised :
    Remote VID Usage Digest : 0
    Remote Management Vlan : 0
    Link Aggregation Status : Disabled
    Link Aggregation Port ID : 0
    8023 ORIGIN SPECIFIC TLV
    AutoNego Support : Supported Enabled
    AutoNego Capability : 1
    Operational MAU Type : 0
    Max Frame Size : 0
    MED Capabilities : Capabilities
    MED Capabilities Dev Type : End Point Class-1
    MED Application Type : Reserved
    MED Vlan id : 0
    MED Tag/Untag: Untagged
    MED L2 Priority : 0
    MED DSCP Val : 0
```

15. Configuring LOOP-DETECT

15.1. Overview of LOOP-DETECT

LOOP-DETECT is an Ethernet loop detection protocol, which is used to quickly detect loop faults on downlink interfaces. If a fault is found, LOOP-DETECT will notify the user to manually close or automatically close the relevant port according to the fault handling method configured by the user, so as to avoid affecting the normal data exchange.

Enable control: Enable control is divided into global enable control and port enable control. When the global enable control is enabled and the loop detection is enabled on the port, the port supports the loop detection function.

Loop action: When a loop fault is detected on the port, the user will be notified to manually handle the loop fault by default, and the automatic closing of the port can also be configured. When the port is automatically shut down, the port can recover from the fault by waiting for timeout, shutdown/no shutdown port, recovery command, or restarting the device.

Specify vlan: By default, the port vlan attribute is ignored; if you need to detect whether a loop fault occurs in a specific vlan domain, you can configure the specified vlan on the port, and only detect Whether there is a loop data path in this vlan domain.

The device supports loop fault alarm and loop fault recovery message traps to the snmp server, which is disabled by default.

15.2. Configuring

15.2.1. Enable LOOP-DETECT Globally

Command	SWITCH(config)#**loop-detect enable** SWITCH(config)#**no loop-detect enable**
Description	Enable the LOOP-DETECT function globally. Disabled by default.

15.2.2. Enable LOOP-DETECT On Interface

Command	SWITCH(config-if)#**loop-detect enable** SWITCH(config-if)#**no loop-detect enable**
Description	Enabe the LOOP-DETECT Function Based on Ports. Disabled by default. Supports physical ports and AP ports, does not support AP members.

Note:

✦ For a port in the block state, the protocol considers that there is no possibility of a loop. Even if the port is enabled for loop detection, the actual function cannot run normally. In an environment where stp and erps are enabled, a similar situation may exist. It is recommended to make the function mutually exclusive in the configuration.

15.2.3. Configure Port Loop Action

Command	SWITCH(config-if)#**loop-detect action (alarm | error-down)** SWITCH(config-if)#**no loop-detect action**

Description	Configure port loop action. Alarm: print alarm information. Error-down: print alarm information and shut down the port at the same time. The default action is alarm.

15.2.4. Specify Vlan Domain To Detect

Command	SWITCH(config-if)#**loop-detect vlan** VID SWITCH(config-if)#**no loop-detect vlan** VID SWITCH(config-if)#**no loop-detect vlan**
Description	Detect whether a data path loop occurs in the specified vlan domain. VID supports single vlan mode and range mode, such as 10-12, separated by "," in the middle. A port can specify up to 8 vlans. By default, if no vlan is specified, the port vlan attribute will be ignored. If the port is in the block state, the data path is considered to be blocked.

15.2.5. Set Packet Sending Interval

Command	SWITCH(config)#**loop-detect interval** SECONDS SWITCH(config)#**no loop-detect interval**
Description	Configure the interval for sending loop detection packets. SECONDS: range 5-300, default 5, unit second.

15.2.6. Set Error-down Recovery Time

Command	SWITCH(config)#**errdisable timeout (interval** SECONDS | enable | disable) SWITCH(config)#**no errdisable timeout interval**
Description	Configure errdisable recovery time. SECONDS: range 10-1000000, unit second. Enable: enable errdisable recovery. Disable: disable errdisable recovery. The default time is 300 seconds. The time is shared by all errdisable applications, configuring this parameter will affect other applications.

15.2.7. Error-down Recovery

Recovery interface from errdisable status. If errdisable timeout is disabled, this command will not work, please use shutdown and no shutdown commands to recovery interface.

Command	SWITCH#**errdisable recovery interface** IFNAME
Description	Recovery Interface to normal.

15.2.8. Enable Trap

Command	SWITCH(config)#**loop-detect trap enable** SWITCH(config)#no **loop-detect trap enable**
Description	Enable trap loop fault occurrence and loop fault recovery messages to the snmp server. Disabled by default.

Definition of loop alarm trap node:

Node	Data
Mib files	DK-LDET-MIB.my
oid	1, 3, 6, 1, 4, 1, 57430, 1, 6, 2,1
Ifindex	port index

Definition of loop alarm recovery trap node:

Node	Data
Mib files	DK-LDET-MIB.my
oid	1, 3, 6, 1, 4, 1, 57430, 1, 6, 2,2
Ifindex	port index

15.3. Examples

Case 1: Configure port gi0/1 to enable the loop detection function, and configure the action to err-down.

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#loop-detect enable
SWITCH(config)#interface gigabitEthernet 0/1
SWITCH(config-if)# loop-detect enable
SWITCH(config-if)# loop-detect action error-down
```

When port gi0/1 detects a loop, it prompts the following information and shuts down the port.

```
LOOPDETECT-4:   %Loop error detected on interface GigabitEthernet 0/1.set
interface err-down.
```

Case 2: Configure port gi0/1 to perform loop detection in the vlan10 domain.

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#vlan 10
SWITCH(config)#loop-detect enable
SWITCH(config)#interface gigabitEthernet 0/1
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)# loop-detect enable
SWITCH(config-if)# loop-detect vlan 10
```

The port gi0/1 sends loop detection messages with tag and vid is 10. If a loop is detected in the vlan10 domain, the log information is output. if peer interface not allow vlan10, no loop detected.

```
LOOPDETECT-4:   %Loop error detected on interface GigabitEthernet 0/1.
```

Case 3: Configure port gi0/1 to enable loop detection, enable trap, and configure the snmp server 192.168.64.1.

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#snmp-server group public v2c read all write all
SWITCH(config)#snmp-server community public
SWITCH(config)#snmp-server host 192.168.64.1 traps v2c  community public
SWITCH(config)#loop-detect enable
SWITCH(config)# loop-detect trap enable
SWITCH(config)#interface gigabitEthernet 0/1
SWITCH(config-if)# loop-detect enable
```

When port gi0/1 detects a loop, the snmp server receives the loop alarm trap information.

15.4. Display Information

15.4.1. Display LOOP-DETECT Information

```
SWITCH#show loop-detect
Global configuration:
   Loop-detect State            : Enabled
```

```
    Loop-detect Interval         : 5
    Loop-detect trap             : Enabled

Interface gigabitEthernet 0/1:
    Loop-detect State            : Enabled
    Loop-detect Action           : Alarm
    Loop-detect Action Last      : Normal
    Loop-detect Action Last Time : --
    Loop-detect Action Count     : 0
    Loop-detect Vlans            : 10, 20, 30-32
```

Analysis of the information:

Global Information	
Loop-detect State	Global enable status, Enabled or Disabled
Loop-detect Interval	Interval for sending loop detection packets, in seconds
Loop-detect trap	Whether to enable the alarm message trap to the server, Enabled or Disabled
Interface Information	
Loop-detect State	Interface enable status, Enabled or Disabled
Loop-detect Action	Action after loop detection, support alarm and error-down
Loop-detect Action Last	The last time a failure occurred: Normal: normal Alarm: output alarm Error-down: The port is down
Loop-detect Action Last Time	Time of last failure: No failures have occurred:-- Happened, for example: 2022-01-10 22:45:23
Loop-detect Action Count	Count of failures
Loop-detect Vlans	Loop packet specified vlan list

16. Configuring GVRP

16.1. Overview of GVRP

16.1.1. Introduction to GVRP

GVRP (GARP VLAN Registration Protocol) is a protocol for dynamically propagate VLAN attributes, and is an application of GARP (Generic Attribute Registration Protocol). It registers and propagates VLAN attributes through the GARP protocol, and implements dynamic creation and deletion of VLANs on the 802.1Q Trunk port.

16.1.2. Introduction to GARP

GARP provides a mechanism to assist members in the same switching network to distribute, propagate and register information such as VLANs and multicast addresses. The application entities following the GARP protocol are called GARP applications. Currently the main GARP applications are GVRP and GMRP.

GVRP is a GARP application. It can dynamically configure and diffuse VLAN attributes, and realize dynamic automatic registration, log out of VLANs on 802.1Q Trunk ports.

GMRP (GARP Multicast Registration Protocol) is another GARP application. It mainly provides a restricted multicast diffusion function similar to the IGMP detection technology.

The GARP protocol is defined in 802.1D.

16.1.3. Port Registration Mode

There are three port registration modes of GVRP: Normal, Fixed and Forbidden:

Normal mode: Allow the port to dynamically register and log out of VLAN, and propagate dynamic VLAN and static VLAN information.

Fixed mode: Port is prohibited from dynamically registering and deregistering VLANs, and only transmits static VLAN information, not dynamic VLAN information. That is to say, the Trunk port set to Fixed mode, even if all VLANs are allowed to pass, the VLANs actually passed only those manually configured.

Forbidden mode: Port is prohibited from dynamically registering and deregistering VLAN, and does not propagate any VLAN information except VLAN1.

16.1.4. Messages and Timers

GARP message

The information exchange between GARP members is accomplished by means of message transmission. There are three main types of messages that work: Join messages, Leave messages, and LeaveAll messages.

When a GARP application entity wants other devices to register its own attribute information, it will send a Join message to the outside; when it receives a Join message from other entities or the device has statically configured some attributes and needs other GARP application entities to register, The Join message will also be sent out.

When a GARP application entity wants other devices to log out its own attribute information, it will send a Leave message to the outside; when it receives a Leave message from other entities to log off some attributes or statically log off some attributes, it will also send a Leave message to the outside information.

After each GARP application entity is started, it will start the LeaveAll timer at the same time. When the

timer expires, the GARP application entity will send a LeaveAll message to the outside. The LeaveAll message is used to cancel all attributes, so that other GARP application entities can re-register with this entity.

The Join message, Leave message and LeaveAll message cooperate to ensure the re-registration or cancellation of information.

Through message exchange, all attribute information to be registered can be propagated to all devices configured with GARP in the same LAN.

GARP Timer

The time interval for sending GARP messages is implemented through timers. GARP defines four timers for controlling the sending period of GARP messages.

Hold timer: When the GARP application entity receives the registration information sent by other devices, it will not immediately send the registration information as a Join message, but start the Hold timer. When the timer expires, the GARP application entity will All registration information received during this period is sent out in the same Join message, thereby saving bandwidth resources.

Join timer: The GARP application entity can send each Join message twice to ensure the reliable transmission of the message. When the Join message sent for the first time is not answered, the GARP application entity will send the Join message for the second time . The time interval between sending two Join messages is controlled by the Join timer.

Leave timer: When a GARP application entity wishes to cancel certain attribute information, it will send a Leave message to the outside world, and the GARP application entity that receives the message starts the Leave timer, and if it does not receive the Join message before the timer expires, it will log out The attribute information.

LeaveAll timer: After each GARP application entity starts, it will start the LeaveAll timer at the same time. When the timer expires, the GARP application entity will send a LeaveAll message to the outside, so that other GARP application entities can re-register all attribute information on this entity . Then start the LeaveAll timer again to start a new cycle.

16.1.5. Packet Format

GVRP protocol packets are encapsulated in Ethernet frames, and the packet format is shown in the figure below.

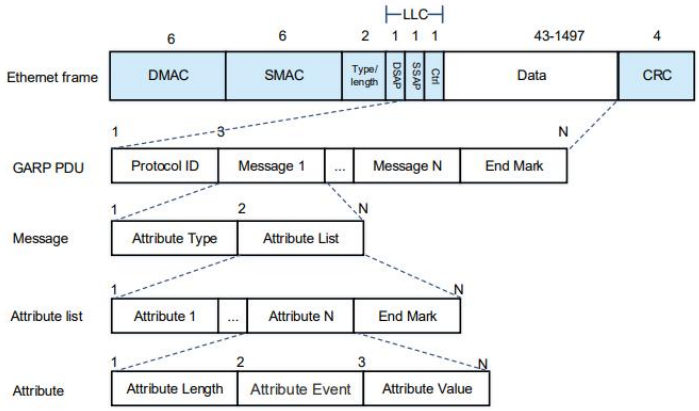


Table GVRP Ethernet packet field meaning:

Packet field	Bytes	Field meaning
Protocol ID	2	Protocol ID, Fixed 0x0001
Message	N	Message content, support N messages

Attribute type	1	Attribute type, GVRP fixed bit 0x01
Attribute list	N	Attribute list, consisting of multiple attributes and end mask
Attribute	N	attribute content
Attribute length	1	attribute content length
Attribute event	1	Events: 0x0:LeaveAll Event 0x1:JoinEmpty Event 0x2:JoinIn Event 0x3:LeaveEmpty Event 0x4:LeaveIn Event 0x5:Empty Event
Attribute value	N	Attribute value
End mask	1	End mask, fixed 0x00

16.2. Configuring

16.2.1. GVRP Enable Control

- Global Enable GVRP

Command	SWITCH(config)#**gvrp enable** SWITCH(config)#**no gvrp enable**
Description	Globally enable the GVRP function By default, the global GVRP function is disabled

- Port Enable GVRP

Command	SWITCH(config-if)#**gvrp enable** SWITCH(config-if)#**no gvrp enable**
Description	Enable the GVRP function on the interface By default, GVRP is disabled on an interface The GVRP function on the interface takes effect only when GVRP is enabled both on the interface and globally.

16.2.2. Set registration Mode

Command	SWITCH(config-if)#**gvrp registration (fixed | forbidden | normal)** SWITCH(config-if)#**no gvrp registration**
Description	Normal mode: Allow the interface to dynamically register and deregister VLANs, and propagate dynamic and static VLAN information. Fixed mode: This interface is prohibited from dynamically registering and deregistering VLANs, and only propagates static VLAN information, not dynamic VLAN information. That is to say, the Trunk interface set to the fixed mode, even if all VLANs are allowed to pass, the VLANs that actually pass can only be those manually configured. Forbidden mode: This interface is prohibited from dynamically registering and deregistering VLANs, and does not propagate any VLAN information to the outside world.

16.2.3. Set Timers

Command	SWITCH(config)#**gvrp timer (join | leave | leaveall)** CENTISEC SWITCH(config)#**no gvrp timer**
Description	Set the value of the GARP timer Join: range <20 32765>, default 20, unit centisecond, required to be less than or equal to 1/3 Leave timer value Leave: range <20 32765>, default 60, unit centiseconds, required to be greater than or equal to 3 times the value of the join timer, less than the value of the leaveall timer

	Leaveall: range <20 32765>, default 1000, unit centisecond, required to be greater than Leave timer value

Note

✦ In the case of multiple devices on the entire network, the value of the LeaveAll timer of each device may be different, but each device will send the LeaveAll message based on the smallest LeaveAll timer on the entire network. Because the LeaveAll message is sent every time the LeaveAll timer expires, other devices will clear the LeaveAll timer after receiving it, so even if there are many different LeaveAll timers on the entire network, only the smallest LeaveAll timer takes effect.

16.2.4. Clear Statistics

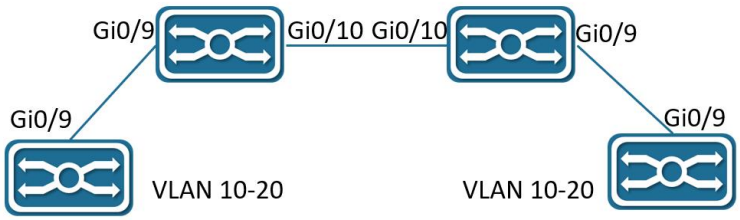
Command	SWITCH#**clear gvrp statistics** (| **interface** IFNAME)
Description	Clear port event statistics Without interface parameter, clear all ports With interface parameter, clear a specific port

16.3. Examples

16.3.1. Typical Cases

Case requirements:

SW1, SW2, SW3, and SW4 are connected through trunk ports. There are static VLANs 10-20 on SW1 and SW4, and SW2 and SW3 are required to learn these VLANs automatically without manual configuration. Enable GVRP globally and on the interfaces of each SW to realize dynamic registration and update of VLAN information between devices.



Steps:

SW1 configuration:

```
SWITCH(config)#Vlan  10-20
SWITCH(config)#gvrp enable
SWITCH(config)#interface gigabitEthernet 0/9
SWITCH(config-if)switchport mode trunk
SWITCH(config-if)gvrp enable
```

SW2 configuration:

```
SWITCH(config)#gvrp enable
SWITCH(config)#interface gigabitEthernet 0/9-10
SWITCH(config-if)switchport mode trunk
SWITCH(config-if)gvrp enable
```

SW3 configuration:

```
SWITCH(config)#gvrp enable
```

```
SWITCH(config)#interface gigabitEthernet 0/9-10
SWITCH(config-if)switchport mode trunk
SWITCH(config-if)gvrp enable
```

SW4 configuration:

```
SWITCH(config)#Vlan  10-20
SWITCH(config)#gvrp enable
SWITCH(config)#interface gigabitEthernet 0/9
SWITCH(config-if)switchport mode trunk
SWITCH(config-if)gvrp enable
```

Verify configuration results:

Execute show gvrp vlan command on SW2 and SW3, and it shows that gi0/9 and gi0/10 have dynamically learned vlan 10-20.

Execute show vlan all conmand on SW2 and SW3, and it shows that gi0/9 and gi0/10 belong to vlan 10-20.

16.4. Display Information

16.4.1. Display GVRP Status Information

```
SWITCH#show gvrp status
GVRP Global Information:
    Global State        :  Enabled
    Join Timer          :  20 centisec
    Leave Timer         :  60 centisec
    LeaveAll Timer      :  1000 centisec

GVRP Port Based Information:
Interface               State        Registration Mode
--------------------    --------     --------------------
gigabitEthernet0/3      Enabled      normal
 po1                     Enabled      normal
```

Displayed message definition:

GVRP Global Information:	Global Configuration Status Information
Global State	Global state, Enabled or Disabled
Join Timer	Join timer value
Leave Timer	Leave timer value
LeaveAll Timer	Leaveall timer value
GVRP Port Based Information:	Port configuration status information, the default status port is ignored and not displayed
Interface	Interface name
State	Port status, Enabled or Disabled
Registration Mode	Port registration mode, Normal, Fixed, Forbidden

16.4.2. Display GVRP VLAN Information

```
SWITCH#show gvrp vlan
Interface gigabitEthernet0/3:
    Static Vlan List    : 1
    Dynamic Vlan List   : 15-21
    Allow Vlan List     : all
Interface po1:
    Static Vlan List    : 1
```

```
    Dynamic Vlan List   : 1000-2000
    Allow Vlan List     : all
SWITCH#show gvrp vlan interface gigabitEthernet 0/3
Interface gigabitEthernet0/3:
    Static Vlan List    : 1
    Dynamic Vlan List   : 15-21
    Allow Vlan List     : all
```

Displayed message definition:

Static Vlan List	Static vlan list supported by the port
Dynamic Vlan List	Dynamic vlan list supported by the port
Allow Vlan List	port allow vlan list

16.4.3. Display GVRP Statistics

```
SWITCH#show gvrp statistics
Interface               Received        Transmitted     Drop
--------------------    ------------    ------------    --------
gigabitEthernet0/3      1462120         7202490         0
po1                     7181418         1790511         0
```

Displayed message definition:

Interface	Interface name
Received	Receive GVRP attribute number
Transmitted	Send GVRP attribute number
Drop	Number of discarded GVRP attributes

```
SWITCH#show gvrp statistics interface gigabitEthernet 0/3
Interface gigabitEthernet0/3:
    Received Valid Attributes           :  1017
    Transmitted Attributes              :  1
    Drop Invalid Attributes             :  0
    Received JoinEmpty Attributes       :  14
    Received JoinIn Attributes          :  2
    Received Empty Attributes           :  1001
    Received LeaveEmpty Attributes      :  0
    Received LeaveIn Attributes         :  0
    Received LeaveAll Attributes        :  0
    Transmitted JoinEmpty Attributes    :  1
    Transmitted JoinIn Attributes       :  0
    Transmitted Empty Attributes        :  0
    Transmitted LeaveEmpty Attributes   :  0
    Transmitted LeaveIn Attributes      :  0
    Transmitted LeaveAll Attributes     :  0
```

Displayed message definition:

Received Valid Attributes	The total number of valid Attributes received
Transmitted Attributes	The total number of Attributes transmitted
Drop Invalid Attributes	The total number of Attributes dropped
Received JoinEmpty Attributes	The number of JoinEmpty Attributes received
Received JoinIn Attributes	The number of JoinIn Attributes received
Received Empty Attributes	The number of Empty Attributes received
Received LeaveEmpty Attributes	The number of LeaveEmpty Attributes received
Received LeaveIn Attributes	The number of LeaveIn Attributes received
Received LeaveAll Attributes	The number of LeaveAll Attributes receiveds

Transmitted JoinEmpty Attributes	The number of JoinEmpty Attributes sent
Transmitted JoinIn Attributes	The number of JoinIn Attributes sent
Transmitted Empty Attributes	The number of Empty Attributes sent
Transmitted LeaveEmpty Attributes	The number of LeaveEmpty Attributes sent
Transmitted LeaveIn Attributes	The number of LeaveIn Attributes sent
Transmitted LeaveAll Attributes	The number of LeaveAll Attributes sent

17. Configuring L3

17.1. Overview of L3

L3 functions include: Layer 3 port management, ARP management and Routing management.

- Layer 3 Port Management:

Layer 3 ports are generally divided into routing ports (physical ports switched to Layer 3 ports) or SVI ports (Switch Virtual Interface, corresponding to a VLAN).

The SVI port is a logical interface, which is constructed on top of all the member ports included in the corresponding VLAN, Unlike the routing port, the packets that are forwarded through the SVI at Layer 3 will first pass through Layer 2 (such as VLAN filtering, address learning, etc.) and then go through three layers, and then go through three layers and then two layers when outputting (such as VLAN output rules).

At the network layer, routing devices use IP addresses to complete packet forwarding. (Protocol specification: RFC 1918: Address Allocation for Private Internets, RFC 1166: Internet Numbers).

Layer 3 port management includes IP address maintenance for Layer 3 ports.

An IP address is composed of 32-bit binary. For the convenience of writing and description, it is generally expressed in dotted decimal. When expressed in dotted decimal, it is divided into four groups, each with 8 digits, ranging from 0 to 255. The groups are separated by ".", for example, "192.168.1.1" is the IP address expressed in decimal.

The IP address, as the name suggests, 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 and the host address part of the IP address 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 is related to the network.

The mask and the obtained is the corresponding part of the network address. Likewise, the netmask can also be directly represented by the mask length.

For example, "192.168.1.1 255.255.255.0" and "192.168.1.1/24" represent the same IP address.

The device supports the configuration of the second IP address, that is, a Layer 3 port can be configured with at most one IP address.

When a Layer 3 port is configured with an IP address, a network segment is determined.

Different Layer 3 ports of the same device must belong to different network segments, and IP addresses configured with different Layer 3 ports must belong to different network segments.

The Layer 3 port represented by the SVI, and the corresponding VLAN is used as the unique identifier of the Layer 3 port.

After the different Layer 3 ports of the device are divided into different network segments, the forwarding between these different network segments (such as VLAN1 and VLAN2) is called "Layer 3 forwarding" (across network segments, or across different VLANs).

- ARP Management:

In a local area network, each IP network device has two addresses:

1) The local address, since it is included in the frame header of the data link layer, should be more precisely the data link layer address, but in fact the local address is processed by the MAC sublayer in the data link layer, Therefore, it is customarily called a MAC address, and a MAC address represents an IP network device on a local area network.

2) The network address represents the IP network device on the Internet, and it also indicates the network to which the device belongs.

To communicate between two IP devices on the LAN, they must know each other's 48-bit MAC address. The process of learning the MAC address from the IP address is called address resolution.

There are two types of address resolution methods:

1) Address Resolution Protocol (ARP).

2) Proxy Address Resolution Protocol (Proxy ARP).

About ARP and Proxy ARP, they are described in RFC 826 and RFC 1027 documents respectively.

ARP (Address Resolution Protocol) is used to bind a MAC address and an IP address. Taking the IP address as an input, ARP can know its associated MAC address. Once the MAC address is known, the IP address to MAC address correspondence is stored in the device's ARP cache. 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 generated by the ARP protocol and static entries derived from static configuration. Dynamic ARP entries are formed by triggering the opening of IP packets. The opening process is an ARP request/response process. If the ARP entries formed after opening are unreachable, they will automatically age out. Static ARP entries do not need to be opened and will not age out.

- Routing Management:

Routing management is responsible for managing routing tables, integrate routes issued by various routing protocols to select the optimal route.

According to different sources, the routing table is usually divided into the following three categories:

- Directly connected route: The route discovered by the link layer protocol is also called the interface route. A direct route is automatically generated when an IP address is configured on a Layer 3 port, and the route prefix is the network directly connected to the Layer 3 port.
- Static route: manually configured by the network administrator.
- Dynamic routes: routes discovered by dynamic routing protocols (such as RIP, OSPF).

A routing table entry consists of two parts:

- Prefix: It is represented by an IP address and network mask (or mask length), which 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 the directly connected network, and the direct connection route belongs to this situation. When configuring a static route, specifying a Layer 3 port instead of an IP address will also generate such a routing table item; the next hop is represented by an IP host address, indicating 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 according to the routing table entry, if the routing table entry specifies the next hop, when the link layer encapsulates the ARP query, the IP of the next hop 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 address of the packet 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 packet. Either way, if the ARP query fails, the route will be opened (a dynamic ARP entry will be generated). If the connection cannot be made, the IP packet cannot be forwarded and will be discarded.

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

17.2. Configuring

- Configuring SVI Port IP/IPv6 Address

Command	**Configure SVI Port IP:** SWITCH(config)#int vlan10 SWITCH(config-if)**#ip address** *IPADDR/MASKLEN [secondary]* SWITCH(config-if)**#ipv6 address** *IP(X:X::X:X/M)* Or SWITCH(config-if)**#ip address** *IPADDR MASK [secondary]* **Delete SVI Port IP:** SWITCH(config)#int vlan10 SWITCH(config-if)**#no ip address** *IPADDR/MASKLEN [secondary]* SWITCH(config-if)**#no ipv6 address** *IP(X:X::X:X/M)* Or SWITCH(config-if)**#no ip address** *IPADDR MASK [secondary]* **Show the IP/IPv6 address of the Layer 3 port:** SWITCH**#show ip interface brief** SWITCH**#show ipv6 interface brief**
Description	Configure in the interface mode of the SVI. When a VLAN is created, the SVI is automatically created, and when the VLAN is deleted, the SVI is automatically deleted. int vlanXX is to enter the interface mode of the SVI. Therefore, when the SVI does not exist (the corresponding VLAN does not exist), entering the interface mode of the SVI will fail. At the same time, when the SVI is deleted, the IP address configured on it will be automatically cleared. Layer 3 ports support IP/IPv6 address configuration update, which has the same effect as deleting and reconfiguring. The IP addresses configured on different Layer 3 ports must belong to different network segments. SVI supports the configuration of the second ip. When configuring the second ip, you need to configure the primary ip first. When deleting the primary ip, if the second ip already exists, you need to delete all the second ip before deleting the primary ip,

	otherwise it cannot be deleted. Note: After this command is configured, the system will clear the management IP configuration (refer to: Configuring Management IP), and use the Layer 3 port IP address as the device management IP instead.

- Configuring Routing Port IP/IPv6 Address

Command	**Configure Routing Port IP:**
	SWITCH(config)#**interface** gigabitEthernet0/1
	SWITCH(config-if)#**no switchport**
	SWITCH(config-if)#**ip address** *IP(A.B.C.D/M) [secondary]*
	SWITCH(config-if)#**ipv6 address** *IP(X:X::X:X/M)*
	Or
	SWITCH(config-if)#ip address IP(A.B.C.D) MASK(A.B.C.D) *[secondary]*
	
	Delete Routing Port IP:
	SWITCH(config)# interface gigabitEthernet0/1
	SWITCH(config-if)#no ip address IP(A.B.C.D/M)
	SWITCH(config-if)#no ipv6 address IP(X:X::X:X/M)
	Or
	SWITCH(config-if)#no ip address IP(A.B.C.D) MASK(A.B.C.D)
	SWITCH(config-if)#switchport

Description	Configure in interface mode. Before configuring the routing port IP, since the default attribute of the interface is the Layer 2 port attribute, you need to use the no switchport command to switch the port from the Layer 2 port attribute to the Layer 3 routing port attribute, and then use the ip address command to configure the routing port attribute. IP configuration, otherwise, switch the routing port to the Layer 2 port attribute, use the switchport command. Layer 3 ports support IP address configuration update, which has the same effect as deleting and reconfiguring. The IP addresses configured on different Layer 3 ports must belong to different network segments. The Layer 3 interface supports the configuration of the second ip. When configuring the second ip, you need to configure the primary ip first. When deleting the primary ip, if the second ip already exists, you need to delete all the second ip before deleting the primary ip, otherwise it cannot be deleted.

- Configuring Static ARP Entries

Command	SWITCH(config)#**arp** IPADDR MACADD SWITCH(config)#**no arp** IPADDR
Description	Configure in global configuration mode. The IP address configured with static ARP must belong to the directly connected network segment, otherwise the configuration fails. Static ARP has a higher priority than dynamic ARP. When the two conflict, static ARP takes effect. When the IP address of the Layer 3 port is deleted or the Layer 3 port is deleted, if the IP address of the static ARP belongs to the directly connected network segment of the Layer 3 port, the static ARP will be 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 a Layer 3 port is configured with an IP address, the ARP entry of the directly connected network segment whose IP address belongs to the Layer 3 port will change from an invalid state to a valid state. (You can see the existence of ARP entries through show arp).

- Clearing ARP Cache

Command	SWITCH#**clear arp-cache**
Description	Clear the ARP cache in privileged mode. This Command only clears dynamic ARP entries, and static ARP entries will not be cleared.

- Configuring Static IPv6 Neighbor Entries

Command	SWITCH(config)# **ipv6 neighbor** *IPv6(X:X::X:X) IFNAME MAC(XXXX.XXXX.XXXX)* SWITCH(config)#**no ipv6 neighbor** *IPv6(X:X::X:X) IFNAME*
Description	Configure in global configuration mode. The IPv6 address configured with the static ipv6 neighbor must belong to the directly connected network segment, otherwise the configuration fails. The static ipv6 neighbor has a higher priority than the dynamic ipv6 neighbor. When the two conflict, the static ipv6 neighbor takes effect. When the IPv6 address of the Layer 3 port is deleted or the Layer 3 port is deleted, if the IPv6 address of the static ipv6 neighbor belongs to the directly connected network segment of the Layer 3 port, the static ipv6 neighbor will be invalid (you can see that the table does not exist through show ipv6 neighbors Item, but show run can see that the configuration is still there); Similarly, when a Layer 3 port is configured with an IPv6 address, the ipv6 neighbor entry whose IPv6 address belongs to the directly connected network segment of the Layer 3 port will change from an invalid state to valid state. (You can see that the neighbors table entry exists by show ipv6 neighbors).

- Configuring Static Routes

Command	SWITCH(config)#**ip route** {IPADDR/MASKLEN) | IPADDR MASK} {NH_IPADDR | IFNAME} SWITCH(config)#**no ip route** {IPADDR/MASKLEN | IPADDR MASK} {NH_IPADDR | IFNAME} SWITCH(config)#**ipv6 route** *[IPv6(X:X::X:X/M) [NH_IPv6(X:X::X:X) | IFNAME]* SWITCH(config)#**no ip v6 route** *[IPv6(X:X::X:X/M) [IPv6(X:X::X:X) | IFNAME]*
Description	Configure in global configuration mode. Recursive routing is not supported (the configured next-hop IP must belong to the directly connected network segment); The route prefix cannot belong to the directly connected network segment (that is, the directly connected route is automatically generated and cannot be statically configured). When a Layer 3 port is configured with an IP address, if the prefix of a static routing entry belongs to the directly connected network segment of the Layer 3 port, the static route will be automatically deleted and a LOG prompt will be displayed; When the IP address of a Layer 3 port is deleted or the Layer 3 port is deleted, if the next hop IP of a static routing entry belongs to the directly connected network segment of the Layer 3 port, the static route is automatically deleted and a LOG prompt is displayed.

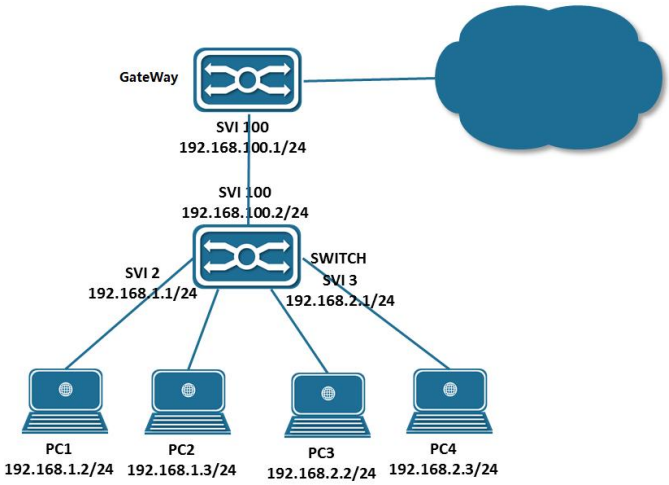
- Configuring ECMP

If there are redundant links in the network environment, that is, there are multiple next hops for the route to the same destination address. On devices that support ECMP technology, multiple next hops can work at the same time, so that redundant links can be fully utilized, and when a link failure occurs on a redundant link, traffic can be switched to other redundant links. Network reliability and stability.

ECMP (Equal-Cost Multipath Routing), this technology enables the device to use multiple next-hop links of the corresponding route concurrently, and balance the traffic among the multiple next-hop links according to the set balance factor distribution; and supports fast switchover of faulty links.

17.3. Examples

Case 1: Weak Layer 3 Gateway



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

- Configure PC:

Configure the IP addresses of PC1, PC2 and PC3 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.

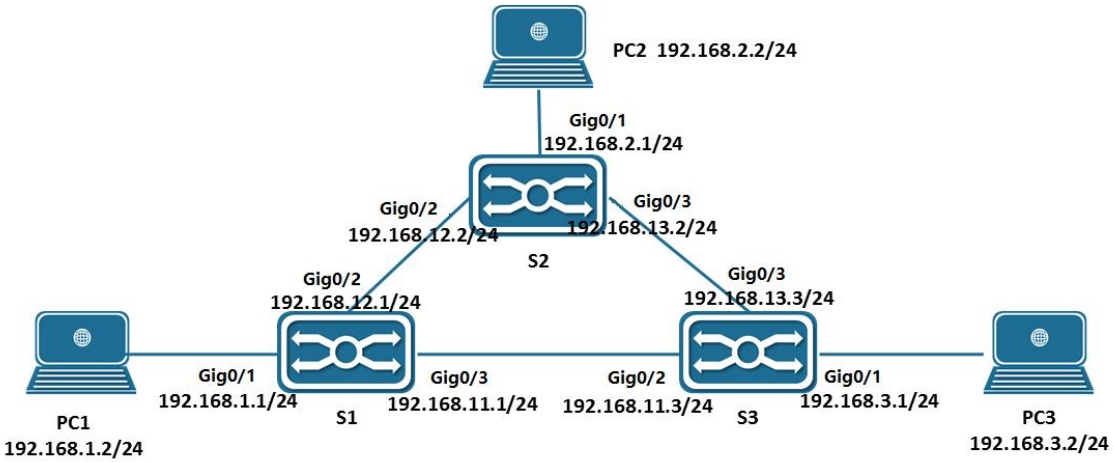
- Configure SWITCH:
  - Configure the Layer 3 port and IP address: (Assume that the interface connecting PC1-PC4 is gigabitEthernet0/1-4, and the uplink interface is gigabitEthernet0/17)

```
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
```

  - Configure a static route (default route):

```
SWITCH(config-if)ip route 0.0.0.0/0 192.168.100.1
```

Case 2: Intranet Layer 3 Interconnection



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

- Configure PC

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

- Configure S1
  - Configure the Layer 3 port and IP address:

```
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
```

  - Configure a static route:

```
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
```

- S2 and S3 are configured similarly to S1.

17.4. Display Information

- Show L3 Interface

```
SWITCH#show ip interface brief
Interface            IP-Address      Admin-Status         Link-Status
GiE0/3               10.10.20.1      up                   down
vlan10               192.168.65.166  up                   up
SWITCH#show ipv6 interface brief
Interface            IPv6-Address           Admin-Status
vlan10               2001:db8:0:f104::1     [up/up]
```

```
vlan1000              unassigned              [up/up]
```

- Show ARP Entries

```
SWITCH#show arp
Address                  HWaddress              Interface      Type
192.168.1.238         00:00:00:00:04:86       vlan2         Static
192.168.2.46           00:00:00:00:05:45       vlan3         Static
192.168.3.110         00:00:00:00:08:59       vlan4         Static
192.168.0.12          00:00:00:00:00:09       vlan1         Static
192.168.0.1            00:0e:c6:d8:c7:f7         vlan1          Dynamic
10.100.2.2             00:01:a0:00:10:11       GiE0/2        Dynamic
```

- Show Ipv6 Neighbor Entries

```
SWITCH #show ipv6 neighbors
IPv6 Address                      MAC Address     Interface          Type
ff02::16                          3333.0000.0016   vlan10            dynamic
ff02::1:ff00:1                    3333.ff00.0001   vlan10            dynamic
ff02::1:ff40:251a                 3333.ff40.251a   vlan10            dynamic
```

- Show Routing Table Entries

```
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
C       10.100.2.0/30 is directly connected, gigabitEthernet0/2
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"
C      2001:db8:0:f104::/64 via ::, vlan10, 00:00:56
```

18. Configuring IPv6 Addresses

18.1. Overview of Ipv6 Address

IPv6 (Internet Protocol Version 6) is the second-generation standard protocol of the network layer protocol, also known as IPng (IP Next Generation). It is a set of specifications designed by the Internet Engineering Task Force (IETF) and is an upgraded version of IPv4 (Internet Protocol Version 4).

18.2. IPv6 Address

The total length of an IPv6 address is 128 bits, usually divided into 8 groups, each group is in the form of 4 hexadecimal numbers, and each group of hexadecimal numbers is separated by a colon. For example: FC00:0000:130F:0000:0000:09C0:876A:130B, which is the preferred format of an IPv6 address.

For the convenience of writing, IPv6 also provides a compressed format. Taking the above IPv6 address as an example, the specific compression rules are as follows:

- The leading "0" in each group can be omitted, so the above address can be written as: FC00:0:130F:0:0:9C0:876A:130B.
- Two or more consecutive groups of 0s contained in the address can be replaced by double colons "::", so the above address can be further abbreviated as: FC00:0:130F::9C0:876A:130B.

IPv6 addresses are divided into three types: unicast addresses, anycast addresses, and multicast addresses. Compared with IPv4, the broadcast address type is cancelled and replaced by a richer multicast address, and the anycast address type is added.

18.2.1. IPv6 Unicast Address

An IPv6 unicast address identifies an interface. Since each interface belongs to a node, the unicast address on any interface of each node can identify the node. Messages sent to a unicast address are received by the interface identified by the address.

IPv6 defines multiple unicast addresses. The commonly used unicast addresses are: unspecified address, loopback address, global unicast address, link-local address, and unique local address (ULA).

- Unspecified Address

The unspecified address in IPv6 is 0:0:0:0:0:0:0:0/128 or ::/128. This address can indicate that an interface or node does not have an IP address and can be used as the source IP address of some messages (for example, it will appear in the duplicate address detection of NS messages). Messages with the source IP address of :: will not be forwarded by routing devices.

- Loopback Address

The loopback address in IPv6 is 0:0:0:0:0:0:0:1/128 or ::1/128. The loopback has the same function as 127.0.0.1 in IPv4 and is mainly used for the device to send packets to itself. This address is usually used as the address of a virtual interface (such as a loopback interface). The loopback address cannot be used as the source IP address or destination IP address in the actual data packet sent.

- Global Unicast Address

A global unicast address is an IPv6 address with a global unicast prefix, which acts like a public address in IPv4. This type of address allows aggregation of routing prefixes, thereby limiting the number of global routing table entries.

- Link-local Address

The link-local address is a limited-scope address type in IPv6 and can only be used between nodes connected to the same local link. It uses the specific link-local prefix FE80::/10 (the highest 10 bits are

1111111010), and adds the interface identifier as the lower 64 bits of the address.

- Unique Local Address

Unique local addresses are another type of address with limited scope, which can only be used within a site. Due to the deprecation of site-local addresses (RFC3879), unique local addresses are used to replace site-local addresses.

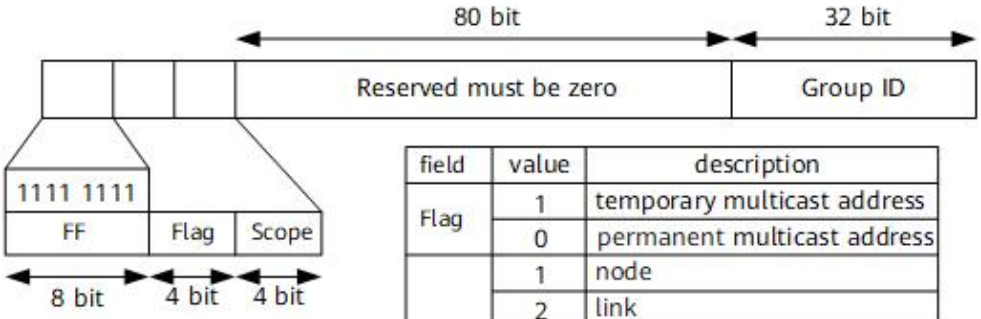
The role of a unique local address is similar to that of a private network address in IPv4. Any organization that has not applied for a global unicast address assigned by a provider can use a unique local address. A unique local address can only be routed and forwarded within a local network and will not be routed and forwarded in the global network.

18.2.2. IPv6 Multicast Address

IPv6 multicast is the same as IPv4 multicast, which is used to identify a group of interfaces, which generally belong to different nodes. A node may belong to 0 or more multicast groups. Messages sent to a multicast address are received by all interfaces identified by the multicast address. For example, the multicast address FF02::1 represents all nodes in the link-local scope, and the multicast address FF02::2 represents all routers in the link-local scope.

An IPv6 multicast address consists of four parts: prefix, flag field, scope field, and multicast group ID:

- Prefix: The prefix of the IPv6 multicast address is FF00::/8.
- Flag field: 4 bits in length. Currently, only the last bit is used (the first three bits must be set to 0). When the value of this bit is 0, it indicates that the current multicast address is a permanent address assigned by IANA. When the value of this bit is 1, it indicates that the current multicast address is a temporary multicast address (non-permanently assigned address).
- Scope field: 4 bits in length, used to limit the range within which the multicast data stream is sent in the network. Figure 9-5 shows the correspondence between the value and meaning of this field.
- Multicast group ID: 112 bits in length, used to identify the multicast group. Currently, RFC2373 does not define all 112 bits as group IDs, but recommends using only the lowest 32 bits of the 112 bits as multicast group IDs, and setting the remaining 80 bits to 0. In this way, each multicast group ID is mapped to a unique Ethernet multicast MAC address (RFC2464).



field	value	description
Flag	1	temporary multicast address
	0	permanent multicast address
Scope	1	node
	2	link
	4	management
	5	site
	8	organization
	E	global
	the rest	unsigned or reserved

IPv6 multicast address format

18.2.3. IPv6 Anycast Address

An anycast address identifies a set of network interfaces (usually belonging to different nodes). A packet

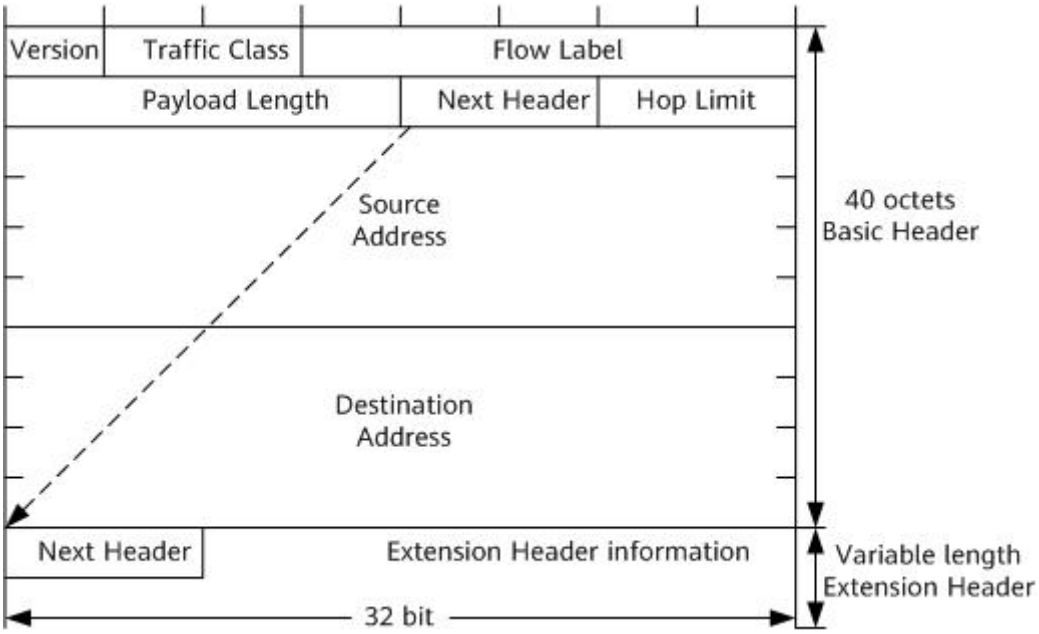
destined for an anycast address is sent to the network interface that is closest to it in terms of routing.
Anycast addresses are designed to provide redundancy and load sharing when providing the same service to multiple hosts or nodes. Currently, anycast addresses are used by sharing unicast addresses. A unicast address is assigned to multiple nodes or hosts. If there are multiple routes to the address in the network, when the sender sends a datagram with the anycast address as the destination IP, the sender cannot control which device can receive it, which depends on the calculation result of the routing protocol in the entire network. This method can be applied to some stateless applications, such as DNS.
IPv6 does not specify a separate address space for anycast, and anycast addresses and unicast addresses use the same address space. Currently, anycast in IPv6 is mainly used in mobile IPv6.

18.3. IPv6 Message Format

An IPv6 message consists of three parts: an IPv6 basic header, an IPv6 extension header, and an upper-layer protocol data unit.
An upper layer protocol data unit generally consists of an upper layer protocol header and its payload, and the payload may be an ICMPv6 message, a TCP message or a UDP message.

- IPv6 Basic Header

The IPv6 basic header has 8 fields and a fixed size of 40 bytes. Every IPv6 datagram must contain a header. The basic header provides basic information for packet forwarding and will be parsed by all devices on the forwarding path.



IPv6 basic header format

The main fields in the IPv6 header format are explained as follows:
Version: Version number, 4 bits in length. For IPv6, the value is 6.
Traffic Class: Traffic class, 8 bits in length. Equivalent to the TOS field in IPv4, it indicates the class or priority of the IPv6 datagram and is mainly used for QoS.
Flow Label : Flow label, length is 20 bits. A new field in IPv6, used to distinguish real-time traffic. Different flow labels + source addresses can uniquely identify a data flow. Intermediate network devices can distinguish data flows more efficiently based on this information.
Payload Length: Payload length, 16 bits. Payload refers to the other parts of the datagram that follow

the IPv6 header (i.e., the extension header and the upper-layer protocol data unit). This field can only represent a payload with a maximum length of 65535 bytes. If the payload length exceeds this value, this field will be set to 0, and the payload length will be represented by the Extra Large Payload Option in the Hop-by-Hop Options extension header.

Next Header: Next header, length 8 bits. This field defines the type of the first extension header (if any) following the IPv6 header, or the protocol type in the upper-layer protocol data unit.

Hop Limit: Hop limit, length is 8 bits. This field is similar to the Time to Live field in IPv4. It defines the maximum number of hops that an IP datagram can go through. The value is reduced by 1 for each device it passes through. When the value of this field is 0, the datagram will be discarded.

Source Address: Source address, length is 128 bits. Indicates the address of the sender.

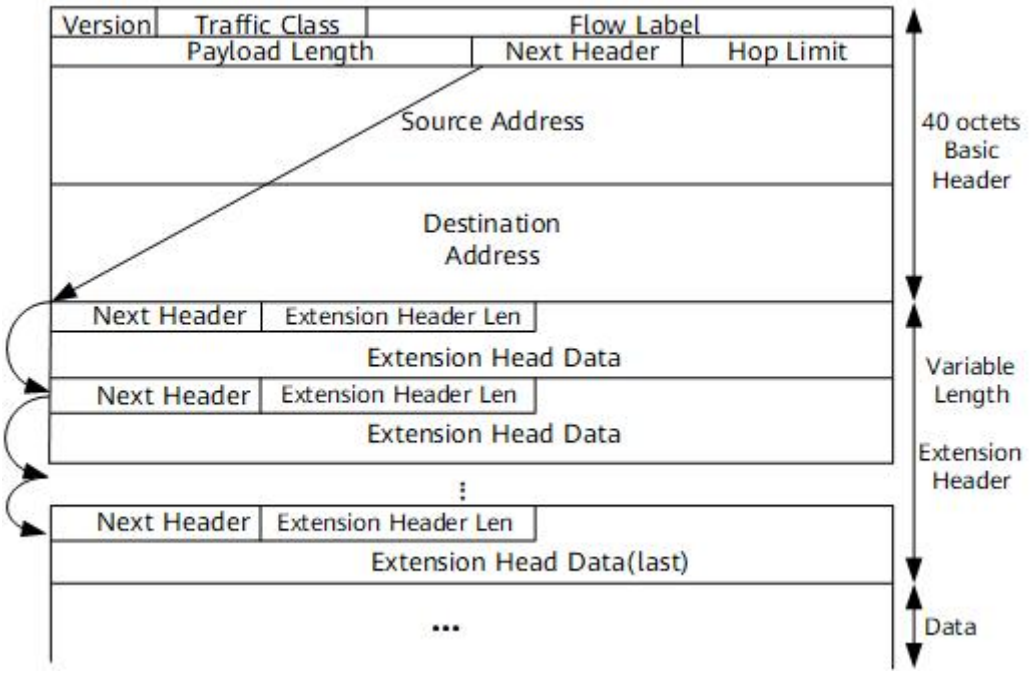
Destination Address: Destination address, 128 bits in length, indicating the address of the recipient.

Compared with IPv4, IPv6 removes the IHL, identifiers, Flags, Fragment Offset, Header Checksum, Options, and Padding fields, and only adds the flow label field. Therefore, the processing of the IPv6 message header is greatly simplified compared with IPv4, which improves the processing efficiency. In addition, in order to better support the processing of various options, IPv6 proposes the concept of extended headers. When adding new options, it is not necessary to modify the existing structure. In theory, it can be expanded infinitely, which reflects excellent flexibility.

- IPv6 Extension Header

In IPv4, the IPv4 header contains optional fields called Options, which include security, timestamp, and record route. These options can extend the length of the IPv4 header from 20 bytes to 60 bytes. During forwarding, processing IPv4 packets carrying these options will occupy a lot of device resources, so they are rarely used in practice.

IPv6 strips these Options from the IPv6 basic header and puts them into the extension header, which is placed between the IPv6 header and the upper-layer protocol data unit. An IPv6 message can contain 0, 1, or more extension headers. The sender will only add one or more extension headers when the device or destination node needs to do some special processing. Unlike IPv4, the IPv6 extension header can be of any length and is not limited to 40 bytes, which makes it easier to add new options in the future. This feature, coupled with the way options are processed, allows IPv6 options to be truly utilized. However, in order to improve the performance of processing option headers and transport layer protocols, the extension header is always an integer multiple of 8 bytes in length.



IPv6 extension header format

The main fields in the IPv6 extension header are explained as follows:

Next Header: The next header is 8 bits long. It has the same function as the Next Header of the basic header. It indicates the next extension header (if it exists) or the type of the upper layer protocol.

Extension Header Len: Header extension length, 8 bits long. Indicates the length of the extension header (excluding the Next Header field).

Extension Header Data: Extension header data, with variable length. The content of the extension header is a combination of a series of option fields and padding fields.

Currently, RFC 2460 defines six IPv6 extension headers: Hop-by-Hop Options Header, Destination Options Header, Routing Header, Fragmentation Header, Authentication Header, and Encapsulating Security Payload Header.

18.4. Configuration Notes

- IPv6 addresses support one of three methods: static configuration, SLAAC configuration, and RA + DHCPv6 configuration . Multiple addresses cannot be shared.
- ND attributes, including the configuration of receiving the default route, must be configured before the address configuration command, otherwise they will not take effect.
- an interface is configured with an IPv6 static address, the device supports the basic RA route advertisement function.

18.5. Configuring

18.5.1. Interface Configuration Commands

- Configure IPv6 Addresses on Interfaces

Command	SWITCH(config- if)# **ipv6 address** { **dhcp** | **autoconfig** | X:X::X:X/M } SWITCH(config-if)#**no ipv6 address**

Description	Configure an IPv6 address for the interface.

- Configure the Interface to Receive RA Advertisements

Command	SWITCH(config-if)# **ipv6 nd accept-router** SWITCH(config-if)# **no ipv6 nd accept-router**
Description	Configure the interface receives the default route advertised by RA. Supported only in SLAAC and DHCPv6 modes . Optional. By default, the default route advertised by RA is not received.

- Interface Configuration to Send RA Routing Advertisements

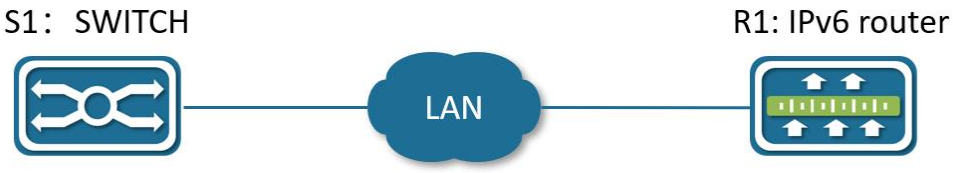
Command	SWITCH(config-if)# **no ipv6 nd suppress-ra** SWITCH(config-if)# **ipv6 nd suppress-ra**
Description	The RA route advertisement service can be enabled only when a static IPv6 address is configured on the interface . Optional. RA route advertisement is suppressed/disabled by default.

18.6. Examples

18.6.1. Conventional SLAAC Address Allocation Scenario

1) Requirement : Switch S1 dynamically obtains an IPv6 address from R1 through the SLAAC protocol

2) Network Diagram



Typical network diagram of SLAAC address allocation

3) Typical Configuration Examples

S1 Configuration :

```
SWITCH(config)#int vlan 1
SWITCH(config-if)# ipv6 nd accept-router
SWITCH(config-if)#ipv6 address autoconfig
```

R1 Configuration :

```
interface VLAN 1
ipv6 address A::A/64
no ipv6 nd suppress-ra
```

18.7. Display Information

- Display Interface IPv6 Address Information

```
SWITCH#show ipv6 interface brief
Interface IPv6-Address            Admin-Status
GiE0/6 *a::76a9:12ff:fe12:312 [up/up]

* address is assigned by SLAAC or DHCPv6 client
```

- Display IPv6 Routing Information

```
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 [0/1024] via fe80::c670:abff:fef4:d6df, gigabitEthernet0/6, 00:01:56
C a::/64 via ::, gigabitEthernet0/6, 00:01:56
```

19. Configuring the DHCP Client

19.1. Overview of DHCP Client

DHCP (Dynamic Host Configuration Protocol) is a network protocol for local area networks that uses the 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 from the DHCP server by sending a request message. When the DHCP client and the server are not on the same subnet, a DHCP relay agent (DHCP Relay) is required to forward DHCP request and response messages.

19.1.1. Protocol Standards

RFC2132 DHCP Options and BOOTP Vendor Extensions. S. Alexander, R. Droms. March 1997. (Format: TXT, HTML) (Obsoletes RFC1533) (Updated by RFC3442, RFC3942, RFC4361, RFC4833, RFC5494) (Status: DRAFT STANDARD) (DOI: 10.174 87/RFC2132)

19.2. Configuration Notes

- The device interface IPv4 address can be either static IP or DHCP dynamic IP. The two methods are mutually exclusive and cannot be shared.
- This document is limited to IPv4 DHCP client. For IPv6 and DHCPv6 client , please refer to the IPv6 configuration section.

19.3. Configuring

19.3.1. Interface Configuration Commands

- Enable /disable DHCP Client on the Interface

Command	SWITCH(config-if) **#ip address dhcp** SWITCH(config-if)# **no ip address**
Description	Enable or disable the DHCP client on the interface .

- Configure DHCP Parameters on the Interface

Command	SWITCH(config- if)# **ip dhcp client request routers** SWITCH(config- if)# **no ip dhcp client request routers**
Description	Interface parameter configuration . Configure whether to request and apply the default route of the DHCP server. Enabled by default, optional configuration.

19.4. Examples

19.4.1. Conventional DHCP Server Address Allocation Scenario

4) Requirements : The switch is connected to a DHCP server and obtains an IP address dynamically through the DHCP protocol.

5) Typical Configuration Examples

Switch configuration:

```
SWITCH(config) #interface vlan1
SWITCH(config-if)#ip address dhcp
```

DHCP server configuration:

```
service dhcp
!
ip dhcp pool a
   network 2.2.2.0 255.255.255.0 2.2.2.10 2.2.2.100
```

6) Check the IP address obtained by the switch

```
 SWITCH#show ip interface brief
 Interface IP-Address Admin-Status Link-Status
 vlan1 *2.2.2.12 up up

 * address is assigned by DHCP client
```

19.5. Display Information

- Display IP Address Allocation

```
SWITCH#show ip interface brief
Interface IP-Address Admin-Status Link-Status
vlan1 *2.2.2.12 up up

* address is assigned by DHCP client
```

- Display the Default Route Assignment

```
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 2.2.2.10 to network 0.0.0.0

S* 0.0.0.0/0 [0/0] via 2.2.2.10, vlan1
C 2.2.2.0/24 is directly connected, vlan1
```

20. Configuring ACL

20.1. Overview of ACL

The ACL Implement packet filtering by configuring matching rules and processing operations for packets. The ACL can effectively prevent illegal users from accessing the network, and can also control traffic and save network resources.

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

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

Standard IP-based ACL: Make rules based only on the source IP address of the packet.

Extended IP-based 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.

IPV6-based ACL: develop rules based on the source IPV6 address, destination IPV6 address, protocol, etc. of the data packet.

20.2. Configuring

20.2.1. Configure IP Standard ACL

- Configure IP-based Standard ACL Rules

Command	SWITCH(config)# **ip-access-list** {<1-99> | <1300-1999>} {**permit** | **deny**} {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} SWITCH(config)# **no ip-access-list** {<1-99> | <1300-1999>}
Description	Create /delete standard IP-based ACL rules

- Create a Standard IP ACL

Command	SWITCH(config)# **ip-access-list standard** {<1-99> | <1300-1999> | NAME} SWITCH(config)# **no ip-access-list standard** {<1-99> | <1300-1999> | NAME}
Description	Create/delete standard IP ACL and switch to IP standard ACL mode

- Configure Standard IP ACL Rules

Command	SWITCH(config-std-acl)# [SN] {**permit** | **deny**} {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} SWITCH(config-std-acl)# no {**permit** | **deny**} {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} SWITCH(config-std-acl)# **no** SN
Description	Create/delete a standard IP ACL rule SN: Serial number of each rule (1-2147483647)

20.2.2. Configure IP Extended ACL

- Configure IP-based Extended ACL Rules

Command	SWITCH(config)# **ip-access-list** {<100-199> | <2000-2699>} {**permit** | **deny**} PROTOCOL {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} [**eq** SPORT] {**host** | DIPADDR DIPADDRMASK | **any**} [**eq** DPORT] SWITCH(config)# **no ip-access-list** {<100-199> | <2000-2699>}
Description	Create /delete IP-based extended ACL rules PROTOCOL list: <0-255>: Specify the ID of the protocol any: any protocol message gre: GRE message icmp: ICMP message igmp: IGMP message ip: IPv4 message (0x4) ipcomp: IPComp message ospf: OSPF message pim: PIM message rsvp: RSVP message tcp: TCP message udp: UDP message vrrp: VRRP message The eq option is only available for TCP and UDP protocols. For the following port number names, you can use the port number name or port number to specify a specific port: TCP port number list: <0-65535> Specify port number bgp (179) ftp (21) ftp-data (20) Login (513) pop2 (109) pop3 (110) smtp (25) telnet (23) www (80) UDP port number list: <0-65535> Specify port number bootpc (68) boots (67) domain (53) echo (7) rip (520) snmp (161) syslog (514) tftp (69)

- Create Extended IP ACL

Command	SWITCH(config)# **ip-access-list extended** {<100-199> | <2000-2699> | NAME} SWITCH(config)# **no ip-access-list extended** {<100-199> | <2000-2699> | NAME}
Description	Create/delete extended IP ACL and switch to IP extended ACL mode

- Configure Extended IP ACL Rules

Command	SWITCH(config-ext-acl)# [SN] {**permit** | **deny**} PROTOCOL {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} [**eq** SPORT] {**host** DIPADDR | DIPADDR DIPADDRMASK | **any**} [**eq** DPORT] SWITCH(config-ext-acl)# **no** {**permit** | **deny**} PROTOCOL {**host** SIPADDR | SIPADDR SIPADDRMASK | **any**} [**eq** SPORT] {**host** DIPADDR | DIPADDR DIPADDRMASK | any} [**eq** DPORT] SWITCH(config-ext-acl)# **no** SN
Description	Create/delete an extended IP ACL rule SN: Serial number of each rule (1-2147483647) PROTOCOL list:

	<0-255>: Specify the ID of the protocol any: any protocol message gre: GRE message icmp: ICMP message igmp: IGMP message ip: IPv4 message (0x4) ipcomp: IPComp message ospf: OSPF message pim: PIM message rsvp: RSVP message tcp: TCP message udp: UDP message vrrp: VRRP message For the following port number names, you can use the port number name or port number to specify a specific port: eq (TCP and UDP only) TCP port number list: <0-65535> Specify port number bgp (179) ftp (21) ftp-data (20) Login (513) pop2(109) pop3(110) smtp (25) telnet (23) www (80) UDP port number list: <0-65535> Specify port number bootpc (68) boots (67) domain (53) echo (7) rip (520) snmp (161) syslog (514) tftp (69)

20.2.3. Configure MAC ACL

- Configure MAC-based ACL Rules

Command	SWITCH(config)# **mac-access-list** <200-699> {**permit** | **deny**} {**host** SMAC | SMAC SMACMASK | **any**} {**host** DMAC | DMAC DMACMASK | **any**} [**ethertype** ETYPE] [**cos** VALUE] SWITCH(config)# **no mac-access-list** <200-699>
Description	Create/delete MAC-based ACL rules ethertype: Ethernet protocol type (0x05DD-0xFFFF) cos: priority value of the message (0-7)

- Create MAC ACL

Command	SWITCH(config)# **mac-access-list** {<200-699> | NAME} SWITCH(config)# **no mac-access-list** {<200-699> | NAME}
Description	Create/delete standard MAC ACL and switch to MAC ACL mode

- Configure MAC ACL Rules

Command	SWITCH(config-mac-acl)# [SN] {**permit** | **deny**} {**host** SMAC | SMAC SMACMASK | **any**} {**host** DMAC | DMAC DMACMASK | **any**} [**ethertype** ETYPE] [cos VALUE] SWITCH(config-mac-acl)# **no** {**permit** | **deny**} {**host** SMAC | SMAC SMACMASK | **any**} {**host** DMAC | DMAC DMACMASK | **any**} [**ethertype** ETYPE] [**cos** VALUE]

	SWITCH(config-mac-ext-acl)# **no** SN
Description	Create/delete a MAC ACL rule SN: Serial number of each rule (1-2147483647) ethertype: Ethernet protocol type (0x05DD-0xFFFF) cos: priority value of the message (0-7)

20.2.4. Configure IPv6 ACL

- Create IPv6 ACL

Command	SWITCH(config)# **ipv6-access-list** {NAME} SWITCH(config)# **no ipv6-access-list** {NAME}
Description	Create/delete IPV6 ACL and switch to IPV6 ACL mode

- Configure IPV6 ACL Rules

Command	SWITCH(config-ipv6-acl)# [SN] {**permit** | **deny**} [PROTOCOL] {SOURCE-IPV6-PREFIX/PREFIX-LENGTH | **any** | **host** SOURCE-IPV6-ADDRESS} [**eq** SPORT] {DESTINATION- IPV6-PREFIX / PREFIX-LENGTH | **any** | **host** DESTINATION-IPV6-ADDRESS} [**eq** DPORT] SWITCH(config-ipv6-acl)# **no** {**permit** | **deny**} [PROTOCOL] {SOURCE-IPV6-PREFIX/PREFIX-LENGTH | **any** | **host** SOURCE-IPV6-ADDRESS} [**eq** SPORT] {DESTINATION- IPV6-PREFIX / PREFIX-LENGTH | **any**| **host** DESTINATION-IPV6-ADDRESS} [**eq** DPORT] SWITCH(config-ipv6-acl)# **no** SN
Description	Create/delete an IPV6 ACL rule SN: Serial number of each rule (1-2147483647) PROTOCOL list: <0-255>: Specify the ID of the protocol any: any protocol message icmp: ICMP message tcp: TCP message udp: UDP message For the following port number names, you can use the port number name or port number to specify a specific port: eq (TCP and UDP only) TCP port number list: <0-65535> Specify port number bgp (179) ftp (21) ftp-data (20) login (513) pop2 (109) pop3 (110) smtp (25) telnet (23) www (80) UDP port number list: <0-65535> Specify port number biff (512) bootpc (68) boots (67) discard (9) dnsix (195) domain 53) echo (7) Isakmp (500) ntp (123) pim-auto-rp (496) rip (520) snmp (161)

	snmptrap (162) tftp (69)

Note

- Up to 128 rules can be configured under a single ACL-ID;
- Mask inversion, if it matches an IP address in the 192.168.1.0/24 range, 192.168.1.0 0.0.0.255 should be configured;
- The name of the ACL can be named, and the first character cannot be a number;
- MAC ACL does not take effect on IPV6 packets;
- The final default configuration of each ACL is deny any item;

20.2.5. Other Configuration Items

- Configure ACL Counters

If the user wants to start the packet matching counting function on the access list, please enable it in the access list.

Command	SWITCH(config-std-acl)# **counter enable** SWITCH(config-std-acl)# **no counter enable**
Description	Enable / disable ACL counter in all ACL modes

- Clear ACL Counter

Command	SWITCH# **clear access-list counter** NAME
Description	Clear the ACL count value

- Configure ACL Descriptor

Command	SWITCH(config-std-acl)# **description** TEXT SWITCH(config-std-acl)# **no description**
Description	Configure/delete ACL descriptors TEXT: descriptor (up to 64 characters) Configurable in all ACL modes

- Trigger ACL Sequence Number Reordering

SN is the sequence number of the rule entry, and the value range is [1,2147483647]. This sequence number determines the priority of this rule entry in the access list. The smaller the sequence number, the greater the priority. The packet with the higher priority will be matched first. If the sequence number is not specified when configuring the matching rule, the system will automatically Assign a sequence number, the starting value of the sequence number is 10, and the increment value is 10.

Command	SWITCH(config-std-acl)# **resequence** START STEP SWITCH(config-std-acl)# **no resequence**
Description	Reorder serial numbers START: starting position (default value: 10, range <1-2147483647>) STEP: step size (default value: 10, range <1-2147483647>)

	Configurable in all ACL modes

Note

✦ The serial number is unique;

✦ When configuring an ACL entry, if the sequence number is not specified, it will be specified in steps after the current maximum sequence number (rules cannot be added if it exceeds the set range);

- Applying ACL to an Interface

Command	SWITCH(config-if)# **access-group** ACLNAME {**in** | **out**} SWITCH(config-if)# **no access-group** ACLNAME {**in** | **out**}
Description	Configure/delete ACL applied to the port

- Apply ACL to a VLAN

Command	SWITCH(config)#**access-group** ACLNAME { **in** | **out** } **vlan** <1-4094> SWITCH(config-if)#**no access-group** ACLNAME { **in** | **out** } **vlan** <1-4094>
Description	Configure/delete ACL applied to a VLAN

Note

✦ When the ACL has been applied to the port or configured as a QOS flow matching rule, if you need to add or delete a rule, you need to first unapply it from the interface or QOS flow matching rule;

✦ The aggregation port does not support ACL application in the out direction, and the member ports of the aggregation port do not support ACL application;

✦ ACL applications not supported by VLAN interfaces;

20.3. Examples

Case 1: Filter the incoming packets of port gigabitEthernet0/1, release the packets with SIP 192.168.1.0/24, and discard other packets.

- Configure ACL rules:

```
SWITCH(config)#ip-access-list 1 permit 192.168.1.0 0.0.0.255
```

or

```
SWITCH(config)#ip-access-list standard 1
SWITCH(config-std-acl)#permit 192.168.1.0 0.0.0.255
```

- Apply ACL to port gigabitEthernet0/1

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#access-group 1 in
```

Case 2: Filter the entry packets of port gigabitEthernet0/1 and reject the packets sent by the host IP 192.168.1.2 with the packet type TCP and the source port number 40. Other packets will pass.

- Configure ACL rules:

```
SWITCH(config)#ip-access-list 100 deny tcp host 192.168.1.2 eq 40 any
SWITCH(config)#ip-access-list 100 permit any any any
```

or

```
SWITCH(config)#ip-access-list extended 100
SWITCH(config-ext-acl)#deny tcp host 192.168.1.2 eq 40 any
SWITCH(config-ext-acl)#permit any any any
```

- Apply ACL to port gigabitEthernet0/1

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#access-group 100 in
```

Case 3: Filter the export packets of port gigabitEthernet0/1 and reject the Ethernet type 0x804 packets sent by the host with MAC 0000.0047.5124. Other packets will pass.

- Configure ACL rules:

```
SWITCH(config)# mac-access-list 200 deny host 0000.0047.5124 any ethertype
0x804
SWITCH(config)# mac-access-list 200 permit any any
```

or

```
SWITCH(config)#mac-access-list 200
SWITCH(config-mac-acl)#deny host 0000.0047.5124 any ethertype 0x804
SWITCH(config-mac-acl)#permit any any
```

- Apply ACL to port gigabitEthernet0/1

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#access-group 200 out
```

Case 4: Filter the ingress packets of port gigabitEthernet0/1 , release the packets with the IPv6 address of the destination host::D0F8:1900:9F51:0000 , and discard other packets.

- Configure ACL rules:

```
SWITCH(config)#ipv6-access-list ip6-acl
SWITCH(config-ipv6-acl)#permit any any host ::D0F8:1900:9F51:0000
```

- Apply ACL to port gigabitEthernet0/1

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#access-group ip6-acl in
```

Case 5: Filter the incoming packets of port gigabitEthernet0/1, release the packets with SIP 192.168. 2. 1, discard other packets , and turn on the counter to view packet statistics .

- Configure ACL rules:

```
SWITCH(config)#ip-access-list standard 1
SWITCH(config-std-acl)#permit host 192.168.2.1
SWITCH(config-std-acl)#counter enable
```

- Apply ACL to port gigabitEthernet0/1

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#access-group 1 in
```

- port gigabitEthernet0/1 , send 10 packets with SIP 192.168.2.1 and SIP 192.168.2.2, check the packet statistics

```
SWITCH#show access-list 1
ip-access-list standard 1
10 permit host 192.168.2.1(10 match)
deng any (10 match)
```

20.4. Display Information

- Display ACL Information

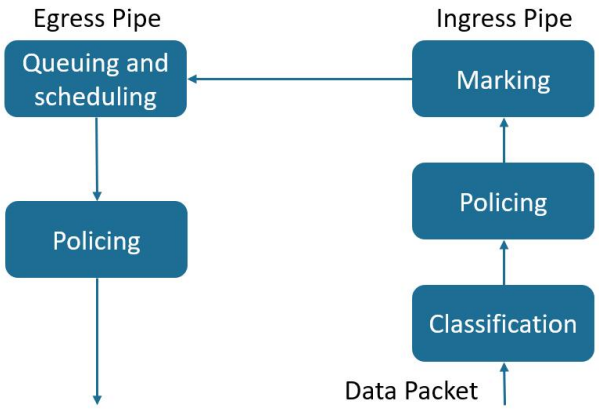
```
SWITCH#show access-list 1
  ip-access-list standard 1
  10 permit host 1.1.1.1
  deny any

SWITCH#show access-list 200
  mac-access-list 200
   10 permit host  0001.0002.0003 any
   deny any

SWITCH#show access-list ip6-acl
  ipv6-access-list ip6-acl
  10 permit tcp host a::1 eq bgp any
  deny any
```

21. Configuring QoS

21.1. Overview of QoS

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped. When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The QoS implementation is based on the Differentiated Services (Diff-Serv) architecture, an emerging standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network. The following Figure shows the model of the QoS.



Classification

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, so no classification occurs.

During classification, the switch performs a lookup and assigns a QoS label to the packet. The QoS label identifies all QoS actions to be performed on the packet and from which queue the packet is sent.

The QoS label is based on the DSCP or the CoS value in the packet and decides the queueing and scheduling actions to perform on the packet. The label is mapped according to the trust setting and the packet type.

Trust CoS:

- QoS with CoS label.
- For tagged packets, the CoS uses the CoS information in the tag.
- For packets without tags, the CoS adopts the default CoS value of the port.

Trust DSCP:

- For non-IP packets, the QoS is labeled with CoS; for packets with tags, CoS uses the CoS information in the tag; for packets without tags, the CoS uses the default CoS of the port.
- For IP packets, QoS has a DHCP label; select the DSCP value of the packet.

No trust:

- QoS with CoS label
- CoS adopts the default CoS value of the port.

Policing(Ingress)

The ingress policer meters the given flow and classifies as either in-profile or out-of-profile. Out-of-profile packets may be discarded or have their QOS attributes remarked.

Marking

After a packet is classified and has a DSCP-based or CoS-based QoS label assigned to it, the marking process can begin.

For packets with CoS labels:

- Use the configured CoS-to-DSCP mapping relationship to generate DSCP values for packets.
- Select the egress queue for the packet through the CoS-to-Queue mapping relationship.

For packets with DSCP labels

- Modify the DSCP value of the packet through the DSCP-to-DSCP mapping relationship.
- Generate a new CoS value for the packet through the DSCP-to-CoS mapping relationship.
- Select the egress queue for the packet through the DSCP-to-Queue mapping relationship.

Queuing and scheduling

Generally, there are 8 queues for QoS exit, which map the 0-7 priority relationship of CoS. The packet enters the corresponding egress queue according to the final marked CoS and CoS-to-Queue relationship. For the priority of packet processing in the egress queue, there are the following algorithms:

- WRR：The weight scheduling algorithm processes the packets in each queue in turn. The weight configuration can be used to change the number of queue packets processed in each cycle. The larger the weight, the higher the queue priority.
- SP： Strict scheduling algorithm, traverse queue 7 to queue 0 in each loop, when the initial processing of the packets in the high-priority queue ends, continue to process the low-priority queue.
- SP+WRR：The combination of WRR and SP, the global WRR mode, supports a specific queue configured as SP mode, and the queue configured as SP mode is a high-priority queue, which is processed first.

Policing(Egress)

The egress policer meters the given flow and classifies as either in-profile or out-of-profile. Out-of-profile packets may be discarded.

21.2. Configuring

- Enabling QoS Globally

Command	SWITCH(config)#**mls qos enable** SWITCH(config)#**no mls qos**
Description	Enabling QoS Globally. Default is disabled.

- Configuring Scheduling algorithm

Command	SWITCH(config)#**mls qos algorithm** {**sp** | **wrr**}
Description	Configuring the queue scheduling algorithm, support two modes: wrr and sp.

- Configuring Queue Wrr-weight

Command	SWITCH(config)#**mls qos weight** <0-7> <0-32>

Description	Configure the queue weight. The queue weight is only valid for wrr mode. The default weight of all queues is 1. When in wrr mode, configure the queue weight to 0, the queue will schedule in sp mode.

- Configuring Trust Mode on the Interface

Command	SWITCH(config-if)#**mls qos trust** {**cos	dscp**} SWITCH(config-if)#**no mls qos trust**
Description	Configure the port trust mode, the default is not trust mode. When in no trust mode, the CoS field and DHCP field of the packet will be modified according to the default CoS of the port. When in trust cos mode, the same as the no trust mode for untagged packets, and for tagged packets, use the own CoS of the packet. When configuring trust dscp mode, for ip packets, select the packet with DSCP, and for non-ip packets, the same as trust cos mode.

- Configuring Default CoS on the interface

Command	SWITCH(config-if)#**mls qos cos** <0-7> SWITCH(config-if)#**no mls qos cos**
Description	Configure the default CoS of the port. The default CoS takes effect for the ingress packets without tags. The default port cos is 0.

- Configuring CoS-to-DSCP Mapping

Command	SWITCH(config)#**mls qos cos-dscp** <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> SWITCH(config)#**no mls qos cos-dscp**
Description	Configure CoS-to-DSCP mapping. Default CoS-to-DSCP mapping: 0-0, 1-8, 2-16, 3-24, 4-32, 5-40, 6-48, 7-56.

- Configuring CoS-to-Queue Mapping

Command	SWITCH(config)#**mls qos cos-queue** <0-7> <0-7> SWITCH(config)#**no mls qos cos-queue** <0-7>
Description	Configure CoS-to-Queue mapping. Default CoS-to-Queue mapping: 0-0, 1-1, 2-2, 3-3, 4-4, 5-5, 6-6, 7-7.

Note

When the configured port is no trust, trust cos or trust dscp and the port is not ip: the cos-dscp configuration takes effect, modify the packet dscp according to the mapping relationship, and the cos-queue configuration takes effect, modify the packet export queue according to the mapping relationship.

- Configuring DSCP-to-CoS Mapping

Command	SWITCH(config)#**mls qos dscp-cos** <0-63> to <0-7> SWITCH(config)#**no mls qos dscp-cos**
Description	Configure DSCP-to-CoS mapping. Default DSCP-to-CoS mapping: <0-7>-0, <8-15>-1, <16-23>-2, <24-31>-3, <32-39>-4, <40-47>- 5, <48-55>-6, <56-63>-7.

- Configuring DSCP-to-DSCP Mapping

Command	SWITCH(config)#**mls qos dscp-mutation** <0-63> to <0-63> SWITCH(config)#**no mls qos dscp-mutation**

Description	Configure DSCP-to-DSCP mapping.

- Configuring DSCP-to-Queue Mapping

Command	SWITCH(config)#**mls qos dscp-queue** <0-63> <0-7> SWITCH(config)#**no mls qos dscp-queue** <0-63>
Description	Configure DSCP-to-Queue mapping. Default DSCP-to-Queue mapping: <0-7>-0, <8-15>-1, <16-23>-2, <24-31>-3, <32-39>-4, <40-47>- 5, <48-55>-6, <56-63>-7.

Note

When configuring the port as trust dscp and ip packets: the dscp-cos configuration takes effect, modify the packet dscp according to the mapping relationship, and the dscp-queue configuration takes effect, and modify the packet egress queue according to the mapping relationship. When a colleague configures dscp-dscp at the same time, first perform dscp-dscp conversion, and then perform dscp-cos mapping as a result.

- Creating Class-map

Command	SWITCH(config)#**class-map** CNAME SWITCH(config-cmap)# SWITCH(config)#**no class-map** CNAME
Description	Create class-map. After creating a class-map, automatically enter the class-map mode.

- Configuring Class-map Maching Rule

Command	SWITCH(config-cmap)# **match access-group** ACLNAME SWITCH(config-cmap)#**no match access-group** ACLNAME
Description	Configure to match ACL entries for class-map.

Command	SWITCH(config-cmap)#**match ip-dscp** <0-63> SWITCH(config-cmap)#**no match ip-dscp**
Description	Configure to match the DHCP field in the IP packet, up to 64 different DHCP values can be configured.

Command	SWITCH(config-cmap)#**match cos** <0-7> SWITCH(config-cmap)#**no match cos**
Description	Configure to match the CoS field in the packet, up to 8 different CoS values can be configured.

Command	SWITCH(config-cmap)#**match ethertype** ETYPE SWITCH(config-cmap)#**no match ethertype**
Description	Configure to match the ethernet protocol type field of the packets.

Command	SWITCH(config-cmap)#**match** {**vlan** <1-4094> | **vlan-range** <1-4094> **to** <1-4094>} SWITCH(config-cmap)**#no match** {**vlan | vlan-range**}

Description	Configure to match vlan field in the packet, support range configuration.

Command	SWITCH(config-cmap)#**match layer4** {**tcp	udp**} {**source-port	destination-port**} VALUE SWITCH(config-cmap)#**no match layer4** {**tcp	udp**} {**source-port	destination-port**} VALUE
Description	Configure to match Layer 4 port fields of TCP and UDP packets.

Command	SWITCH(config-cmap)#**match vlan-range** <1-4094> to <1-4094> **ethertype** ETYPE SWITCH(config-cmap)#**no match vlan-range**
Description	Configure to match vlan and etype fields in the packets.

- Creating Policy-map

Command	SWITCH(config)#**policy-map** PNAME SWITCH(config-pmap)# SWITCH(config)#**no policy-map** PNAME
Description	Configure policy-map

- Attaching Policy-map to Class-map

Command	SWITCH(config-pmap)# **class** CNAME SWITCH(config-pmap-c)# SWITCH(config-pmap)#**no class** CNAME
Description	Attach class-map to policy-map. A policy-map can attach up to 8 class-maps.

- Configuring Action

Command	SWITCH(config-pmap-c)#**set cos** <0-7> SWITCH(config-pmap-c)#**no set cos**
Description	Configure policy action: modify the cos field of packets.

Command	SWITCH(config-pmap-c)#**set ip-dscp** <0-63> SWITCH(config-pmap-c)#**no set ip-dscp**
Description	Configure policy action: modify the ip-dscp field of packets.

Command	SWITCH(config-pmap-c)#**set vlan** <1-4094> SWITCH(config-pmap-c)#**no set vlan**
Description	Configure policy action: modify packet vlan.

Command	SWITCH(config-pmap-c)#**nest vlan** <1-4094> SWITCH(config-pmap-c)#**no nest vlan**
Description	Configure policy action: add external tags to matching packets.

Command	SWITCH(config-pmap-c)#**police cir** <32-1000000> **cbs** <4-31250> **exceed-action drop** SWITCH(config-pmap-c)#**no police**

Description	Configure policy action: rate-limit. Cir is the speed limit water line, in kbps. Cbs is burst capacity, unit Kbyte.

Note

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

- Applying Policy-map on the Interface

Command	SWITCH(config-if)#**service-policy input** PNAME SWITCH(config-if)#**no service-policy input** PNAME
Description	Apply the policy-map on the interface. Only one policy-map can be applied to an interface.

- Configuring Ingress Rate-limit on the interface

Command	SWITCH(config-if)#**rate-limit input** <64-1000000> <32-16384> SWITCH(config-if)#**no rate-limit input**
Description	Configure port ingress rate limit. The first parameter is limit level, in kbps. The second parameter is burst level, in Kbyte.

- Configuring Egress Rate-limit on the interface

Command	SWITCH(config-if)#**rate-limit output** <64-1000000> <32-16384> SWITCH(config-if)#**no rate-limit output**
Description	Configure port egress rate limit. The first parameter is limit value, in kbps. The second parameter is burst value, in Kbyte.

Note

The limit value is determinable. For example, if the speed limit is 1M, then the limit value is 1024, but the burst value is taken from the experience value. When the burst value is large, the flow peak is higher, and the speed limit is stable, but the average rate may be higher than the speed limit value; when the burst value is small, the flow peak is lower, the speed limit fluctuates greatly, and the average rate may be lower than the speed limit value. . It is recommended that the burst configuration be 4 times the limit value.

21.3. Examples

Example 1: This example shows how to Configure ingress and egress rate-limit on the interface.

Step 1: Configuring Ingress rate-limit on interface gigabitEthernet0/1.

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

Step 2: Configuring Egress rate-limit on interface gigabitEthernet0/1.

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

Example 2: This example shows how to configure flow-based rate-limit.

Step 1: Enable QoS globally.

```
SWITCH(config)#mls qos enable
```

Step 2: Create ACL rule.

```
SWITCH(config)#ip-access-list 1 permit 192.168.64.1
```

Step 3: Create class-map, policy-map, attach ACL to the class-map, attach class-map to the policy-map, and configure the policy-map action.

```
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 c1
SWITCH(config-pmap-c)#police cir 1024 cbs 4096 exceed-action drop
```

Step 4: Apply policy-map to the interface.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#service-policy input p1
```

Example 3: This example shows how to configure port-based QoS service, to Implement preferential forwarding of specific port packets.

Step 1: Enable QoS globally.

```
SWITCH(config)#mls qos enable
```

Step 2: Configure interface gigabitEthernet0/1 and gigabitEthernet0/2 trust cos. Set gigabitEthernet0/1 default CoS to 0. Set gigabitEthernet0/2 default CoS to 2.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#mls qos trust cos
SWITCH(config-if)#mls qos cos 0
SWITCH(config-if)#exit
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#mls qos trust cos
SWITCH(config-if)#mls qos cos 2
```

Step 3: Configure CoS-to-Queue mapping.

```
SWITCH(config)#mls qos cos-queue 0 0
SWITCH(config)#mls qos cos-queue 2 2
```

Step 4: Configure scheduling algorithm wrr.

```
SWITCH(config)#mls qos algorithm wrr
```

Step 5: Configuring queue 2 weight 0.

```
SWITCH(config)#mls qos weight 2 0
```

21.4. Display Information

- Display Scheduling Algorithm and Weight Information

```
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
```

- Display CoS-to-DSCP and CoS-to-Queue Mapping Information

```
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
```

- Display DSCP-to-CoS, DSCP-to-DSCP and DSCP-to-Queue Mapping Information

```
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
```

- Display QoS Configuration on the Interfaces

```
SWITCH#show mls qos interfaces
--------------------------------
Interface     Trust mode  Cos
--------------------------------
GiEO/1        Not         0
GiEO/2        Not         0
GiEO/3        Not         0
GiEO/4        Not         0
GiEO/5        Not         0
GiEO/6        Not         0
GiEO/7        Not         0
GiEO/8        Not         0
```

- Display Class-map Configuration

```
SWITCH#show class-map

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

- Display Policy-map Configuration

```
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)
```

- Display Rate-limit Configuration on the Interfaces

```
SWITCH#show rate-limit
-------------------------------------------------------
Interface     In limit  In burst  Out limit  Out burst
-------------------------------------------------------
GiE0/1        --        --        --         --
GiE0/2        --        --        --         --
GiE0/3        1024      4096      --         --
GiE0/4        --        --        --         --
GiE0/5        --        --        --         --
GiE0/6        --        --        --         --
GiE0/7        --        --        --         --
GiE0/8        --        --        --         --
GiE0/9        --        --        --         --
GiE0/10       --        -         1024       4096
```

22. Configuring DHCP Snooping

22.1. Overview of DHCP Snooping

DHCP snooping (Dynamic Host Configuration Protocol) is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. When DHCP snooping is enabled on a VLAN, the system examines DHCP messages sent from untrusted hosts associated with the VLAN and extracts their IP addresses and lease information. This information is used to build and maintain the DHCP snooping database.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

Trusted Sources

The DHCP snooping feature determines whether traffic sources are trusted or untrusted. DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server. The default trust state of all interfaces is untrusted.

DHCP Snooping Limit Rate

Configure the number of DHCP packets per second that an interface can receive, to reduce or eliminate the impact of DHCP packet attack from this interface.

MAC Address Verification

With DHCP snooping MAC address verification enabled, DHCP snooping verifies that the source MAC address and the client hardware address match in DHCP packets that are received on untrusted ports. The source MAC address is a Layer 2 field associated with the packet, and the client hardware address is a Layer 3 field in the DHCP packet.

Option-82 Insertion

DHCP Option82 option is also called DHCP relay agent information option, one of many dhcp options. The Option82 option is a DHCP option proposed to enhance the security of the DHCP server and improve the IP address allocation strategy. The addition and stripping of options are implemented by the relay component.

DHCP Database

The DHCP snooping feature dynamically builds and maintains the database using information extracted from intercepted DHCP messages. The database contains an entry for each untrusted host with a leased IP address if the host is associated with a VLAN that has DHCP snooping enabled. The database does not contain entries for hosts connected through trusted interfaces. When the ip verify source function is enabled on the interface, database entrys act as valid users on the interface.

22.2. Configuring

- Enable DHCP Snooping Globally

Command	SWITCH(config)#**ip dhcp snooping** SWITCH(config)#**no ip dhcp snooping**
Description	Enables DHCP snooping globally.

- Enable DHCP Snooping on Vlans

Command	SWITCH(config)#**ip dhcp snooping vlan** VID SWITCH(config)#**no ip dhcp snooping vlan** VIID
Description	Enables DHCP snooping on a VLAN or VLAN range, For example: Ip dhcp snooping vlan 3-10. By default, DHCP Snooping is enabled on all VLANs.

- Configuring Trust Resources

Command	SWITCH (config-if)#**ip dhcp snooping trust** SWITCH (config-if)#**no ip dhcp snooping trust**
Description	Configures the interface as trusted. By default, All interfaces are untrusted.

- Enabling Mac Address Verification

Command	SWITCH (config)#**ip dhcp snooping verify mac-address** SWITCH (config)#**no ip dhcp snooping verify mac-address**
Description	Enables DHCP snooping MAC address verification. By default is disabled.

- Configuring Rate Limit on Interface

Command	SWITCH (config-if)#**ip dhcp snooping rate-limit** PPS SWITCH (config-if)#**no ip dhcp snooping rate-limit**
Description	Configures DHCP packet rate limiting. PPS range from 0 to 128. If PPS is set to 0, this interface will drop all Incoming DHCP packets.

Note

✦ Due to hardware limitations, for DHCP rate limit, when the limit value is not 0, the software rate limit is used, and when the limit value is 0, the hardware rate limit is used. Software rate limit will consume CPU resources.

- Enabling Option-82 Data Insertion

Command	SWITCH (config)#**ip dhcp snooping information option-82 (| extend-format)** SWITCH (config)#**no ip dhcp snooping information option-82**
Description	Enables DHCP option-82 data insertion. This option is disabled by default Extend format: remote-id, circuit-id compatible with Cisco format

- Configuring Option-82 Circuit-id

Command	SWITCH (config-if)#**ip dhcp snooping information option-82 circuit-id** WORD SWITCH (config-if)#**no ip dhcp snooping information option-82 circuit-id**
Description	Configure circuit-id customization content. The default information is vlan+port WORD: String information, valid length 3-63 characters.

For Option-82 Default Format：

Default Circuit-id Suboption

Suboption type (1 byte)	Length (1 byte)	Data (4 bytes)
1	4	vlan(2 bytes) | module(1 bytes) | port(1 bytes)

For User-configured Circuit-id Suboption

Suboption type (1 byte)	Length (1 byte)	Data (3-63 bytes)
1	N	N bytes

For Option-82 Extend-format:

Default Circuit-id Suboption

Suboption type (1 byte)	Length (1 byte)	Remote ID Type (1 byte)	Length (1 byte)	Data (4 bytes)
1	6	0	4	vlan(2 bytes) | module(1 bytes) | port(1 bytes)

For User-configured Circuit-id Suboption

Suboption type (1 byte)	Length (1 byte)	Remote ID Type (1 byte)	Length (1 byte)	Data (3-63 bytes)
1	N + 2	1	N	N bytes

- Configuring Option-82 Remote-id

Command	SWITCH (config-if)#**ip dhcp snooping information option-82 remote-id** WORD SWITCH (config-if)#**no ip dhcp snooping information option-82 remote-id**
Description	Configure remote-id custom content. The default information is the MAC address of the device WORD: String information, valid length 1-63 characters.

For Option-82 Default Format:

Default Remote-id Suboption

Suboption type (1 byte)	Length (1 byte)	Data (6 bytes)
2	6	MAC address

For User-configured Remote-id Suboption

Suboption type (1 byte)	Length (1 byte)	Data (1-63 bytes)
2	N	N bytes

For Option-82 Extend-format:

Default Remote-id Suboption

Suboption type (1 byte)	Length (1 byte)	Remote ID Type (1 byte)	Length (1 byte)	Data (6 bytes)
2	8	0	6	MAC address

For User-configured Remote-id Suboption

Suboption type (1 byte)	Length (1 byte)	Remote ID Type (1 byte)	Length (1 byte)	Data (1-63 bytes)
2	N+ 2	1	N	N bytes

- Configuring DHCP Snooping Database Write-delay Time

Command	SWITCH (config)#**ip dhcp snooping database write-delay** SECONDS SWITCH (config-if)#**no ip dhcp snooping database write-delay**
Description	Configuring DHCP Snooping data to be written to flash at regular intervals SECONDS range from 600 to 86400 by unit second.

- Trigger DHCP Snooping Database Write-flash

Command	SWITCH (config)#**ip dhcp snooping database write-flash**
Description	Trigger DHCP Snooping database write-flash.

- Trigger DHCP Snooping Database renew from flash

Command	SWITCH(config)#**ip dhcp snooping database renew**
Description	Trigger DHCP Snooping database renew from flash.

- Clear DHCP Snooping Database

Command	SWITCH#**clear ip dhcp snooping database (vlan** VLANID **| interface** IFNAME **| mac-address** XXXX.XXXX.XXXX **| ip-address** A.B.C.D **| flash)**
Description	Clear DHCP Snooping database based on port, vlan, MAC address, or IP address. Support to clear database in flash.

22.3. Examples

Example 1： This is an example of DHCP Snooping typical application. The interface of gigabitEthernet0/8 is connected to DHCP server; USER-A obtains IP address by dynamic; There are other DHCP servers in the LAN, which will affect the IP address assignment of USER-A. Diagram as show in the Figure 1-1 below.

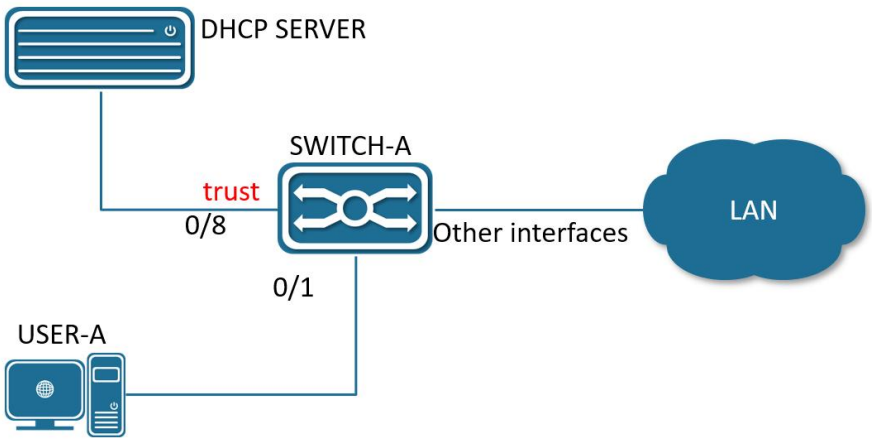


Figure 1-1 Typical application of DHCP Snooping Diagram

- Enable DHCP Snooping Globally.

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

- Configuring gigabitEthernet0/8 as Trusted Resource.

```
SWITCH(config)#interface gigabitEthernet0/8
SWITCH(config-if)#ip dhcp snooping trust
```

22.4. Display Information

- Display DHCP Snooping Information

```
SWITCH#show ip dhcp snooping
Ip dhcp snooping                    : Enabled
No ip dhcp snooping vlan            : 2-5
Verify mac-address                  : Disabled
Information option-82               : No
database write-delay                : 0 seconds

Interface               Trusted         Rate limit (pps)
------------------------------------------------------------
gigabitEthernet0/16     yes             unlimited
```

23. Configuring 802.1X Authentication

23.1. Overview of 802.1X Authentication

The IEEE802 LAN/WAN committee proposed the 802.1X protocol 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 Ethernet.

The 802.1X protocol is a port based network access control protocol. "Port-based network access control" means that, at the port level of the LAN access device, the access to the network resources is controlled through authentication for the connected user equipment.

23.1.1. 802.1X Architecture

The 802.1X system is a typical Client/Server structure, as shown in Figure 1, including three entities: Client, Device and Authentication server.

Figure 1 802.1X Authentication System Architecture

- A client is an entity on a local area network that is authenticated by the device on 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 side is another entity on the local area network that authenticates connected clients. The device side is usually a network device that supports the 802.1X protocol. It provides the client with a port 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 for user authentication, authorization and accounting, 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 packets use the EAPOL encapsulation format and are 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 packet is relayed by the device, and is carried in the RADIUS protocol using

the EAPOR (EAP over RADIUS) encapsulation format; the other is that the EAP protocol packet is terminated by the device. Packets with the PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) attribute interact with the RADIUS server for authentication.

23.1.3. 802.1X Basic Concepts

23.1.3.1. 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 controlled and uncontrolled ports.

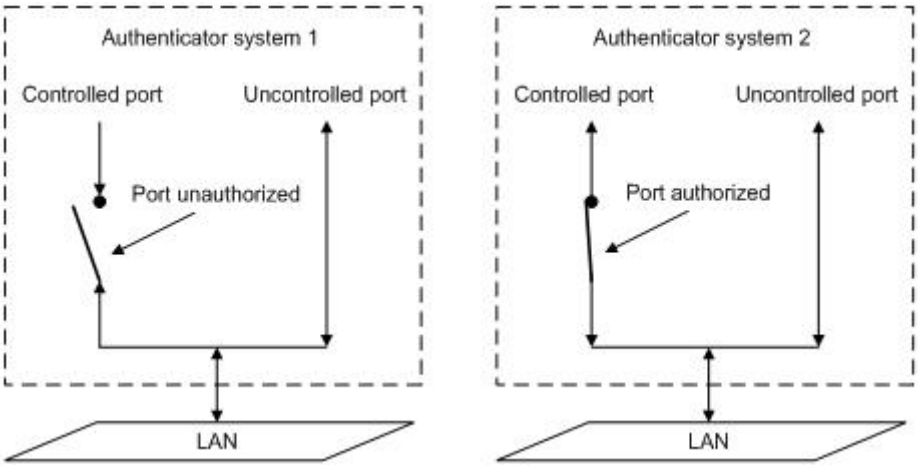
- The uncontrolled port is always in a two-way connection state and is mainly used to transmit EAPOL protocol frames to ensure that the client can always send or receive authentication packets.
- The controlled port is in a bidirectional connection state in the authorized state and is used to transmit service packets; in the unauthorized state, it is forbidden to receive any packets from the client.

23.1.3.2. Authorized/Unauthorized Status

The device uses the authentication server to authenticate the client that needs to access the LAN, and controls the authorization/unauthorized status of the controlled port according to the authentication result (Accept or Reject).

Figure 2 Shows the effect of different authorization states on the controlled port on packets passing through this 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 opening the port switch), and the controlled port of system 2 is in an authorized state (equivalent to closing the port switch).

Figure 2 Effects 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:

- Forced authorization mode (**authorized-force**): indicates that the port is always in an authorized state, allowing users to access network resources without authorization.
- Force unauthorized mode **unauthorized-force**): Indicates that the port is always in an unauthorized state and does not allow users to authenticate. The device does not provide authentication services for clients accessing through this port.
- Auto-identification mode (**auto**): indicates that the initial state of the port is an unauthorized state, only EAPOL packets are allowed to send and receive, and users are not allowed to access network resources; If the authentication is passed, the port switches to the authorized state, allowing the user to access network resources. This is also the most common case.

23.1.3.3. Controlled Direction

In the unauthorized state, the controlled port can be set as one-way controlled and two-way controlled.

- When two-way control is implemented, the transmission and reception of frames are prohibited;
- When unidirectional control is implemented, receiving frames from the client is prohibited, but sending frames to the client is allowed.

23.1.4. Authentication process for 802.1X

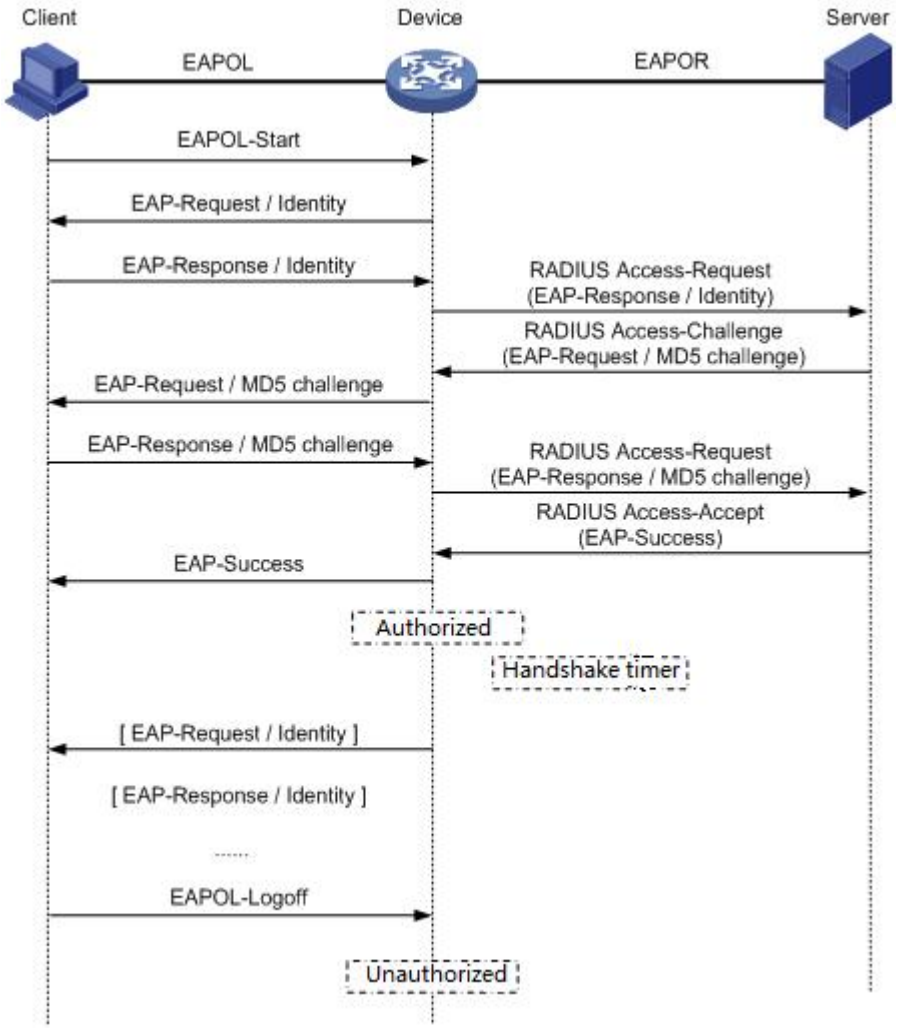
The 802.1X system supports EAP relay mode and EAP termination mode to interact with the remote RADIUS server to complete authentication. The following descriptions of the two authentication methods take the client's initiative to initiate authentication as an example.

23.1.4.1. EAP Relay Mode

This method is specified by the IEEE 802.1X standard, and EAP (Extensible Authentication Protocol) is carried in other high-level protocols, such as EAP over RADIUS, so that the extensible authentication protocol packets can reach the authentication server through complex networks. Generally speaking, the EAP relay mode requires the RADIUS server to support EAP attributes: EAP-Message and Message-Authenticator, which are used to encapsulate EAP packets and protect RADIUS packets carrying EAP-Message respectively.

The following takes EAP-MD5 as an example to introduce the basic business process, as shown in Figure3

Figure3 IEEE 802.1X EAP relay business process of authentication system



The authentication process is as follows:

1) When the user needs to access the network, open the 802.1X client program, enter the username and password that have been applied and registered, and initiate a connection request (EAPOL-Start message).At this point, the client program will send a message requesting authentication to the device to start an authentication process.
2) After receiving the data frame requesting authentication, the device will send a request frame (EAP-Request/Identity message) to request the user's client program to send the entered username.
3) The client program responds to the request from the device and sends the username information to the device through a data frame (EAP-Response/Identity message). The device sends the data frame sent by the client through packet processing (RADIUS Access-Request message) to the authentication server for processing.
4) After receiving the username information forwarded by the device, the RADIUS server compares the information with the username table in the database, finds the password information corresponding to the username, and encrypts it with a randomly generated encrypted word, and

also send this encrypted word to the device through the RADIUS Access-Challenge message, and the device forwards it to the client program.

5) After receiving the encrypted word (EAP-Request/MD5 Challenge message) from the device, the client program uses the encrypted word to encrypt the password part (this encryption algorithm is usually irreversible), generate an EAP-Response/MD5 Challenge packet, and send it to the authentication server through the device.

6) The RADIUS server compares the received encrypted password information (RADIUS Access-Request message) with the local encrypted password information. If they are the same, the user is considered to be a legitimate user, and the authentication is passed. messages (RADIUS Access-Accept packets and EAP-Success packets).

7) After receiving the authentication message, the device changes the port to the authorized state, allowing users to access the network through the port. During this period, the device will monitor the user's online status by periodically sending handshake messages to the client. By default, if the two handshake request packets are not answered by the client, the device will log the user offline, preventing the user from going offline due to abnormal reasons and the device cannot sense it.

8) The client can also send an EAPOL-Logoff message to the device to actively request to log off. The device changes the port status from authorized to unauthorized, and sends an EAP-Failure packet to the client.

23.2. Configuring

- Enabling/disabling 802.1X Authentication Globally

Command	SWITCH(config)# **dot1x enable** SWITCH(config)#**no dot1x enable**
Description	Enable and disable the 802.1X function globally.

- Enabling/disabling 802.1X authentication on the Interface

Command	SWITCH(config-if)# **dot1x port-control auto** SWITCH(config-if)#**no dot1x port-control auto**
Description	The port enables or disables the 802.1X function.

- Configuring RADIUS Server

Command	SWITCH(config)# **radius-server host** A.B.C.D **auth-port** <0-65535> **acct-port** <0-65535> **key** WORD SWITCH(config)#**no radius-server host** A.B.C.D
Description	Configure authentication server information. The default authentication port is 1812 and the accounting port is 1813. Please ensure that the RADIUS server and the device management address communicate with each other.

- Configuring EAPOL Protocol Version Number

Command	SWITCH(config-if)# **dot1x protocol-version** <1-2> SWITCH(config-if)#**no dot1x protocol-version**
Description	Configure the version number of the EAPOL protocol on the specified port. Optional configuration, default is 2.

- Configuring Authentication Silent Time

Command	SWITCH(config-if)# **dot1x quiet-period** <1-65535> SWITCH(config-if)#**no dot1x quiet-period**
Description	Configure the hold time of the HELD state. Optional configuration, the unit is seconds, the default is 60.

- Configuring the Re-authentication Function

Command	SWITCH(config-if)# **dot1x reauthentication** SWITCH(config-if)#**no dot1x reauthentication**
Description	The re-authentication function is enabled on the configuration port. Optional configuration, disabled by default.

- Configuring the Maximum Number of Re-authentications

Command	SWITCH(config-if)# **dot1x reauthMax** <1-10> SWITCH(config-if)#**no dot1x reauthMax**
Description	Configure the maximum number of times for port re-authentication. If the number of re-authentication requests exceeds the limit and there is no response, the port becomes unauthorized. Optional configuration, default 2 times.

- Configuring to Enable key Transfer Capability

Command	SWITCH(config-if)# **dot1x keytxenabled { disable | enable}**
Description	Configure the port key transfer function. Optional, disabled by default.

- Configuring Timer Timeout

Command	SWITCH(config-if)# **dot1x timeout {re-authperiod** <1-4294967295> **| server-timeout** <1-65535> **| supp-timeout** <1-65535> **| tx-period** <1-65535>**}** SWITCH(config-if)#**no dot1x timeout {re-authperiod | server-timeout | supp-timeout | tx-period}**
Description	Configure the port timer time. Optional configuration, the default re-authentication period is 3600 seconds, the server timeout is 30 seconds, the client authentication timeout is 30 seconds, and the client request timeout is 30 seconds.

- Enabling/disabling MAC Authentication Globally

Command	SWITCH(config)# **mac-auth enable**

	SWITCH(config)#**no mac-auth enable**
Description	Enable or disable the MAC authentication function globally.

- Enabling/disabling MAC Authentication on the Interface

Command	SWITCH(config-if)# **mac-auth {enable | disable}**
Description	The port enables or disables the MAC authentication function.

- Enabling/disabling MAC Authentication Dynamic VLAN Delivery on the Interface

Command	SWITCH(config-if)# **mac-auth dynamic-vlan-creation {enable | disable}**
Description	The port enables or disables dynamic VLAN delivery of MAC authentication. The current version is not supported.

- Configuring MAC Authentication Failure Handling

Command	SWITCH(config-if)# **mac-auth auth-fail-action {drop-traffic | restrict-vlan** <2-4094>**}**
Description	Configure the behavior of MAC authentication failure. Optional configuration, default is drop-traffic: drop traffic. The current version is not supported.

- Configuring RADIUS Server Death Time

Command	SWITCH(config)# **radius-server deadtime** <0-1440> SWITCH(config)# **no radius-server deadtime**
Description	Configure the RADIUS server death time.During the authentication process, the dead server will be automatically skipped, and the non-dead server will be selected for authentication. Optional configuration, the default is 0 minutes.

- Configuring RADIUS Server Default Key

Command	SWITCH(config)# **radius-server key** STRING SWITCH(config)# **no radius-server key**
Description	Configure the RADIUS server default key. Optional configuration.

- Configuring RADIUS Server Retransmission Times

Command	SWITCH(config)# **radius-server retransmit** <1-100> SWITCH(config)# **no radius-server retransmit**
Description	Configure the RADIUS server retransmission times. Optional configuration, the default is 3 times.

- Configuring RADIUS Server Timeout

Command	SWITCH(config)# **radius-server timeout** <1- 60> SWITCH(config)# **no radius-server timeout**

Description	Configure the RADIUS server timeout period. Optional configuration, the default is 5 seconds.

23.3. Examples

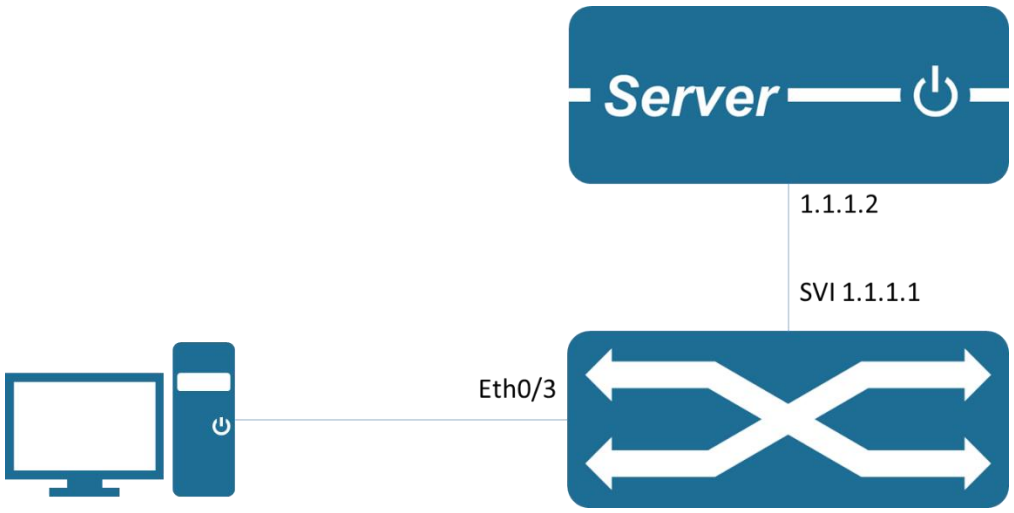
23.3.1. 802.1X Port Authentication Scenario

7) Requirement

- Requires authentication of access users on port GigabitEthernet0/3 to control their access to the Internet.
- RADIUS server group IP address 1.1.1.2.
- Set the shared key to be used when the system exchanges packets with the RADIUS server as name.

8) Network Diagram

Figure 4 802.1X Typical network diagram for 802.1x authentication



9) Typical configuration example

Device side:

```
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:

Configure NAS authentication device 1.1.1.1 and communication key name.

Add user account test password test.

The corresponding authentication method needs to be supported, such as EAP-MSCHAPv2

Client:

Enable 802.1X authentication client and log in with account test.

The corresponding authentication method needs to be supported, such as the EAP-MSCHAPv2 method.

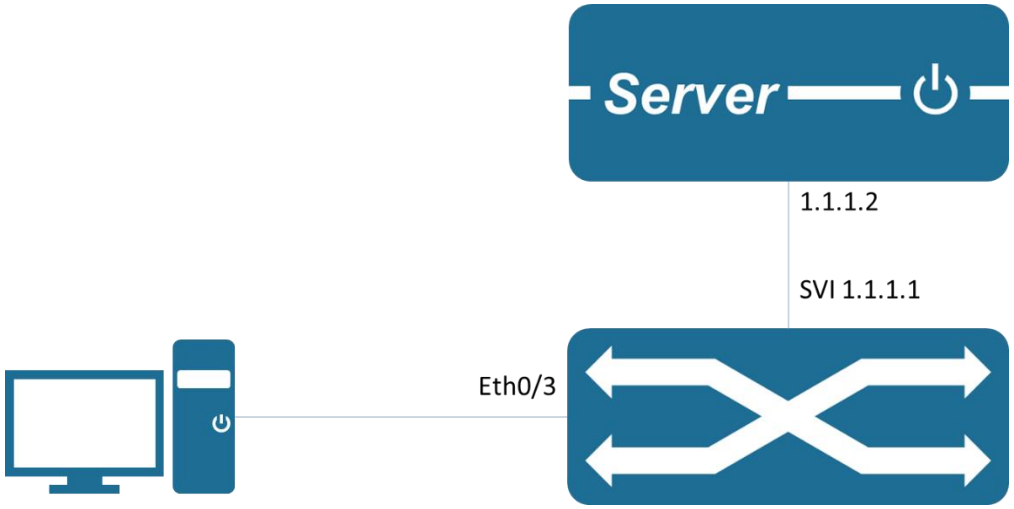
23.3.2. MAC Authentication Scenario

1) Requirement

- Requires authentication of access users on port GigabitEthernet0/3 to control their access to the Internet.
- RADIUS server group IP address 1.1.1.2.
- Set the shared key when the system and the RADIUS server exchange messages as name.

2) Network Diagram

Figure 5 Typical network diagram for MAC authentication



3) Typical configuration example

Device side:

```
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:

Configure NAS authentication device 1.1.1.1 and communication key name.

Add the client MAC address as the user account and password to the user database.

Client:

Enable the 802.1X authentication client and log in with any account.

23.4. Display Information

- Show 802.1X Port Authentication Information

```
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
```

- Display MAC Authentication Information

```
        SWITCH#show bridge
         Bridge CVLAN SVLAN BVLAN Port MAC Address FWD Time-out
         ---------+------+------+------+-----------+-- ---------------+-----+------
---+
```

24. Configuring Port Security

24.1. Overview of Port Security

You can use port security to block input to a Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses that are specified for that port. Alternatively, you can use port security to filter traffic that is destined to or received from a specific host that is based on the host MAC address.

The maximum number of MAC addresses that you can allocate for each port depends on your network configuration. After you allocate the maximum number of MAC addresses on a port, you can either specify the secure MAC address for the port manually or have the port dynamically configure the MAC address of the connected devices.

When a secure port receives a packet, the source MAC address of the packet is compared to the list of secure source addresses that were manually configured or autoconfigured (learned) on the port. If a MAC address of a device that is attached to the port differs from the list of secure addresses, A violation occurs. Users can set a port to the following two modes to handle a security violation:

Restrict: Drops all packets from insecure hosts, but remains enabled, until the MAC of the host aged out dynamic. You can manually shutdown and no-shutdown the interface to recover from violation.

Shutdown: The shutdown mode option allows you to specify whether the port is to be permanently disabled or disabled for only a specified time. The default is for the port to shut down permanently. You can manually shutdown and no-shutdown the interface to recover from violation.

If you want to convert dynamic security users to static security users, you can enable the sticky function on the port. If the sticky function is enabled, the dynamic users learned on the port will exist as static users. If the configuration is saved, it will still exist after the device restarts.

Note

- ✧ Only support L2 port for port security, such as physical port and L2 AP port.
- ✧ Only supports configuring port security function in access mode.
- ✧ Do not support AP member port configuration port security function.
- ✧ The destination port of the SPAN does not support the port security function.
- ✧ Does not support the port security function on ports that have been configured with static MAC addresses.

24.2. Configuring

- Enable Port Security

Command	SWITCH(config-if)#**switchport port-security** SWITCH(config-if)#**no switchport port-security**
Description	Enable Port Security on the interface.

- Setting the Max Number of Security Mac-address

Command	SWITCH(config-if)#**switchport port-security maximum** VALUE SWITCH(config-if)#**no switchport port-security maximum**

Description	The default maximum number of secure addresses is 1 VALUE range from 1 to 1024.

- Entering a Security Mac-address

Command	SWITCH(config-if)#**switchport port-security mac-address** MAC_ADDR SWITCH(config-if)#**no switchport port-security mac-address** MAC_ADDR
Description	Enters a secure MAC address for the interface. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses will be dynamically learned.

- Enable sticky

Command	SWITCH(config-if)# **switchport port-security mac-address sticky** SWITCH(config-if)#**no switchport port-security mac-address sticky**
Description	Enable sticky learning on the interface.

- Configuring Port Security Aging

Command	SWITCH(config-if)#**switchport port-security aging time** MINUTES SWITCH(config-if)#**no switchport port-security aging time**
Description	Sets the aging time for the secure port. Valid range for aging_time is from 0 to 1440 minutes. If the time is equal to 0, aging is disabled for this port.

- Enable Port Security Aging Static Mac-address

Command	SWITCH(config-if)# **switchport port-security aging static** SWITCH(config-if)#**no switchport port-security aging static**
Description	enables aging for statically configured secure addresses on this port.

- Setting the Violation Mode

Command	SWITCH(config-if)# **switchport port-security violation** { **strict** | **shutdown** } SWITCH(config-if)#**no switchport port-security violation**
Description	Sets the violation mode, the action to be taken when a security violation is detected, as one of these: Restrict: A port security violation restricts data and causes the SecurityViolation counter to increment and send an SNMP trap notification. Shutdown: The interface is error-disabled when a security violation occurs. You can manually reenable the by entering the shutdown and no shut down commands. When a secure port is in the error-disabled state, it will recover after errdisable recovery time.

24.3. Examples

Example 1： This is an example of Port Security typical application. Port Security is enabled on the interface gigabitEthernet0/1, the MAX secure Mac-address of the interface gigabitEthernet0/1 is 3, and we enter 3 secure Mac-address on the interface.

When the interface gigabitEthernet0/1 receives a packet, If the SRC MAC-address of the packet differs from the list of secure Mac-addresses, the packet will be dropped.

```
SWITCH(config-if)#switchport port-security
SWITCH(config-if)#switchport port-security maximum 3
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0001
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0002
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0003
```

24.4. Display Information

- Display Interfaces Port Security Brief

```
SWITCH#show port-security brief
interface   mac-address     mac-address     violation    violation
                  maxinum          count          count     action
-----------------------------------------------------------------------------------------------
GiE0/1      10              3               0          shutdown
GiE0/2      1               0               0          restrict
GiE0/3      1               0               0          restrict
GiE0/4      1               0               0          restrict
GiE0/5      1               0               0          restrict
GiE0/6      1               0               0          restrict
GiE0/7      1               0               0          restrict
GiE0/8      1               0               0          restrict
```

- Display an Interface Port Security Information

```
SWITCH#show port-security interface gigabitEthernet0/1
Port Security               : Enabled
Maimum MAC Addresses     : 10
Violation Mode              : Shutdown
Aging Time(mins)           : 10
Aging static                : Enabled
Total MAC Addresses        : 3
Configured MAC Addresses   : 2
Security Violation Count      : 0
Last Violate Address         : --
```

- Display Secure Mac-address

```
SWITCH#show port-security Mac-address
interface   vlan    mac-address         type        left-time(min)
-----------------------------------------------------------------------------
GiE0/1      1       0001.0002.0004      static      10
GiE0/1      1       0001.0002.0003      static      10
GiE0/1      1       000e.c6c1.3a03      dynamic     10
```

- Display an Interface Secure Mac-address

```
SWITCH#show port-security mac-address interface gigabitEthernet0/1
interface   vlan    mac-address         type        left-time(min)
-----------------------------------------------------------------------------
GiE0/1      1       0001.0002.0004      static      10
GiE0/1      1       0001.0002.0003      static      10
GiE0/1      1       000e.c6c1.3a03      dynamic     10
```

25. Configuring Ip Source Guard

25.1. Overview of Ip Source Guard

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings: Entries in the Dynamic Host Configuration Protocol (DHCP) snooping binding table; Static IP source entries that you configure.

Filtering on trusted IP and MAC address bindings helps prevent spoofing attacks, in which an attacker uses the IP address of a valid host to gain unauthorized network access.

Note

- ✧ Only support L2 port for port security, such as physical port and L2 AP port.
- ✧ Do not support AP member port configuration port security function.

25.2. Configuring

- Enabling Ip Source Guard

Command	SWITCH(config-if)#**ip verify source** SWITCH(config-if)#**no ip verify source**
Description	Enables IP Source Guard on the interface.

- Configuring Static Ip Source Binding Entry

Command	SWITCH(config)# **ip source binding** XXXX.XXXX.XXXX **vlan** VALUE A.B.C.D **interface** IFNAME SWITCH(config)#**no ip source binding** XXXX.XXXX.XXXX **vlan** VALUE A.B.C.D **interface** IFNAME
Description	Creates a static IP source binding entry for the current interface. Example: SWITCH(config)# ip source binding 0001.0001.0001 vlan 1 1.1.1.10 interface gigabitEthernet0/1 A single port can be configured with a maximum of 128 entries.

25.3. Examples

Example 1: This is an example of Ip Source Guard typical application. Ip Source Guard is enabled on the interface gigabitEthernet0/1, and we enter 3 static binding entrys on the interface.

When the interface gigabitEthernet0/1 receives a packet, If the IP address and the MAC address of the packet differs from the list of static entrys, the packet will be dropped.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#ip verify source
SWITCH(config)#ip source binding 0001.0001.0001 vlan 1 1.1.1.10 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0002 vlan 1 1.1.1.11 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0003 vlan 1 1.1.1.12 interface gigabitEthernet0/1
```

25.4. Display Information

- Display Ip Verify Source Binding Rules

```
SWITCH#show ip verify source
```

```
interface  Filter-type  Filter     IP-address      Mac-address  vlan
------------------------------------------------------------------------
GiE0/1     Ip        Permit    1.1.1.1         0001.0001.0001 1
GiE0/1     Ip        Deny      All             All            All
GiE0/2     Ip        Deny      All             All            All
```

- Display Ip Verify Source Binding Entrys on the Interface

```
SWITCH#show ip verify source interface gigabitEthernet0/1
interface  Filter-type  Filter     IP-address      Mac-address  vlan
-----------------------------------------------------------------------------------------------
GiE0/1     Ip        Permit    1.1.1.1         0001.0001.0001 1
GiE0/1     Ip        Deny      All             All            All
```

- Display Ip Source Binding Entrys

```
SWITCH#show ip source binding
interface  vlan  IP-address      Mac-address    Lease    Type
-----------------------------------------------------------------------------------------------
GiE0/1     1     1.1.1.1         0001.0001.0001 infinite    static
GiE0/2     1     1.1.2.1         0001.0002.0001 infinite    static
```

- Display Ip Source Binding Entrys on the Interface

```
SWITCH#show ip source binding interface gigabitEthernet0/1
interface  vlan  IP-address      Mac-address    Lease    Type
-----------------------------------------------------------------------------------------------
GiE0/1     1     1.1.1.1         0001.0001.0001 infinite    static
```

26. Configuring Arp-check

26.1. Overview of Arp-check

Arp-check is a per-interface traffic filter that permits ARP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings: Entries in the Dynamic Host Configuration Protocol (DHCP) snooping binding table; Static IP source entries that you configure.

Filtering on trusted IP and MAC address bindings helps prevent spoofing attacks, in which an attacker uses the IP address of a valid host to gain unauthorized network access.

Note

- ✧ Only support L2 port for port security, such as physical port and L2 AP port.
- ✧ Do not support AP member port configuration port security function.

26.2. Configuring

- Enabling Arp-check on the Interface

Command	SWITCH(config-if)#**arp-check** SWITCH(config-if)#**no arp-check**
Description	Enables Arp-check on the interface.

26.3. Examples

Example 1: This is an example of Arp-check typical application. Arp-check is enabled on the interface gigabitEthernet0/1, and we enter 3 static binding entrys on the interface.

When the interface gigabitEthernet0/1 receives a ARP packet, If the IP address and the MAC address of the packet differs from the list of static entrys, the packet will be dropped.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#ip verify source
SWITCH(config-if)#arp-check
SWITCH(config)#ip source binding 0001.0001.0001 vlan 1 1.1.1.10 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0002 vlan 1 1.1.1.11 interface gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0003 vlan 1 1.1.1.12 interface gigabitEthernet0/1
```

27. Configuring Dos Protection

27.1. Overview of Dos Protection

The purpose of a DoS (Denial of Service) attack is to prevent a computer or network from providing normal services. There are many types of DoS attacks, and they are implemented in various ways. What they have in common is that the victim host or network cannot receive and process external requests in a timely manner. Here are some typical DoS attack types.

SYN Flood attack

SYN Flood attack is the most common DDOS attack on the current network and the most classic DoS attack. By sending a large number of attack packets with forged source addresses to the port where the network service is located, the connection queue of the target server is filled, thereby preventing other legitimate users from accessing.

ICMP Flood attack

ICMP Flood is a DDOS attack that sends a large number of ping packets to the destination host in a short period of time, consuming host resources. After the host resources are exhausted, other services cannot be provided.

ARP Flood attack

ARP Flood is a DDOS attack that sends a large number of ARP request packets to the destination host in a short period of time, consuming host resources. After the host resources are exhausted, it cannot respond to other ARP requests.

NULL SCAN attack

The NULL SCAN attack mainly involves the attacker sending TCP packets without setting any flags to the target host IP. Some operating systems actively feedback RST packets, allowing the attacker to obtain the port of the unclosed session. The essence of preventing NULL SCAN attacks is to discard TCP packets without any TCP flag bits, which can effectively prevent attackers from obtaining the shutdown status of each port through NULL SCAN and launching subsequent attacks.

TCP message with SYN and FIN set at the same time

Under normal circumstances, the SYN flag (connection request flag) and FIN flag (connection teardown flag) cannot appear in a TCP message at the same time, and the RFC does not specify how the IP protocol stack handles such malformed messages. An attacker can use this feature to determine the type of operating system by sending messages with SYN and FIN set at the same time.

TCP message with FIN set but no ACK set

Under normal circumstances, except for the first message (SYN message), all messages have the ACK flag set, including TCP connection teardown messages (messages with the FIN flag set). However, some attackers may send TCP messages to the target host with the FIN flag set but the ACK flag not set, which may cause the target host to crash.

TCP packet with SYN set and source port number 0-1023

Port numbers 0-1023 are well-known port numbers assigned by IANA, and on most systems can only be used by system (or root) processes or programs executed by privileged users. These ports (0-1023) cannot be used as the source port number of the first TCP message sent by the client (with the SYN flag set). When the anti-illegal TCP packet attack function is enabled , the device will check the non-TCP packets based on their characteristics and discard them if they are illegal.

27.2. Configuring

27.2.1. Configure SYN Flood Anti-attack

- Global Configuration

Command	SWITCH(config)# **dos syn-flood rate-limit** <0-10000> SWITCH(config)#no **dos syn-flood rate-limit**
Description	Configure global SYN Flood anti-attack <0-10000>, speed limit range, deny all attack packets at 0, unit kbps

- Interface Configuration

Command	SWITCH(config-if)# **dos syn-flood rate-limit** <0-10000> SWITCH(config-if)#no **dos syn-flood rate-limit**
Description	Configure interfaces to resist SYN Flood attacks <0-10000>, speed limit range, deny all attack packets at 0, unit kbps

- Counter Enable

Command	SWITCH(config)# **dos syn-flood counter enable** SWITCH(config)# **no dos syn-flood counter enable**
Description	Configure and enable SYN Flood anti-attack counters Off by default When the counter is enabled, hit attack packets will be counted. Run the show dos syn -flood counter command to view statistical information.

27.2.2. Configure ARP Flood Anti-attack

- Global Configuration

Command	SWITCH(config)# **dos arp-flood rate-limit** <0-10000> SWITCH(config)# **no dos arp-flood rate-limit**
Description	Configure global ARP Flood anti-attack <0-10000>, speed limit range, deny all attack packets at 0, unit kbps

- Interface Configuration

Command	SWITCH(config-if)# **dos arp-flood rate-limit** <0-10000> SWITCH(config-if)# **no dos arp-flood rate-limit**
Description	Configure interfaces to resist ARP Flood attacks <0-10000>, speed limit range, deny all attack packets at 0, unit kbps

- Counter Enable

Command	SWITCH(config)# **dos arp-flood counter enable** SWITCH(config)# **no dos arp-flood counter enable**
Description	Configure ARP Flood anti-attack counter enablement Off by default When the counter is enabled, hit attack packets will be counted. Run the show dos arp -flood counter command to view the statistical information.

27.2.3. Configure ICMP Flood Anti-attack

- Global Configuration

Command	SWITCH(config)# **dos icmp-flood rate-limit** <0-10000> SWITCH(config)# **no dos icmp-flood rate-limit**

Description	Configure global ICMP Flood anti-attack <0-10000>, speed limit range, deny all attack packets at 0, unit kbps

- Interface Configuration

Command	SWITCH(config-if)# **dos icmp-flood rate-limit** <0-10000> SWITCH(config-if)# **no dos icmp-flood rate-limit**
Description	Configure interfaces to resist ICMP flood attacks <0-10000>, speed limit range, deny all attack packets at 0, unit kbps

- Counter Enable

Command	SWITCH(config)# **dos icmp-flood counter enable** SWITCH(config)# **no dos icmp-flood counter enable**
Description	Configure ICMP Flood anti-attack counter enablement Off by default When the counter is enabled, hit attack packets will be counted. Use the show dos icmp-flood counter command to view statistical information.

27.2.4. Configure NULL SCAN Anti-attack

- Configure NULL SCAN Anti-attack

Command	SWITCH(config)# **dos null-scan deny** SWITCH(config)# **no dos null-scan deny**
Description	Configure global resistance to NULL SCAN attacks After enabling, discard TCP packets without any flags set.

27.2.5. Configure SYN FIN Anti-attack

- Configure SYN FIN Anti-attack

Command	SWITCH(config)#dos **syn-fin deny** SWITCH(config)# **no dos syn-fin deny**
Description	Configure global SYN FIN anti-attack After enabling, discard TCP packets with both SYN and FIN set at the same time.

27.2.6. Configure SYN SPORTL1024 Anti-attack

- Configure SYN SPORTL1024 Anti-attack

Command	SWITCH(config)#dos **syn-sportl1024 deny** SWITCH(config)# **no dos syn-sportl1024 deny**
Description	Configure global SYN SPORTL1024 anti-attack After enabling, discard source port (0-1023) TCP synchronization packets.

27.2.7. Configure FIN NO-ACK Anti-attack

- Configure FIN NO-ACK Anti-attack

Command	SWITCH(config)# **dos fin-noack deny** SWITCH(config)# **no dos fin-noack deny**
Description	Configure global FIN NO-ACK Anti-attack After enabling, discard TCP packets with FIN set but no ACK set.

27.3. Examples

27.3.1. SYN Flood Anti-attack Example

Port gi0/1 is connected to the FTP server, and ports gi0/2 and gi0/3 are connected to the terminal device respectively. The terminal connected to port gi0/2 launches a syn flood attack, causing the terminal connected to port gi0/3 to be unable to access the FTP server normally.

```
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#dos syn-flood rate-limit 10
```

Enable syn flood attack prevention on port gi0/2, limit the speed to 10kbps, and restore normal access to the FTP server from the terminal on port gi0/3.

27.3.2. ICMP Flood Anti-attack Example

Port gi0/1 is connected to the FTP server, and ports gi0/2 and gi0/3 are connected to the terminal device respectively. The terminal connected to port gi0/2 initiates a large number of ICMP request messages, causing the FTP server to be unable to respond to other ICMP messages. The terminal connected to port gi0/3 cannot access the FTP server normally.

```
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)# dos icmp-flood rate-limit 10
```

27.3.3. ARP Flood Anti-attack Example

Port gi0/1 is connected to the FTP server, and ports gi0/2 and gi0/3 are connected to the terminal device respectively. The terminal connected to port gi0/2 forges a large number of IP and MAC addresses to launch ARP Flood attacks, causing the FTP server to be unable to process ARP messages for normal requests .

```
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)# dos arp-flood rate-limit 10
```

27.4. Display Information

- Show Dos Configuration

```
SWITCH#show dos
Interface:Global
Dos syn-flood state: Enable rate-limit :10
 Dos icmp-flood          state: Enable       rate-limit :10
 Dos arp-flood           state: Enable       rate-limit :10
 Dos null-scan deny      state: Disable
 Dos syn-fin deny        state: Disable
 Dos syn-sportl1024 deny  state: Disable
 Dos fin-noack deny      state: Disable
Interface:GiE0/2
 Dos syn-flood           state: Enable       rate-limit :10
 Dos icmp-flood          state: Enable       rate-limit :10
Dos arp -flood state: Enable rate-limit :10
```

- Show Dos ARP Flood Counter

```
SWITCH#show dos arp-flood counter

 arp -flood counter status: Enable

Interface Rate-limit( kbps) Drops(Byte) Permit(Byte)
---------- ---------- ---------- ----------
Global 10 374660 25492
GiE0/2 10 245820 11680
```

- Show Dos SYN Flood Counter

```
SWITCH#show dos syn-flood counter

 syn-flood counter status: Enable

Interface   Rate-limit(kbps)    Drops(Byte)     Permit(Byte)
------------------------------------------------------------------------
Global      10                  348840          27404
GiE0/2      10                  348976          11832
```

- Show Dos ICMP Flood Counter

```
SWITCH#show dos icmp-flood counter

 icmp-flood counter status: Enable

Interface   Rate-limit(kbps)    Drops(Byte)     Permit(Byte)
------------------------------------------------------------------------
Global      10                  1193302         58576
GiE0/2      10                  274516          16050
```

28. Configuring SNMP Network Management

28.1. Overview of SNMP Network Management

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

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

Currently the following versions of SNMP 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:

- Make sure that data is not tampered with during transmission.
- Make sure the data is sent from a legitimate data source.
- Encrypt messages to ensure data confidentiality.

28.2. Configuring

- Configuring Communication Community Words

Command	SWITCH(config)# **snmp-server community** COMMUNITY **{ ro | }** SWITCH(config)# **no snmp -server community** COMMUNITY
Description	Configure/delete SNMP communication community word. **ro** : read-only identifier, configure the community word as a community word with only read permission; the default configuration is a community word with both read and write permissions. Supports configuring multiple community characters at the same time.

- Configuring SNMPv3 Views

Command	SWITCH(config)# **snmp -server view** NAME **{include | exclude}** OID SWITCH(config)# **no snmp -server view** name
Description	Configure/delete SNMPv3 views; Supports configuring multiple views at the same time, and supports configuring multiple rules for a single view; The system has all and none views by default and cannot be modified

- Configuring SNMP Groups

Command	SWITCH(config)# **snmp -server group** NAME **{v3 | } { noAuthNoPriv | authNoPriv | authPriv } read** RVIEW **write** WVIEW SWITCH(config)# **snmp -server group** NAME **{v1 | v2c} read** RVIEW **write** WVIEW SWITCH(config)# **no snmp -server group** name
Description	configure/delete SNMP groups; Support to configure multiple groups at the same time;

	create group information in order to be compatible with the old configuration when configuring the community , usually without additional attention

- Configuring SNMPv3 Users

Command	SWITCH(config)# **snmp -server user** NAME **group** GROUPNAME **auth {md5 | sha}** {AUTHPASS} **priv { aes | des}** PRIVPASS SWITCH(config)# **no snmp -server user** name
Description	configure/delete SNMP users; Support to configure multiple users at the same time;

- Configuring SNMP Host Notification Server

Command	SWITCH(config)# **snmp -server host** IPADDR **{informs | traps} {v3 |}** **{ noAuthNoPriv | authNoPriv | authPriv } user** NAME SWITCH(config)# **snmp -server host** IPADDR **{informs | traps} {v1 | v2c} community** NAME SWITCH(config)# **no snmp -server hostname** _
Description	configure/delete SNMP server; Support to configure multiple servers at the same time;

28.3. Examples

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

- Enter the global configuration mode configuration:

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH( config)#snmp-server community public
SWITCH( config)#snmp-server 2.2.2.2 community public
SWITCH( config)#
```

Case requirements: The IP address of the SNMP network management server is 2.2.2.2, SNMPv3 is used, the user test password is 12345678, the encryption key is 87654321; the authentication algorithm MD5, the encryption algorithm DES

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH( config)# snmp -server group test v3 authPriv read all write all
SWITCH( config)# snmp -server user test group test auth MD5 12345678 priv
DES 87654321
SWITCH( config)# snmp -server host 2.2.2.2 informs v3 authPriv user test
```

29. Configuring RMON

29.1. Overview of RMON

SNMP is the most widely used network management protocol in the Internet. The collection and statistics of network communication information are realized through the agent software embedded in the device. The management software obtains the information by sending query signals to the MIB of the agent through polling, and realizes the management of the network through the obtained information. The management software sends queries to the proxy MIB by means of a query to obtain this information and manages the network through the information obtained. Although the MIB counter records the sum of the statistics, it does not allow historical analysis of the day-to-day communication situation. In order to provide a comprehensive view of the flow and traffic changes over the day, web hosting software requires continuous poll to analyze the status of the network through the information available.

Polling with SNMP has two distinct disadvantages:

- Occupies a lot of network resources. In a large-scale network, a large number of network communication packets will be generated by polling, which will cause network congestion and even cause network congestion. Therefore, SNMP is not suitable for managing large-scale networks. , not suitable for recycling large amounts of data, such as routing table information.
- The task of collecting data in SNMP polling is done by the network administrator through the network management software. If the network administrator monitors more than 3 network segments, it may occur that the network is overloaded due to the heavy burden. A situation in which a manager is unable to complete a task.

In order to improve the availability of management information, reduce the burden of management stations, 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 expanding distributed interconnection. The monitoring function of the data traffic of the network segment and even the entire network. The following are the features of RMON:

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

RMON is implemented based on the SNMP architecture and is compatible with the existing SNMP framework. It is still composed of the network management workstation NMS and the agent running on each network device. Since RMON does not use another set of mechanisms, which are shared between NMS and SNMP, network managers do not need additional learning and are therefore simpler to achieve.

- RMON enables SNMP to monitor remote network devices 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 obtain the value of the MIB variable through polling multiple times for comparison. The purpose of efficiently managing large interconnected networks.

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

- Through a dedicated RMON Probe (detector), the NMS directly obtains management information from the RMON Probe and controls network resources. In this way, all the information of the RMON MIB can be obtained.
- Embed RMON Agent directly into network devices, making them network devices with RMON Probe function. The NMS uses SNMP to exchange data information with it and collect network management information. This method is limited by device resources and generally cannot obtain all the data of the RMON MIB. Basically, only four groups (alarms, events, history, and statistics) are collected.

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

29.2. Rationale

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, and is used for remote monitoring and management of managed devices by management devices in the network.

The RMON statistics function can be implemented through the RMON statistics group or the RMON history group, which are divided into Ethernet statistics functions and historical statistics functions.

- Historical statistics function (corresponding to the historical group in the RMON MIB): The system periodically samples and collects network status statistics and stores them for subsequent processing. The system will periodically collect statistics on various traffic information, including bandwidth utilization, number of error packets and total number of packets.
- Ethernet statistics function (corresponding to the statistics group in the RMON MIB): The system collects basic statistics about 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 error frames of various types, the number of collisions, etc. The system will keep track of all traffic information on a regular basis, including bandwidth utilization, erroneous packages and total packages.

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

- 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, it can record logs or send Trap to the network management station.
- Set the 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 pre-defines 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 will be triggered; When the value of the variable is less than or equal to the lower limit threshold, a lower limit alarm event is triggered. RMON Agent will record the above monitored status as a log or send Trap to the network management station.

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

- Statistics group

The statistics group specifies that the system will continuously collect statistics on various traffic information of the Ethernet interface, and store the statistical results in the Ethernet statistics table (etherStatsTable) for the management device to view at any time. Statistics include the number of network collisions, the number of CRC check error packets, the number of data packets that are too small (or too large), the number of broadcast and multicast packets, the number of bytes received, and the number of received packets.

After the statistics entry is successfully created on the specified interface, the statistics group collects statistics on the number of packets on the current interface, and the statistics result is a continuous accumulated value.

- History group

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

The history group contains two tables:

  - historyControlTable: It is mainly used to set control information such as sampling interval time.
  - etherHistoryTable: It is mainly used to store the historical data collected by the historical group on a regular basis for network status statistics, and to provide network administrators with historical data on network segment traffic, error packets, broadcast packets, utilization, and collision times and other statistical information.

- Event group

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

  - 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

Alarm groups allow monitoring of a predefined set of thresholds for alarm variables (which can be arbitrary objects in 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 limit threshold, an upper limit alarm event will be 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 perform corresponding processing according to the definition of the event.

29.3. Configuring

- Configuring Statistics Group

Command	SWITCH(config)# **rmon statistics** <1-65535> **interface** IFNAME **{owner** OWNERNAME **|}** SWITCH(config-if)# **no rmon statistics** <1-65535>
Description	configure/delete statistics group. <1-65535>: Group index. IFNAME *:* interface name. OWNERNAME *:* owner information.

- Configuring History Group

Command	SWITCH(config)# **rmon history** <1-65535> **interface** IFNAME **buckets** <1-65535> **interval** <1-3600> **{owner** OWNERNAME **|}** SWITCH(config-if)# **no rmon history** <1-65535>
Description	configure/delete history group. <1-65535>: Group index. IFNAME *:* interface name. <1-65535>: History bucket size. <1-3600>: Recording period; the unit is seconds. OWNERNAME *:* owner information.

- Configuring Event Groups

Command	SWITCH(config)# **rmon event** <1-65535> **{description** DESCRIPTION **|} {log | trap** COMMUNITY **| log-trap** COMMUNITY **| none} {owner** OWNERNAME **|}** SWITCH(config-if)# **no rmon event** <1-65535>

Description	configure/delete event groups. <1-65535>: Group index. DESCRIPTION: Event description. COMMUNITY: Trap communication group word. OWNERNAME: owner information.

- Configuring an Alarm Group

Command	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 **|}** SWITCH(config-if)# **no rmon alarm** <1-65535>
Description	Configure/delete alarm groups. <1-65535>: Group index. STRING: OID of alarm monitoring; for example, 1.3.6.1.2.1.2.2.1.10.1 indicates the number of bytes received by monitoring interface 1. <1-65535>: Monitoring period; the unit is seconds. <1-2147483645>: Rising Threshold. <1-65535>: Rising event index; corresponds to the index in the event group. <1-2147483645>: Falling Threshold. <1-65535>: Fall event index; corresponds to the index in the event group. OWNERNAME: owner information.

- Configuring the Upper Limit of Log Entries

Command	SWITCH(config)# **rmon max-log** <1-65535> SWITCH(config-if)# **no rmon max-log**
Description	Configure/reset the upper limit of log entries. <1-65535>: Number of 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 logs generated exceeds the limit of entries, the old logs will be deleted according to the generation time to maintain the upper limit.

29.4. Examples

Requirements

The IP address of the SNMP network management server is 2.2.2.2, and the community word for read and write communication is public.

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

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

Configuration steps

Initialize the network management configuration

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH(config)#snmp-server community public
SWITCH(config)#snmp-server 2.2.2.2 community public
SWITCH(config)#
```

Configure the rmon statistics group (the following rmon configurations can be configured on the NMS through the MIB)

SWITCH(config)# rmon statistics 1 interface gigabitEthernet0/1 owner abc

Configure rmon events and alarm groups (the following rmon configurations can be configured on the NMS through MIB)

```
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
```

29.5. Display Information

- Show Event Group LSog

```
SWITCH#show rmon log
event 1 log 226 time 2304 desc
event 1 log 227 time 2314 desc
event 1 log 228 time 2324 desc
event 1 log 229 time 2334 desc
event 1 log 230 time 2344 desc
event 1 log 231 time 2354 desc
event 1 log 232 time 2364 desc
event 1 log 233 time 2374 desc
……
```

30. Configure sFlow

30.1. Overview

sFlow is a network monitoring technology jointly developed by InMon , HP and Foundry Networks in 2001. It has been standardized and can provide complete second to fourth layer information and can adapt to traffic analysis in extremely large network traffic environments. Allows users to analyze the performance , trends and existing problems of network transmission streams in detail and in real time.

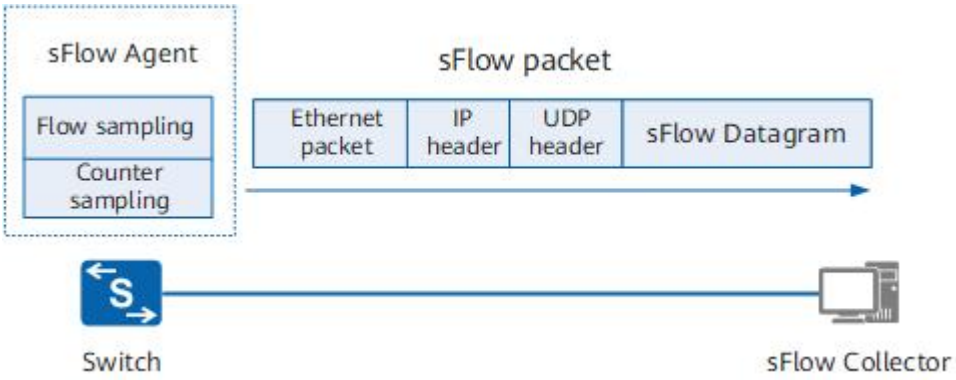
sFlow has the following advantages:

- Enables precise monitoring of network traffic on gigabit or higher-speed networks.
- sFlow Collector can monitor thousands or hundreds of sFlow Agents, has good scalability.
- sFlow agent is embedded in the network device and the cost is low.

30.2. Principle

30.2.1. sFlow system composition

As shown in the figure, the sFlow system includes an sFlow Agent embedded in the device and a remote sFlow Collector. Among them, sFlow Agent obtains interface statistics and data information through sFlow sampling, and encapsulates the information into sFlow messages. When the sFlow message buffer is full or the sFlow message cache time times out (the cache time is 1 second), sFlow Agent The sFlow message will be sent to the specified sFlow Collector. sFlow Collector analyzes sFlow messages and displays the analysis results.



30.2.2. sFlow sampling

sFlow Agent provides two sampling methods for users to analyze network traffic conditions from different perspectives, namely Flow sampling and Counter sampling.

Flow sampling

Flow sampling means that the sFlow Agent device performs sampling and analysis on packets on a specified interface according to a specific sampling direction and sampling comparison to obtain information related to the packet data content. This sampling method mainly focuses on the details of traffic, so that the traffic behavior on the network can be monitored and analyzed.

Field	Description
Raw packet	Intercept all or part of the header of the original message (the specific length of the interception is determined by the configuration), encapsulate this part of the original message into an sFlow message and send it to the Collector.

Field	Description
Ethernet Frame Data	For Ethernet messages, parse the Ethernet header information of the message, encapsulate the parsed data into sFlow messages and send them to the Collector.
Extended Switch Data	For forwarded Ethernet packets, record the VLAN conversion and VLAN priority conversion of the packets, encapsulate the forwarding information into sFlow packets and send them to the Collector. When the VLAN ID is 0, it indicates an invalid VLAN.

Counter sampling

Counter sampling allows the sFlow Agent device to periodically obtain traffic statistics information on the interface. Counter sampling supports the acquisition of sampling information as shown in the following table. Compared with Flow sampling, Counter sampling only focuses on the quantity of traffic on the interface, but not on the detailed information of the traffic.

Field	Description
Generic Interface Counters	General interface statistics, including basic interface information and general interface traffic statistics.
Ethernet Interface Counters	For the Ethernet interface, it is used to collect Ethernet-related traffic statistics.
Processor Information	Used to count device CPU usage and memory usage.

30.2.3. sFlow message

sFlow messages are encapsulated by UDP, and the default destination port number is the well-known port 6343. There are four header formats for sFlow messages, namely Flow sample, Expanded Flow sample, Counter sample, and Expanded Counter sample. The Expanded Flow sample and Expanded Counter sample are new additions to sFlow version 5 and are extensions of the Flow sample and Counter sample, but are not forward compatible. All Extended sampling content must be encapsulated using the Expanded sampling packet header.

30.3. Configuration commands

- Configure agent address

Order	SWITCH(config)# **sflow agent { ip** IPV4ADDR **| ipv6** IPV6ADDR **}** SWITCH(config)# **no sflow agent { ip | ipv6}**
describe	Configure/delete a gent address; IPV4ADDR: agent/ device IPv4 address IPV6ADDR: a gent/device IPv6 address Supports configuring ipv 4 and ipv 6 addresses at the same time, for collectors of ipv 4 and ipv 6 respectively There is no configuration by default. If not configured, the protocol may not send packets.

- Configure collector

Order	SWITCH(config)# **sflow collector** <1-2> **{ ip** IPV4ADDR **| ipv6** IPV6ADDR **}** **[datagram-size** <200-9000> **| port** <1024-65535> **| description** STRING **]** SWITCH(config)# **no sflow collector** <1-2>
describe	Configure/delete collector; <1-2>: collector index IPV4ADDR: collector/ server IPv4 address IPV6ADDR: collector/ server IPv6 address

	<200-9000>: Maximum length of data packet, optional, default 1 400 <1024-65535>: Server port number, optional, default 6 343 STRING: c collector description information, optional, default is none

- Configure interface flow sampling

Order	SWITCH(config -if) #sflow **flow -sampling collector** <1-2> SWITCH(config -if)# **no flow-sampling collector**
describe	Configure/delete interface flow sampling; <1-2>: c collector index ss

- Configure interface counter sampling

Order	SWITCH(config -if)# **sflow counter-sampling collector** <1-2> SWITCH(config -if)# **no counter-sampling collector**
describe	Configure/delete interface counter sampling; <1-2>: collector index ss

- Configure interface flow sampling parameters

Order	SWITCH(config-if)# **sflow flow-sampling direction { inbound | outbound }** SWITCH(config-if)# **sflow flow-sampling rate** <1024-65536> SWITCH(config-if)# **sflow flow-sampling max-header** <18-256> SWITCH(config-if)# **no flow-sampling direction** SWITCH(config -if)# **no flow-sampling rate** SWITCH(config -if)# **no flow-sampling max-header**
describe	Configure/ reset interface flow sampling parameters; { inbound | outbound } : flow sampling direction, optional, the default is to sample inbound + outbound at the same time <1024-65536>: flow sampling rate, optional, default is 2 048, one sample for every 2 048 flows <18-256> : Flow sampling message length, unit byte, optional, default 6 4

- Configure interface counter sampling parameters

Order	SWITCH(config -if)# **sflow counter-sampling interval** <3-65535> SWITCH(config -if)# **no sflow counter-sampling interval**
describe	Configure/reset interface counter sampling parameters; <3-65535>: counter sampling period, unit seconds, optional, default 1 0

30.4. Examples

Requirements

sFlow network management server is 2.2.2.2 and the device IP address is 2.2.2.95.

The network management server needs to monitor the status of device port 3 through sFlow . It is required to perform flow sampling and counter sampling at the same time. The parameters can be defaulted.

Configurations

Initialize network management configuration

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH(config )# sflow -agent- ip 2.2.2.95
SWITCH(config )# sflow collector 1 ip 2.2.2.2
SWITCH(config )#
```

Configure sampling for port 3

```
SWITCH( config)#int gi 0/3
```

```
SWITCH( config-if)#sflow flow-sampling collector 1
SWITCH( config-if)#sflow counter-sampling collector 1
```

30.5. Display Information

- Show sFlow

```
SWITCH#show sflow
Collector 1:
Address: 2.2.2.2 Agent: 2.2.2.95
Port: 6343 Datagram-Size: 1400 Description:
        Fd : 11 Seq: 45 Tx Timer: (nil)
        Buf : 0xab0d8 Alloc : 1400 Used: 0
------------------------------------------------- ----------------------------------
| Flow | Counter |
Interface | ID Rate Direction Max-header Sequence | ID Interval Sequence |
------------------------------------------------- ----------------------------------
GiE0/3 1 2048 both 64 2 1 10 7462
SWITCH#
```

31. Configuring DHCP Server

31.1. Overview of DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a local area network network protocol that works using the 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 from the DHCP server by sending a request message, and other configuration information. When the DHCP client and server are not on the same subnet, there must be a DHCP relay agent (DHCP Relay) to forward DHCP request and reply messages.

Protocol Standard:

RFC2132 DHCP Options and BOOTP Vendor Extensions. S. Alexander, R. Droms. March 1997. (Format: TXT, HTML) (Obsoletes RFC1533) (Updated by RFC3442, RFC3942, RFC4361, RFC4833, RFC5494) (Status: DRAFT STANDARD) (DOI: 10.17487/RFC2132)

31.2. Configuring

31.2.1. Global Configuration Commands

- Enabling/disabling DHCP Server Globally

Command	SWITCH(config)# **ip dhcp-server enable** SWITCH(config)#**no ip dhcp-server enable**
Description	Enable and disable the DHCP server globally.

- Configuring Global Parameters

Command	SWITCH(config)# **ip dhcp-server parameter** NAME VALUE SWITCH(config)# **ip dhcp-server parameter (authoritative (on|off) | server-name** NAME **| server-identifier** IDENTIFY **| default-lease-time** <1-2147483648> **| max-lease-time** <1-2147483648> **| ping-timeout-ms** <1-65535> **| ping-timeout** <1-65535>**)** SWITCH(config)# **no ip dhcp-server parameter** NAME SWITCH(config)# **no ip dhcp-server parameter (authoritative | server-name | server-identifier | default-lease-time | max-lease-time | ping-timeout-ms | ping-timeout)**
Description	Global parameter configuration. When parameter values conflict, global parameters take precedence over parameters for subnets and address pools with more precise ranges. Default lease time: 43200s/12h. Optional.

- Configuring Global Options

Command	SWITCH(config)# **ip dhcp-server option** NAME VALUE SWITCH(config)# **ip dhcp-server option (routers** A.B.C.D **| domain-name** NAME **| domain-name-servers** A.B.C.D **| capwap-ac-v4** A.B.C.D**)** SWITCH(config)# **no ip dhcp-server option** NAME SWITCH(config)# **no ip dhcp-server option (routers | domain-name | domain-name-servers | capwap-ac-v4)**
Description	Global option configuration. When option values conflict, global options take precedence over options for subnets and address pools with more precise ranges. Optional.

- Configuring Custom Domain Fields

Command	SWITCH(config)# **ip dhcp-server custom-space** NAME **[code width** <1-4>**] [length**

	width <1-4>**] [hash size** <1-65535>**]** SWITCH(config)#**no ip dhcp-server custom-space** NAME
Description	Configure custom domain information fields. Optional.

- Configuring Custom Options

Command	SWITCH(config)# **ip dhcp-server custom-option** NAME **code** <1-255> **(boolean|integer|ip-address|text|string|encapsulate)** SWITCH(config)#**no ip dhcp-server custom-option** NAME
Description	Configure custom options fields. The configured custom option code value cannot conflict with the configured common options. Optional.

- Configuring Force Send Options

Command	SWITCH(config)# **ip dhcp-server force-option** <1-255> SWITCH(config)#**no ip dhcp-server force-option** <1-255>
Description	Configure mandatory options fields. Optional.

- Configuring Static Address

Command	SWITCH(config)# **ip dhcp-server static-lease** NAME XX:XX:XX:XX:XX:XX A.B.C.D SWITCH(config)#**no ip dhcp-server static-lease** NAME
Description	Configure static address binding. Optional.

- Configuring Whitelist

Command	SWITCH(config)# **ip dhcp-server whitelist** NAME XX:XX:XX:XX:XX:XX SWITCH(config)#**no ip dhcp-server whitelist** NAME
Description	Configure the whitelist. Optional.

- Configuring Blacklist

Command	SWITCH(config)# **ip dhcp-server blacklist** NAME XX:XX:XX:XX:XX:XX SWITCH(config)#**no ip dhcp-server blacklist** NAME
Description	Configure the blacklist. Optional.

- Configuring Custom Classification

Command	SWITCH(config)# **ip dhcp-server class** NAME **match** EXP SWITCH(config)#**no ip dhcp-server class** NAME
Description	Configure custom classification. For professional usage, please configure it under the guidance of technicians. Example: ip dhcp-server class win_pc match " substring (option vendor-class-identifier,0,4)=MSFT " Optional.

31.2.2. Subnet Configuration Command

- Configuring Subnet Information

Command	SWITCH(config)# **ip dhcp-server subnet** A.B.C.D/M SWITCH(config)#**no ip dhcp-server subnet** A.B.C.D/M

Description	Configure subnet information and enter subnet configuration mode. At least one correct subnet configuration is required for the server to start normally.

- Configuring Subnet Address Range

Command	SWITCH(config-dhcp-subnet)# **range** A.B.C.D A.B.C.D SWITCH(config-dhcp-subnet)#**no range** A.B.C.D
Description	Configure the address range of the subnet. The server needs at least one assignable address range to start normally, which can be configured in the address pool below. Can be configured multiple times, with different ranges.

- Configuring Subnet Parameters

Command	SWITCH(config-dhcp-subnet)# **parameter** NAME VALUE SWITCH(config-dhcp-subnet)# **parameter (authoritative (on|off) | server-name** NAME **| server-identifier** IDENTIFY **| default-lease-time** <1-2147483648> **| max-lease-time** <1-2147483648> **| ping-timeout-ms** <1-65535> **| ping-timeout** <1-65535>**)** SWITCH(config-dhcp-subnet)#**no parameter** NAME SWITCH(config-dhcp-subnet)#**no parameter (authoritative | server-name | server-identifier | default-lease-time | max-lease-time | ping-timeout-ms | ping-timeout)**
Description	Configuration parameter information. Optional.

- Configuring Subnet Options

Command	SWITCH(config-dhcp-subnet)# **option** NAME VALUE SWITCH(config-dhcp-subnet)# **option (routers** A.B.C.D **| domain-name** NAME **| domain-name-servers** A.B.C.D **| capwap-ac-v4** A.B.C.D**)** SWITCH(config-dhcp-subnet)#**no option** NAME SWITCH(config-dhcp-subnet)#**no option (routers | domain-name | domain-name-servers | capwap-ac-v4)**
Description	Configuration option information. It is usually necessary to configure the gateway routing address and DNS server address of the subnet. Optional.

31.2.3. Address Pool Configuration Command

- Configuring Address Pool Information

Command	SWITCH(config-dhcp-subnet)# **pool** NAME SWITCH(config-dhcp-subnet)#**no pool** NAME
Description	Configure the address pool in subnet mode. Subnets can be further divided through the address pool and used on demand. Optional.

- Configuring the Address Range of the Address Pool

Command	SWITCH(config-dhcp-pool)# **range** A.B.C.D A.B.C.D SWITCH(config-dhcp-pool)#**no range** A.B.C.D
Description	Configure the address range of the address pool. The server needs at least one assignable address range to start normally, which can be configured in the above subnet. Can be configured multiple times, with different ranges.

- Configuring Address Pool Parameters

Command	SWITCH(config-dhcp-pool)# **parameter** NAME VALUE SWITCH(config-dhcp-pool)# **parameter (authoritative (on|off) | server-name** NAME **| server-identifier** IDENTIFY **| default-lease-time** <1-2147483648> **| max-lease-time** <1-

	2147483648> **| ping-timeout-ms** <1-65535> **| ping-timeout** <1-65535>**)** SWITCH(config-dhcp-pool)#**no parameter** NAME SWITCH(config-dhcp-pool)#**no parameter (authoritative | server-name | server-identifier | default-lease-time | max-lease-time | ping-timeout-ms | ping-timeout)**
Description	Configuration parameter information. Optional.

- Configure Address Pool Options

Command	SWITCH(config-dhcp-pool)# **option** NAME VALUE SWITCH(config-dhcp-pool)# **option (routers** A.B.C.D **| domain-name** NAME **| domain-name-servers** A.B.C.D **| capwap-ac-v4** A.B.C.D**)** SWITCH(config-dhcp-pool)#**no option** NAME SWITCH(config-dhcp-pool)#**no option (routers | domain-name | domain-name-servers | capwap-ac-v4)**
Description	Configuration option information. It is usually necessary to configure the gateway routing address and DNS server address of the address pool. Optional.

- Configuring Condition Filter Command

Command	SWITCH(config-dhcp-pool)# **(allow|deny|ignore)** CLASSNAME SWITCH(config-dhcp-pool)# **(allow|deny|ignore) (known-clients|unknown-clients|bootp|duplicates|declines)** SWITCH(config-dhcp-pool)# **no (allow|deny|ignore) (**CLASSNAME**|known-clients|unknown-clients|bootp|duplicates|declines)**
Description	Configure the address pool filter conditions. Custom CLASSNAME refer to the Configuring Custom Classifications section in the global configuration. Optional.

31.3. Examples

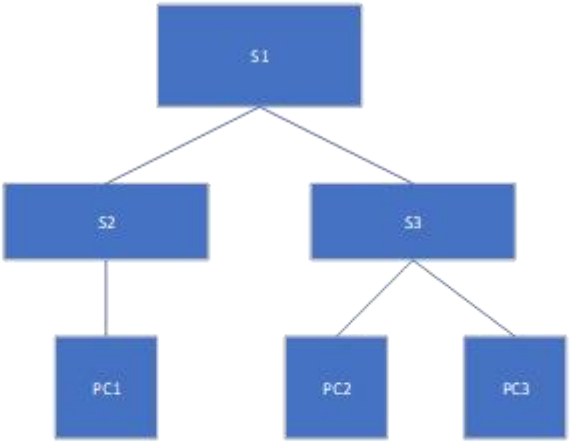
31.3.1. General DHCP Server Address Assignment Scenario

10) Requirement

See the description of the network diagram.

11) Network Diagram

Figure1- 1 DHCP server typical network diagram



S1: Layer 3 switch
VLAN 100: 192.168.100.1/24 Directly connected to S2
VLAN 200: 192.168.200.1/24 directly connected to S3
S2, S3 : Layer 2 switches
PC1, PC2, and PC 3 are automatically assigned IP
Expect:
PC1 and PC2 can obtain the IPs of their respective network segments, and can ping each other.
PC3 can be assigned to the address of 192.168.200.2

Description: The MAC address of PC3 during the test is 00:0E:C6:C1:38:41

12) Typical Configuration Example

S1:

```
SWITCH(config)# ip dhcp-server subnet 192.168.100.0/24
SWITCH(config-dhcp-subnet)#range 192.168.100.2 192.168.100.254
SWITCH(config-dhcp-subnet)#option routers 192.168.100.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)# ip dhcp-server subnet 192.168.200.0/24
SWITCH(config-dhcp-subnet)#range 192.168.200.2 192.168.200.254
SWITCH(config-dhcp-subnet)#option routers 192.168.200.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)# ip dhcp-server static-lease pc3 00:0E:C6:C1:38:41 192.168.200.2
SWITCH(config)#ip dhcp-server option domain-name-servers 114.114.114.114
SWITCH(config)#ip dhcp-server enable
```

S2/S3: Empty configuration transparent transmission.

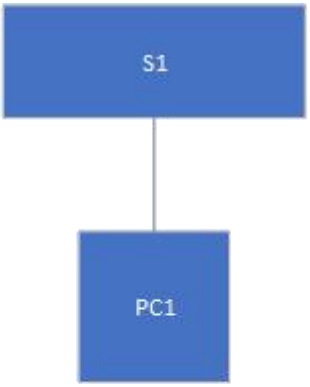
31.3.2. Supports DHCP Server Address Allocation Scenarios Delivered by Private Attributes

1) Requirement

See the description of the network diagram.

2) Network Diagram

Figure 1-2 DHCP server typical network diagram



S1: Layer 3 switch
VLAN 100: 192.168.100.1/24 Directly connected to PC1
PC1 automatically assigns IP
Expect:
PC1 can get the correct IP and private option information

3) Typical Configuration Example

S1:

```
SWITCH(config)# ip dhcp-server custom-space dkwl code width 1 length width 1
SWITCH(config)# ip dhcp-server custom-option dkwl.name code 1 string
SWITCH(config)# ip dhcp-server custom-option dkwl.ip code 2 ip-address
SWITCH(config)# ip dhcp-server custom-option vendor_dkwl code 43 encapsulate dkwl
SWITCH(config)# ip dhcp-server option dkwl.ip 1.1.1.1
SWITCH(config)# ip dhcp-server option dkwl.name "dockeer"
SWITCH(config)# ip dhcp-server subnet 192.168.100.0/24
SWITCH(config-dhcp-subnet)#range 192.168.100.2 192.168.100.254
SWITCH(config-dhcp-subnet)#option routers 192.168.100.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)#ip dhcp-server option domain-name-servers 114.114.114.114
SWITCH(config)#ip dhcp-server enable
```

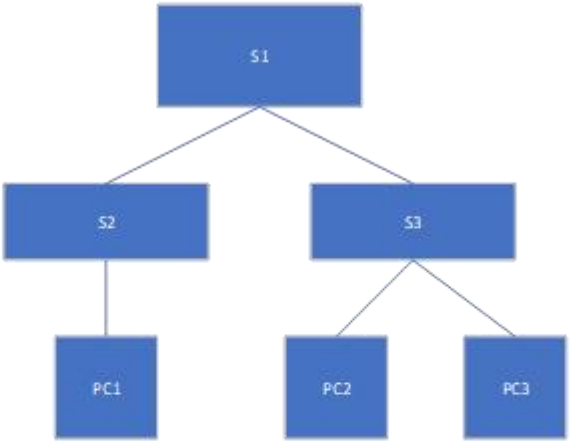
31.3.3. A DHCP Server Address Assignment Scenario that Supports Guest Separation

1) Requirement

- See the description of the network diagram.
- Normal user allocation addresses 192.168.100.2-192.168.100.100 and 192.168.200.2-192.168.200.100.
- Guest assigned address 192.168.100.200-192.168.100.254.

2) Network Diagram

Figure 1-3 DHCP server typical network diagram



S1: Layer 3 switch
VLAN 100: 192.168.100.1/24 Directly connected to S2
VLAN 200: 192.168.200.1/24 directly connected to S3
S2, S3 : Layer 2 switches
PC1, PC2, and PC 3 are automatically assigned IP
Expect:
PC1 and PC2 can obtain the normal user IP respectively
PC3 can be assigned to the guest segment address

3) Typical Configuration Example

S1:

```
SWITCH(config)# ip dhcp-server subnet 192.168.100.0/24
SWITCH(config-dhcp-subnet)#range 192.168.100.2 192.168.100.100
SWITCH(config-dhcp-subnet)#option routers 192.168.100.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)# ip dhcp-server subnet 192.168.200.0/24
SWITCH(config-dhcp-subnet)#pool employee
SWITCH(config-dhcp-pool)#range 192.168.200.2 192.168.200.100
SWITCH(config-dhcp-pool)#deny unknown-clients
SWITCH(config-dhcp-pool)#pool guest
SWITCH(config-dhcp-pool)#range 192.168.200.200 192.168.200.254
SWITCH(config-dhcp-pool)#allow unknown-clients
SWITCH(config-dhcp-pool)#exit
SWITCH(config-dhcp-subnet)#option routers 192.168.200.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)#ip dhcp-server option domain-name-servers 114.114.114.114
SWITCH(config)#ip dhcp-server enable
```

S2/S3: Empty configuration transparent transmission.

31.4. Display Information

- Display DHCP Server Status Information

```
SWITCH#show ip dhcp-server status
DHCP Server: Enable (conf.Enable)
```

- Display Address Assignment Information

```
SWITCH#show ip dhcp-server leases
Name MAC IP Begin End Manufacturer
------------------- ------------------- --- ----------------- -------------------
------------ ------- --------------------
liulang-work 00:0e:c6:c1:38:4a 3.3.3.254 1970-01-01 00:00:36 1970-01-01 00:10:36
ASIX ELECTRONICS CORP.
```

32. Configuring AAA

32.1. Overview of AAA

AAA is the abbreviation of Authentication Authorization and Accounting, which provides for authentication, authorization and accounting function into the configuration of the consistency framework. AAA provides the following services in a modular fashion:

- Authentication: Verify whether the user can obtain access rights. Optionally use RADIUS protocol, TACACS+ protocol or Local (local) and so on. Identity authentication is a method of identifying a user's identity before allowing access to the network and network services.
- Authorization: Which services are available to authorized users. AAA authorization is achieved by defining a series of attribute pairs, these attribute pairs describe the operations that the user is authorized to perform. These attribute pairs can be stored on a network device or remotely on a secure server.
- Accounting: record the user's use of network resources. When AAA accounting is enabled, the network device starts to send user usage of network resources. Each accounting record is composed of attribute pairs and stored on a secure server. These records can be read and analyzed by special software, so as to realize accounting, statistics and tracking of users' use of network resources.

Using AAA has the following advantages:

- Flexibility and controllability.
- Scalability.
- Standardized Certification.
- Multiple backup systems.

AAA has the following relevant standards:

RFC2865 Remote Authentication Dial In User Service (RADIUS). C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000. (Format: TXT, HTML).

RFC2866 RADIUS Accounting. C. Rigney. June 2000. (Format: TXT, HTML).

RFC8907 The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol. T. Dahm, A. Ota, DC Medway Gash, D. Carrel, L. Grant. September 2020.

32.2. Configuring

- Enabling/disabling AAA Function Globally

Command	SWITCH(config)# **aaa new-model** SWITCH(config)# **no aaa new-model**
Description	Globally enable or disable the AAA function.

- Configuring AAA Server Group

Command	SWITCH(config)# **aaa group server (radius) (default|** NAME **)** SWITCH(config) # **aaa group server (tacacs +) (default|** NAME **)** SWITCH(config)# **no aaa group server (radius|tacacs +) (default|** NAME **)**
Description	Server group configuration. Optional. By default there is no server group configuration and no server method is used.

- Configuring AAA Server

Command	SWITCH(config-gs-rad)# **server** A.B.C.D **(auth-port** <1-65535> **|) (acct-port** <1-65535> **|) (key** STRING **)** SWITCH(config-gs-tac)# **server** A.B.C.D **(port** <1-65535> **|) (key** STRING **)** SWITCH(config-gs-rad)# **no server** A.B.C.D SWITCH(config-gs-tac)# **no server** A.B.C.D
Description	**server group mode .** Configure RADIUS, TACACS + server information, including basic IP address, port information, shared key Optional. **Note: Due to implementation restrictions, the current radius accounting port number is always the authentication port number + 1, and the configuration is invalid.**

- Configuring Server Group Timeout

Command	SWITCH(config-gs-rad)# **timeout** <1-120> SWITCH(config-gs-tac)# **timeout** <1-120> SWITCH(config-gs-rad)# **no timeout** SWITCH(config-gs-tac)# **no timeout**
Description	**server group mode .** **Configure the timeout period for servers in the group.** Optional. Note: The actual effective range of the radius service timeout is 5-60 seconds; it is not recommended to be used in web authentication and authorization

- Configuring AAA Method Information

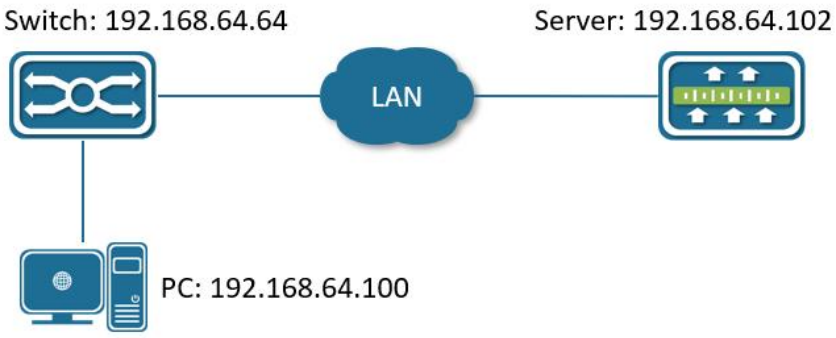
Command	SWITCH(config)# **aaa (authentication | authorization) (login | ssh | web) default {group (radius | tacacs+ |** NAME **) | local}** SWITCH(config)# **no aaa (authentication | authorization) (login | ssh | web) default**
Description	**Global configuration mode.** **Configure AAA method information .** **Login: serial port authentication or telnet authentication, authorization** **Ssh: ssh authentication and authorization** **Web: web authentication, authorization** **Optional configuration. Local authentication and authorization are used by default.** Note: It is not recommended to enable radius authorization separately, unless the same group is specified for authentication and authorization. Tacplus and local authorization will not verify the password again.

32.3. Examples

32.3.1. Use Tacacs+ Method for SSH Login Authentication and Authorization

1) Requirement : PC users log in to the switch and implement remote authentication and authorization through tacacs+ Server.

2) Network Diagram



Typical network diagram of SSH through tacacs+ server authentication and authorization

3) Typical Configuration

Server:

Server selects tacacs+ server, running on Ubuntu system

Server Configuration

```
#/etc/tacacs+/tac_plus.conf
key = testing123
user = admin {
    global = cleartext "admin"
    service = exec {
            priv-lvl=15
    }
}
```

Switch :

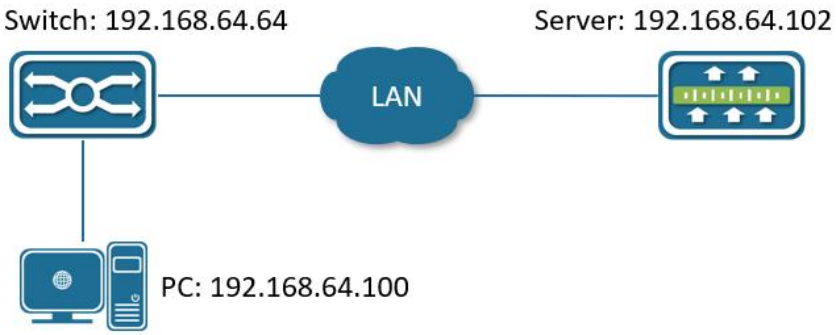
```
SWITCH(config)# aaa new-model
SWITCH(config)# aaa group server tacacs+ default
SWITCH(config-gs- tac )# server 192.168.64.102 key testing123
SWITCH(config-gs- tac )# exit
SWITCH(config)# aaa authentication ssh default group tacacs+
SWITCH(config)# aaa authorization ssh default group tacacs+
```

For device IP configuration and ssh configuration, refer to the corresponding sections of the configuration document, which are omitted here.

32.3.2. **Use the radius method for Telnet login authentication and authorization**

1) Requirement : PC users log in to the switch and implement remote authentication and authorization through the Radius Server.

2) Network Diagram



Typical network diagram of Telnet through radius server and local authentication and authorization

3) Typical Configuration Examples

Server:

S erver selects freeradius 3.0 as the server, running on the Ubuntu system

Server configuration:

```
#/etc/freeradius/3.0/clients.conf
client 192.168.64.64 {
    ipaddr = 192.168.64.64
    secret = testing123
}

#/etc/freeradius/3.0/users
admin   Cleartext-Password := "admin"
        Service-Type = 7,
        Management-Privilege-Level = 15
```

Switch :

```
SWITCH(config)# aaa new-model
SWITCH(config)# aaa group server radius default
SWITCH(config-gs- rad )# server 192.168.64.102 key testing123
SWITCH(config-gs- rad )# exit
SWITCH(config)# aaa authentication login default group radius local
SWITCH(config)# aaa authorization login default group radius local
```

Device IP configuration and telnet configuration, refer to the corresponding chapters in the configuration document, which are omitted here.

33. Configuring USB

33.1. Overview of USB

Universal Serial Bus (USB), jointly formulated by computer companies and communication companies such as Intel, Compaq, Digital, IBM, Microsoft, NEC and Northern Telecom in 1995, and gradually formed an industry standard.

As a high-speed serial bus, the high transmission speed of the USB bus can meet the application environment requirements of high-speed data transmission, and the bus also has the advantages of simple power supply, convenient installation and configuration, simple expansion ports, diversified transmission methods, and compatibility. Good (backward compatibility after product upgrade) and other advantages.

This device supports the following functions based on USB: configuration import, configuration export, product firmware upgrade, system log export. The USB device can only be used as a storage device, and the function can be completed through CLI commands. It can also be set through the configuration file in the USB device, and the configuration function is automatically completed after the USB device is inserted.

This document mainly introduces operations such as configuration import, configuration export, product firmware upgrade, and system log export through CLI commands.

33.2. Configuring

- Installing USB Device

Command	SWITCH#**usb install** UID
Description	Install the USB device. You can view the online usb device and obtain the UID information by the show usb command.

- Removing USB Device

Command	SWITCH#**usb remove** UID
Description	Uninstall the USB device. You can view the online usb device and obtain the UID information by the show usb command.

- Importing Configuration

Command	SWITCH#**copy usb** FILE **startup-config**
Description	Copy FILE from USB device to override startup-config file in the system.

- Exporting Configuration

Command	SWITCH# **copy startup-config usb** DIR
Description	Copy the startup-config file to the DIR directory of the USB device.

- Firmware Upgrade

Command	SWITCH# **upgrade usb** FILE

Description	System firmware upgrade, use FILE in USB device as firmware.

- Exporting Syslog

Command	SWITCH# **copy log syslog usb** DIR
Description	Copy the system log file to the DIR directory of the USB device.

33.3. Examples

33.3.1. Example of Import Configuration

This example shows how to import configuration from USB device. The configuration file startup.conf is saved in the USB device, and the USB device is inserted.

Configuring steps:

Step 1: Check the USB device is online.

```
SWITCH#show usb
Uid   Status   Installed   system   Total size(1K)   Used size(1K)   Dir
-------------------------------------------------------------------------------------------------------
0     online   no          --       --               --              --
```

Step2: Install the USB device and get the information of the USB device after loading, such as Dir path.

```
SWITCH#usb install 0
SWITCH#show usb
Uid   Status   Installed   system   Total size(1K)   Used size(1K)   Dir
-------------------------------------------------------------------------------------------------------
0     online   yes         vfat     15343616         105488          /usb0
```

Step 3: View the files in the USB device Dir path.

```
SWITCH#show usb 0
-rwxr-xr-x  1 root root    4 Jan  1 00:03 startup.conf
```

Step4: Import configuration.

```
SWITCH#copy usb /usb0/startup.conf startup-config
Copy Success
```

Step5: Restart the device to confirm that the configuration is imported successfully.

33.3.2. Example of Export Configuration

This example shows how to export configuration to the USB device. The USB device is inserted.

Configuring steps:

Step 1: Check the USB device is online.

```
SWITCH#show usb
Uid   Status   Installed   system   Total size(1K)   Used size(1K)   Dir
-------------------------------------------------------------------------------------------------------
0     online   no          --       --               --              --
```

Step2: Install the USB device and get the information of the USB device after loading, such as Dir path.

```
SWITCH#usb install 0
SWITCH#show usb
Uid   Status   Installed   system   Total size(1K)   Used size(1K)   Dir
-------------------------------------------------------------------------------------------------------
0     online   yes         vfat     15343616         105488          /usb0
```

Step 3: Export configuration.

```
SWITCH#copy startup-config usb /usb0
Copy Success
```

Step 4: View the files in the USB device Dir path to confirm that the operation was successful.

```
SWITCH#show usb 0
-rwxr-xr-x  1 root root    4 Jan  1 00:03 startup.conf
```

33.3.3. Example of Firmware Upgrade

This example shows how to upgrade firmware by USB device. The firmware file firmware.bin is saved in

the USB device, and the USB device is inserted.

Configuring steps:

Step 1: Check the USB device is online.

```
SWITCH#show usb
Uid   Status   Installed   system   Total size(1K)   Used size(1K)   Dir
-------------------------------------------------------------------------------------------------------
0     online   no          --       --               --              --
```

Step2: Install the USB device and get the information of the USB device after loading, such as Dir path.

```
SWITCH#usb install 0
SWITCH#show usb
Uid   Status   Installed   system   Total size(1K)   Used size(1K)   Dir
-------------------------------------------------------------------------------------------------------
0     online   yes         vfat     15343616         105488          /usb0
```

Step 3: View the files in the USB device Dir path.

```
SWITCH#show usb 0
-rwxr-xr-x  1 root root    62M Jan  1 00:03 firmware.bin
```

Step 4: Upgrade firmware.

```
SWITCH#  upgrade usb /usb0/firmware.bin
```

Step 5: After the execution is completed, the prompt "Reboot system to finish upgrade?" pops up, enter 'y' to restart the device to complete the upgrade operation.

33.3.4. Example of Export Syslog

This example shows how to export syslog to USB device. The USB device is inserted.

Configuring steps:

Step 1: Check the USB device is online.

```
SWITCH#show usb
Uid   Status   Installed   system   Total size(1K)   Used size(1K)   Dir
-------------------------------------------------------------------------------------------------------
0     online   no          --       --               --              --
```

Step2: Install the USB device and get the information of the USB device after loading, such as Dir path.

```
SWITCH#usb install 0
SWITCH#show usb
Uid   Status   Installed   system   Total size(1K)   Used size(1K)   Dir
-------------------------------------------------------------------------------------------------------
0     online   yes         vfat     15343616         105488          /usb0
```

Step 3: Export syslog to USB device.

```
SWITCH#copy log syslog usb /usb0
```

Step 4: View the files in the USB device Dir path to confirm that the operation was successful.

```
SWITCH#show usb 0
-rwxr-xr-x  1 root root    4 Jan  1 00:03 syslog
```

33.4. Display Information

- Show USB

```
SWITCH#show usb
Uid   Status   Installed   system   Total size(1K)   Used size(1K)   Dir
-------------------------------------------------------------------------------
0     online   yes         vfat     15343616         105488          /usb0
```

- Show USB File Information

```
SWITCH#show usb 0
       total 48K

       drwxr-xr-x  5 root root  16K Jan  1 00:03 .

       drwxr-xr-x 28 root root 2.0K Jan  1 00:00 ..
```

```
       drwxr-xr-x  4 root root 8.0K Jul 29  2024 EFI

       drwxr-xr-x  2 root root 8.0K Jul 29  2024 System Volume Information

       drwxr-xr-x  3 root root 8.0K Jul 29  2024 WEPE

        -rwxr-xr-x  1 root root    4 Jan  1 00:03 test
```

- Show USB File Information in a Certain Directory

```
SWITCH#show usb 0 EFI
       total 40K

       drwxr-xr-x 4 root root 8.0K Jul 29  2024 .

       drwxr-xr-x 5 root root  16K Jan  1 00:03 ..

       drwxr-xr-x 2 root root 8.0K Jul 29  2024 BOOT

       drwxr-xr-x 3 root root 8.0K Jul 29  2024 MICROSOFT
```

34. Fault Diagnosis

34.1. Ping/tracerout

- ping

Command	SWITCH#**ping** {ip IPADDR | ipv6 IPV6ADDR}
Description	Ping a remote host through IP.

- traceroute

Command	SWITCH# **traceroute** {**ip** IPADDR | **ipv6** IPV6ADDR }
Description	Trace the path that packets take through the network.

34.2. Port Optical Module

34.2.1. Configuring Port Optical Module

- Configuring Optical-transceiver Monitor Enable

Command	SWITCH(config-if)# **optical-transceiver monitor enable** SWITCH(config-if)# **no optical-transceiver monitor enable**
Description	Enable monitor the specified interface, detect the status of optical module periodically. Default is disabled.

- Configuring Optical-transceiver Monitor Interval

Command	SWITCH(config)# **optical-transceiver monitor interval** MINUTES SWITCH(config-if)# **no optical-transceiver monitor interval**
Description	Set the interval of the transceiver monitor. Default is 15 minutes. Range from 1 to 1440 minutes.

- Configuring Optical-transceiver Temperature Threshold

Command	SWITCH(config-if)# **optical-transceiver threshold temperature** HALARM HWARN LWARN LALARM SWITCH(config-if)# **no optical-transceiver threshold temperature**
Description	By default, the optical module has own temperature threshold setting, so it is not recommended to configure the temperature threshold. HALARM: high-alarm threshold value, range from -255 to 255 C HWARN: high-warning threshold value, range from -255 to 255 C LWARN: low-warning threshold value, range from -255 to 255 C LALARM: low-alarm threshold value, range from -255 to 255 C The HALARM value should not smaller than HWARN value. The LWARN value should not smaller than LALARM value.

- Configuring Optical-transceiver Voltage Threshold

Command	SWITCH(config-if)# **optical-transceiver threshold voltage** HALARM HWARN LWARN LALARM SWITCH(config-if)# **no optical-transceiver threshold voltage**
Description	By default, the optical module has own voltage threshold setting, so it is not recommended to configure the voltage threshold. HALARM: high-alarm threshold value, range from 0.00 to 5.00 V HWARN: high-warning threshold value, range from 0.00 to 5.00 V

	LWARN: low-warning threshold value, range from 0.00 to 5.00 V LALARM: low-alarm threshold value, range from 0.00 to 5.00 V The HALARM value should not smaller than HWARN value. The LWARN value should not smaller than LALARM value.

- Configuring Optical-transceiver Bias Threshold

Command	SWITCH(config-if)# **optical-transceiver threshold bias** HALARM HWARN LWARN LALARM SWITCH(config-if)# **no optical-transceiver threshold bias**
Description	By default, the optical module has own bias threshold setting, so it is not recommended to configure the bias threshold. HALARM: high-alarm threshold value, range from 0.00 to 500.00 mA HWARN: high-warning threshold value, range from 0.00 to 500.00 mA LWARN: low-warning threshold value, range from 0.00 to 500.00 mA LALARM: low-alarm threshold value, range from 0.00 to 500.00 mA The HALARM value should not smaller than HWARN value. The LWARN value should not smaller than LALARM value.

- Configuring Optical-transceiver Rx-power Threshold

Command	SWITCH(config-if)# **optical-transceiver threshold rx-power** HALARM HWARN LWARN LALARM SWITCH(config-if)# **no optical-transceiver threshold rx-power**
Description	By default, the optical module has own rx-power threshold setting, so it is not recommended to configure the rx-power threshold. HALARM: high-alarm threshold value, range from -40.00 to 10.00 dBm HWARN: high-warning threshold value, range from -40.00 to 10.00 dBm LWARN: low-warning threshold value, range from -40.00 to 10.00 dBm LALARM: low-alarm threshold value, range from -40.00 to 10.00 dBm The HALARM value should not smaller than HWARN value. The LWARN value should not smaller than LALARM value.

- Configuring Optical-transceiver Tx-power Threshold

Command	SWITCH(config-if)# **optical-transceiver threshold tx-power** HALARM HWARN LWARN LALARM SWITCH(config-if)# **no optical-transceiver threshold tx-power**
Description	By default, the optical module has own tx-power threshold setting, so it is not recommended to configure the tx-power threshold. HALARM: high-alarm threshold value, range from -40.00 to 10.00 dBm HWARN: high-warning threshold value, range from -40.00 to 10.00 dBm LWARN: low-warning threshold value, range from -40.00 to 10.00 dBm LALARM: low-alarm threshold value, range from -40.00 to 10.00 dBm The HALARM value should not smaller than HWARN value. The LWARN value should not smaller than LALARM value.

34.2.2. Alarm/Warning Trap

In addition to the alarm or warning message, the optical module monitor will also send a trap message to the smmp server.

Node	data
Mib files	TNPL_private_2.1.89(interface_ddm).mib
Alarm oid	1, 3, 6, 1, 4, 1, 37831, 101, 110, 1
Warning oid	1, 3, 6, 1, 4, 1, 37831, 101, 110, 2
Ifindex oid	1, 3, 6, 1, 4, 1, 37831, 100, 30, 2, 1, 1
Information oid	1, 3, 6, 1, 4, 1, 37831, 100, 30, 2, 1, 2

34.2.3. Display Port Optical Module DDM Information

- Show interface optical-transceiver information

Display the information of the optical/copper module inserted in the optical port.

Command	SWITCH#**show interface {**IFNAME **|} optical-transceiver {info |}**
Description	If no interface-id is specified, the module information of all ports will be displayed. If info is not specified, the DDM information of the port module will be displayed, and if specified, the complete module information (basic information, alarm information, manufacturer information) will be displayed.

DDM information display elements are as follows:

Key Word	Description
Temp	The temperature of the module, in °C, accurate to 1°C.
Voltage	The voltage of the module, the unit is V, accurate to 0.01V.
Bias	The current of the module, in mA, accurate to 0.01mA.
RX power	The received optical power of the module, in dBm, accurate to 0.01dBM.
TX power	The transmit optical power of the module, in dBm, accurate to 0.01dBM.
OK	normal, no intervention required.
WARN	Alarm, indicating that the allowable range of the device is exceeded, and attention should be paid to.
ALARM	Abnormal, indicating that the device's allowable state is seriously exceeded and immediate intervention is required.
ABSENT	Absent.
NA	Port not supported/module not supported.
TIMEOUT	Time out.
ERR	Mistake.

Display all port module DDM information

```
SWITCH#show interface optical-transceiver
  Port      Temp        Voltage        Bias          RX power       TX power
            [C]           [V]          [mA]           [dBm]          [dBm]
-------- ----------- -------------- -------------- -------------- --------------
GiE0/9     42(OK)         3.20(OK)      32.34(OK)      -3.98(OK)       1.64(OK)
GiE0/10    ABSENT         ABSENT        ABSENT         ABSENT         ABSENT
GiE0/11    ABSENT         ABSENT        ABSENT         ABSENT         ABSENT
GiE0/12    ABSENT         ABSENT        ABSENT         ABSENT         ABSENT
```

- Display the overall information of the port optical module/copper module

Error message:

Key Word	Description
Transceiver absent!	Failed to get information, maybe the module is not in place.
Get transceiver info timeout!	Timeout to get information, need to get it again.
Port doesn't support get module info!	The port does not support getting module information.

Basic Information

Key Word	Description
Transceiver Type	module type.
Connector Type	Interface Type.

Wavelength(nm)	Wavelength.
Link Length	Supported link lengths.
Digital Diagnostic Monitoring	Whether to support DDM function.
Vendor Serial Number	Module serial number.

Warning Information

Key Word	Description
RX Channel loss of signal	Received signal loss.
RX Channel power high	High received optical power alarm.
RX Channel power low	Low received optical power alarm.
TX Channel fault	Send Error.
TX Channel bias high	Bias current high alarm.
TX Channel bias low	Bias current low alarm.
TX Channel power high	Sending high optical power alarm.
TX Channel power low	Sending low optical power alarm.
Temperature high	High temperature alarm.
Temperature low	Low temperature alarm.
Voltage high	High voltage alarm.
Voltage low	Low voltage alarm.
None	no alarm.
This module doesn't support getting alarm!	The module does not support getting alarm information.

Manufacturer information

Key Word	Description
Vendor Name	Manufacturer Names.
Vendor OUI	Manufacturer OUI.
Vendor Part Number	Manufacturer part number.
Vendor Revision	Manufacturer version number.
Manufacturing Date	Production Date.
Encoding	encoding type.

Displays overall information about a single port module

```
SWITCH#show interface gigabitEthernet0/9 optical-transceiver info
#####################################################
                  gigabitEthernet0/9
+-------------------------------------------------+
|Transceiver base information:                    |
+-------------------------------------------------+
|Transceiver Type    :  1000BASE-ZX-SFP           |
|Connector Type      :  LC                        |
|Wavelength(nm)      :  1550                      |
|Link Length     :                                |
|    SMF fiber                                    |
|        -- 80km                                  |
|Digital Diagnostic Monitoring  : YES             |
|Vendor Serial Number           : WT1703230031    |
+-------------------------------------------------+
|Transceiver current alarm information:           |
+-------------------------------------------------+
|None                                             |
+-------------------------------------------------+
|Transceiver vendor information:                  |
```

```
+-----------------------------------------------+
|Vendor Name          : OEM                     |
|Vendor OUI           : 000000                  |
|Vendor Part Number   : SFP-GE-ZX-SM1550        |
|Vendor Revision      : V2                      |
|Manufacturing Date   : 2017-03-25              |
|Encoding             : 8B10B                   |
+-----------------------------------------------+
SWITCH#
```

Displays overall information for all port blocks

```
SWITCH#show interface optical-transceiver info
#####################################################
                  gigabitEthernet0/9
+-----------------------------------------------+
|Transceiver base information:                  |
+-----------------------------------------------+
|Transceiver Type    :  1000BASE-ZX-SFP         |
|Connector Type      :  LC                      |
|Wavelength(nm)      :  1550                    |
|Link Length     :                             |
|    SMF fiber                                  |
|        -- 80km                                |
|Digital Diagnostic Monitoring  : YES           |
|Vendor Serial Number           : WT1703230031  |
+-----------------------------------------------+
|Transceiver current alarm information:         |
+-----------------------------------------------+
|None                                           |
+-----------------------------------------------+
|Transceiver vendor information:                |
+-----------------------------------------------+
|Vendor Name          : OEM                     |
|Vendor OUI           : 000000                  |
|Vendor Part Number   : SFP-GE-ZX-SM1550        |
|Vendor Revision      : V2                      |
|Manufacturing Date   : 2017-03-25              |
|Encoding             : 8B10B                   |
+-----------------------------------------------+
#####################################################
                  gigabitEthernet0/10
+-----------------------------------------------+
|Transceiver base information:                  |
+-----------------------------------------------+
|Transceiver Type    :  1000BASE-GT-SFP         |
|Connector Type      :  Unknown or unspecified  |
|Wavelength(nm)      :  16652                   |
|Link Length     :                             |
|    Cable Assembly copper                      |
|        -- 100m                                |
|Digital Diagnostic Monitoring  : NO            |
|Vendor Serial Number           : MTC100046     |
+-----------------------------------------------+
|Transceiver current alarm information:         |
+-----------------------------------------------+
This module doesn't support getting alarm!
|This module doesn't support getting alarm!     |
+-----------------------------------------------+
|Transceiver vendor information:                |
+-----------------------------------------------+
```

```
|Vendor Name          : OEM                          |
|Vendor OUI           : 000000                       |
|Vendor Part Number   : SFP-T-CBTX                   |
|Vendor Revision      : F                            |
|Manufacturing Date   : 2014-10-01                   |
|Encoding             : 8B10B                        |
+------------------------------------------------+
##################################################
                    gigabitEthernet0/11
Get result error(Maybe Transceiver absent)!
##################################################
                    gigabitEthernet0/12
Get result error(Maybe Transceiver absent)!
SWITCH#
```

- Show interface opticatl-transceiver threshold information

Display the information of the optical/copper module inserted in the optical port.

Command	SWITCH#**show interface {**IFNAME **|} optical-transceiver threshold**
Description	If no IFNAME is specified, the module information of all ports will be displayed. If the threshold is not configured, the own threshold information of the module will be displayed.

```
SWITCH#show interface optical-transceiver threshold

Interface tengigabitEthernet0/25:
Item            High-alarm      High-warn       Low-warn        Low-alarm
Temp(Celsius)   100             90              -40             -50
Voltage(V)       3.50            3.47            3.15            3.04
Bias(mA)        15.00           12.00           4.00            5.58
RX power(dBm)   10.25           5.30            -10.22          -12.40
TX power(dBm)   2.100           1.100           -9.100          -11.00
```

34.3. Dying Gasp

Dying Gasp is referenced in section 7.1.2.5.3 of ITU-T Recommendation G.991.2 (12/2003) as the Power Status bit.

The networking devices rely on a temporary back-up power supply on a capacitor, that allows for a graceful shutdown and the generation of the dying-gasp message. This temporary power supply is designed to last from 10 to 20 milliseconds to perform these tasks.

In addition to the dying-gasp message, the power-down device will also send a trap message to the smmp server.

Node	data
Mib files	DOT3-OAM-MIB.mib
oid	1, 3, 6, 1, 2, 1, 158, 1, 6, 1, 4
value	dyingGaspEvent(257)

- Enable dying-gasp

Command	SWITCH(config)#**dying-gasp enable** SWITCH(config)#**no dying-gasp**
Description	Enable dying gasp function

LOG messages

For example：”Device 00:d0:f8:c8:23:12 power down.”

34.4. Cable Detect

A cable fault may cause the interface to be in the Down state or the interface rate to be abnormal even though the interface is in the Up state. Users can execute this command to detect whether the cable is faulty and locate the fault point to help solve the cable fault. Please pay attention to the following points when using the cable detection function:

✧ Only copper interfaces support this command.

✧ When this command is executed, the normal service of the interface may be affected in a short period of time.

✧ When the line length is less than 6 meters, there will be a deviation between the test results and the actual value. The shorter the line, the greater the deviation.

- Port Performs Cable Detection Function

Command	SWITCH(config-if)#**cable-detect**
Description	Perform a cable detection on the port. After 2 seconds, use the show command to view the detection results.

Perform a cable test on port g i0 /1:

```
SWITCH# configure terminal
SWITCH(config)#interface gigabitEthernet 0/1
SWITCH(config-if)#cable-detect

%Please wait for about 2 seconds and execute the show cable-detect command to view
the execution results.
```

View cable test results:

```
SWITCH#show cable-detect interface gigabitEthernet 0/1
Pair A length(meters): 0
Pair B length(meters): 0
Pair C length(meters): 0
Pair D length(meters): 0
Pair A state: OK
Pair B state: OK
Pair C state: OK
Pair D state: OK
```

Field	Explain
Pair X length(meters)	Cable length. When there is a fault, it represents the length from the interface to the fault. Unit: meter
Pair X state	Network cable status: OK: Indicates that the line pair is terminated normally. Open: Indicates that the line pair is open. Short: Indicates a short circuit on the pair. Unknown: Other unknown causes of failure.

Switch Web Operation Manual

pages 221-363

The corresponding software version of this manual is： Release 7.3.x

Document version number：V6.0

Release time：2024.11.23

1 Overview

1.1 Introduction

In order to facilitate network administrators to operate and maintain network devices, our company has specially launched the device's web management function, which allows administrators to intuitively manage and maintain devices using the web interface. The operating environment of the Web network management is shown in Figure 1-1.

Figure 1-1 Web network management operation environment

1.2 Log in to the Web network management.

When a user logs into the web network management for the first time, he or she needs to use the default account to log in. After logging in, in order to ensure the security of the device, he or she needs to change the password immediately. The specific operation steps are as follows:

- Log in to the Web administrator using the default account
- Change user password

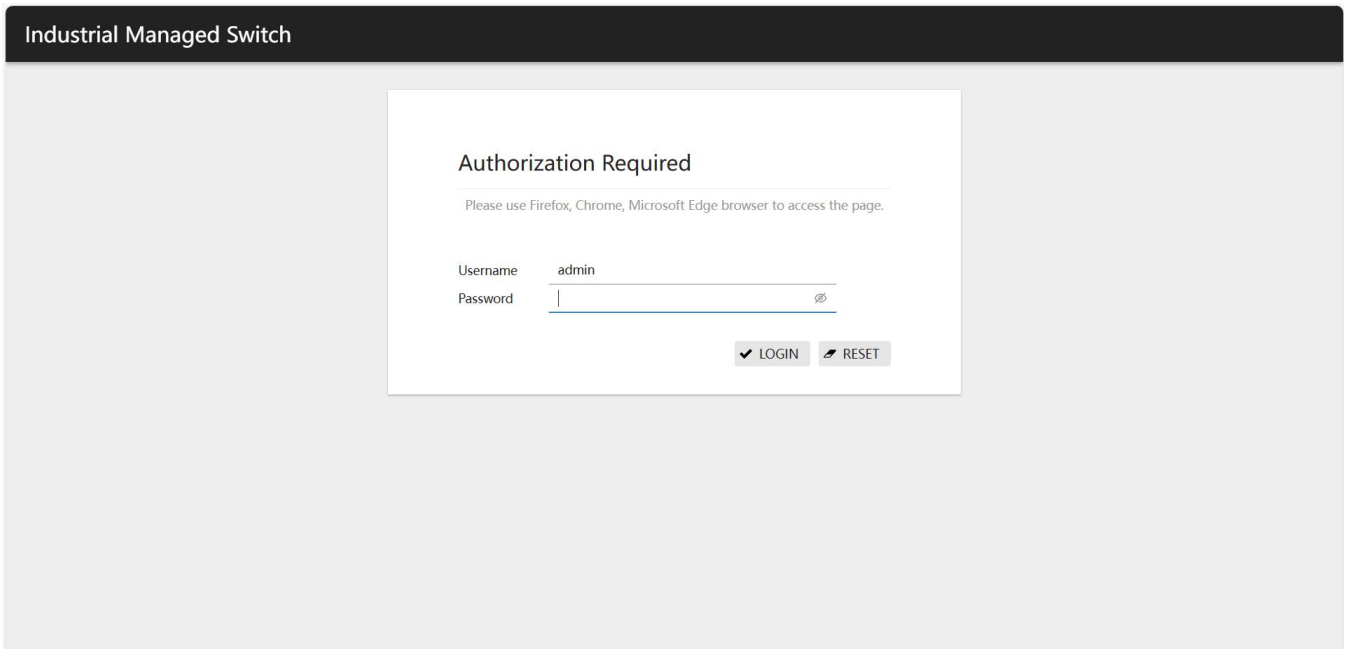
---

illustrat

For the specific operation process of changing the password, see Chapter 7.2, see User Management.

The Web server service is enabled by default when the device leaves the factory, and there is a default login account: the user name is admin, the login password is admin, and the IP address is 192.168.1.168. Users can use this information to complete the first login of the Web network management. It introduces how to log in to the device through the web. The specific steps are as follows:

Figure 1-2 Web login interface



(1) Connect the device and PC, and use a network cable to connect the PC to the Ethernet port on the device (by default, all ports belong to VLAN 1).

(2) Configure the IP address for the PC and set the IP address of the PC and the default VLAN interface IP address of the device are the same as the network segment (except for the default IP address of the device), such as 192.168.1.123.

(3) Start the browser and enter the login information.

Start the browser on the PC, enter "192.168.1.168" in the address bar and press Enter to enter the device's web login page, as shown in Figure 1-2. Enter the default account "admin" and password "admin", click the [Login] button to log in to the Web network administrator

In order to get better display effects, it is recommended to use Edge, Firefox or Chrome browser. Please upgrade to the latest version of Chrome browser.

1.3 Exit of Web Network Management

Notice

• When exiting Web network management, the system will not automatically save the current configuration. Therefore, it is recommended that users set and save the current configuration before exiting the Web network management.

Operation steps:

Click the logout icon button on the navigation bar of the Web Network Management page to click "Login" to exit the WEB Network Management. (as shown in Figure 1-3)

Figure 1-3 Exit of Web Network Management

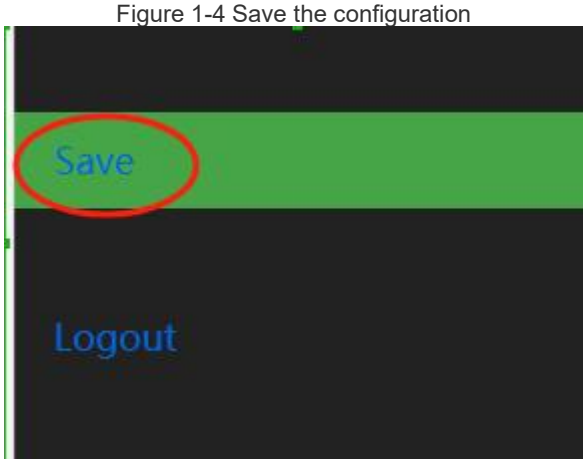
1.4 Save configuration

Notice

- After all projects are configured on the page, be sure to save the configuration, otherwise unsaved configuration information will be lost due to restart and other operations.

Click the save icon button in the upper right corner of the Web Network Management page (as shown in Figure 1-4) to save the current configuration to the configuration file. The configuration is still valid after restarting or power-down restart.

Figure 1-4 Save the configuration



There are two situations for saving configuration:

(1) Click the [OK] or [Apply] button on the current configuration interface to save the current configuration to memory. Saving at this time does not mean that the configuration item is actually saved to the configuration file. If the switch fails or other failures at this time, the configuration of the interface will fail.

(2) Click the [Save] button below the navigation bar, and the system will automatically save the configuration of all pages to the configuration file.

1.5 Restart the device

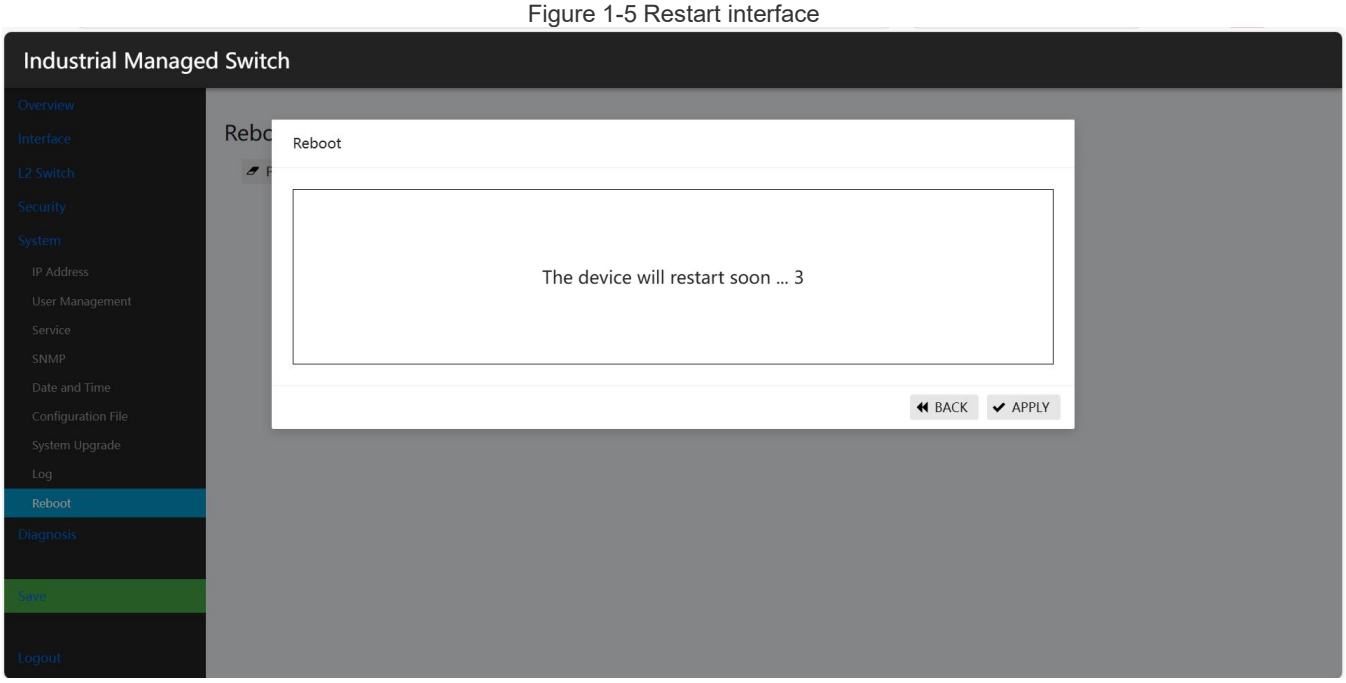
Notice

•Be sure to save the configuration before restarting the device, otherwise all unsaved configurations will be lost after restarting.

•After the device restarts, the user needs to log in to the device again.

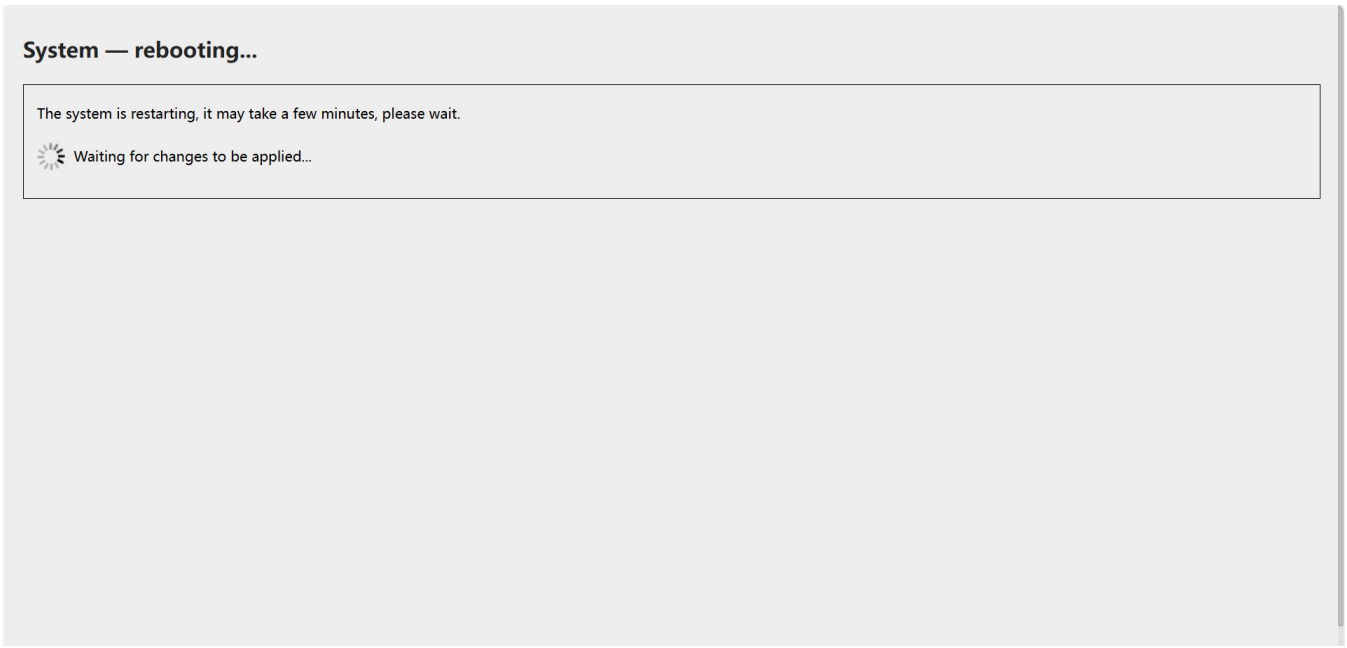
Step 1: Click the restart icon button of the Web network management navigation bar page system (as shown in Figure 1-5), and click the "Execute Restart" button in the pop-up dialog box.

Figure 1-5 Restart interface



Step 2: If the [Application] button is not clicked, you need to wait for the countdown to end and the device enters a restart state. The device will take a certain amount of time to restart, please be patient.

Figure 1-6 Restart waiting interface



1.6 Introduction to Web Management Page Layout

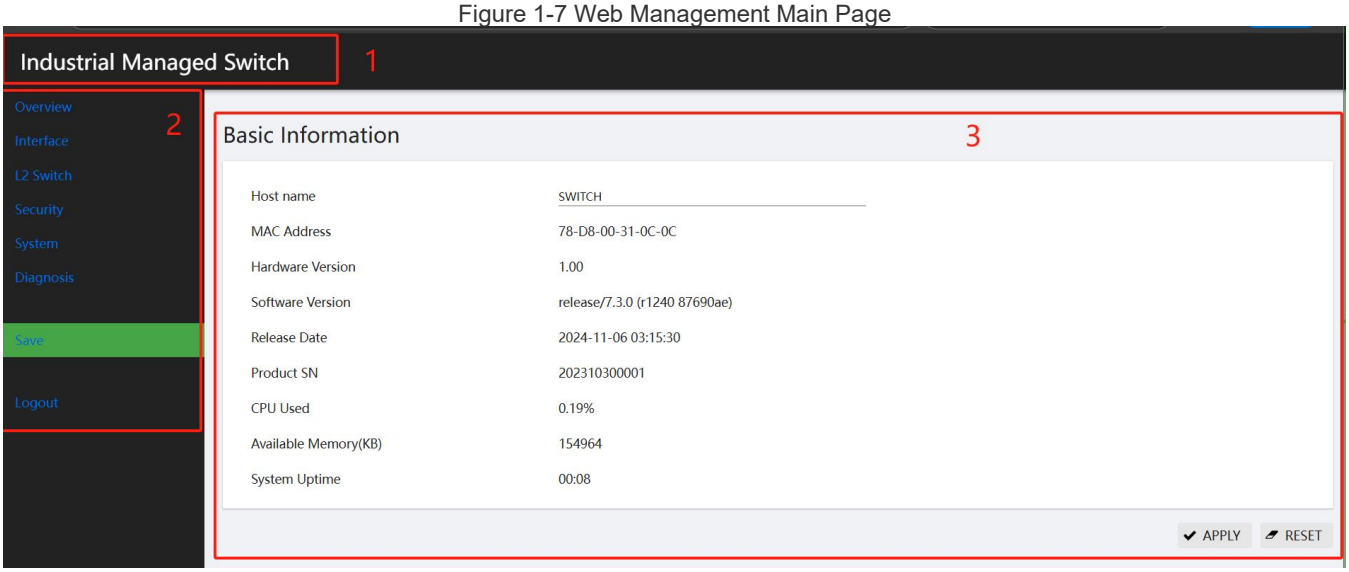
As shown in Figure 1-7, the main web management page is divided into four parts: product model, navigation bar, language selection button, configuration area, and each part of the functions.

As shown in 1-8.

Table 1-8 Web layout description

Configuration Items	illustrate
Product model	Used to display the model of the product
Navigation bar	The web network management function menu of the device is organized in the form of a navigation tree, and users can easily select the function menu results in the navigation bar Displayed in the configuration area.
Configuration area	Used to configure functions

Figure 1-7 Web Management Main Page



(1) Product model	(2) Navigation bar	(3) Configuration area	

1.7 Introduction to Web Management Functions

The specific description of the Web network management function is shown in Table 1-9.

Table 1-9 Web network management function description

Menu/Tab		Function Description
Overview		Basic Information
interface	Interface Port Management	Displays relevant information about all ports and sets various characteristics of the port
	Port speed limit	Display/set the port speed limit
	Storm Control Display	set the suppression ratio of broadcast, multicast, and unknown list broadcast of ports
	Port statistics Display	query, and clear interface statistics information
	Port mirroring	Display/set/delete port mirroring
	Port isolation	Display/set/delete port isolation

	Port aggregation	Display/configure port aggregation algorithm
Swap	VLAN	Create, modify, and delete VLANs, configure port properties and VLAN homes
	QinQ	functions for displaying, configuring, and deleting ports
	ERPS	displays the status of ERPS, previous event, ring number, east interface, west interface, etc.
	IGMP Snooping	IGMP Snooping Turn on/off IGMP Snooping function
	Spanning Tree	Displays port loop status
	MAC address management	Set the aging time of the MAC address
	LLDP	display, configure, and delete the LLDP function of the device
Apply	DHCP Server	to configure the device's DHCP server functionality
Routing	Layer 3 port	Display/configure IP based on port
	Static routing	Configure static routing
	ARP neighbor	Configure ARP/neighbor function
Secure	ACL	Configure the ACL function of the device
	DOS	configuration device DoS functionality
	QOS	configuration device DoS function
	DHCP Snooping	Configure the DHCP Snooping function of the device
	802.3X authentication	Configure 802.1X authentication
	MAC Authentication	Configuring MAC Authentication Overview
	RADIUS	Configure the RADIUS server
	Port security	Configure and delete port security functions
	IP Source Guard	Configuring and deleting IP Source Guard functions
System	Management Information	Set the management IP address of the device
	User Management	Set user password
	Service	Configure the telnet, ssh, HTTP Server servers to turn on/off

	SNMP	Configure SNMP Server
	Date and Time	Display/set the current date and time of the system
	Configuration file	Configure download backup, restore backup, and restore factory configuration
	System upgrade	configuration upgrade firmware
	Log	Configure download logs to create, edit, and delete syslog server
	Restart	Restart the switch
Diagnosis	Network tools	Perform ping/trace route operation and display execution results
	Dying Gasp	Turn on/off the dying gasp power-down alarm function
	Optical module	information View optical module information, such as manufacturer information, serial number, optical power, etc.
Save		Globally save switch configuration information
Log out		Exit WEB management

2 Overview

Click [Overview] in the navigation bar to enter the system basic information page. This page can display the device's MAC address, software and hardware version and other information. The specific parameter description is shown in Table 2-1 System Basic Information

Basic information	
Host Name	**SWTCH**
MAC address	**78-D8-00-31-0C-0C**
Hardware version	**V1.00**
Software version	**release/7.3.0** **(r1240 87690ae)**
Release time	**2024-11-06 03:15:30**
Product serial number	**202310300001**
CPU usage	**0.59%**
Available memory (KB)	**166892**
Running time	**00:20**

Table 2-1 Basic information parameter description

Configuration Item	Description

Host name	Used to indicate the product model of the device
MAC address	Used to indicate the MAC address of the device
Hardware version	Used to indicate the hardware version number of the device
Release time	Used to indicate the software version of the device
Software version	Used to indicate the software version number of the device
Product serial number	Used to indicate the product serial number of the device
CPU occupancy is	used to display the current CPU occupancy rate
Available memory is	used to display the available memory of the current system
Run time	Used to indicate the duration of continuous operation of the device after the last startup. The device will be re-timed after restarting.

3 interface

3.1 Port Management

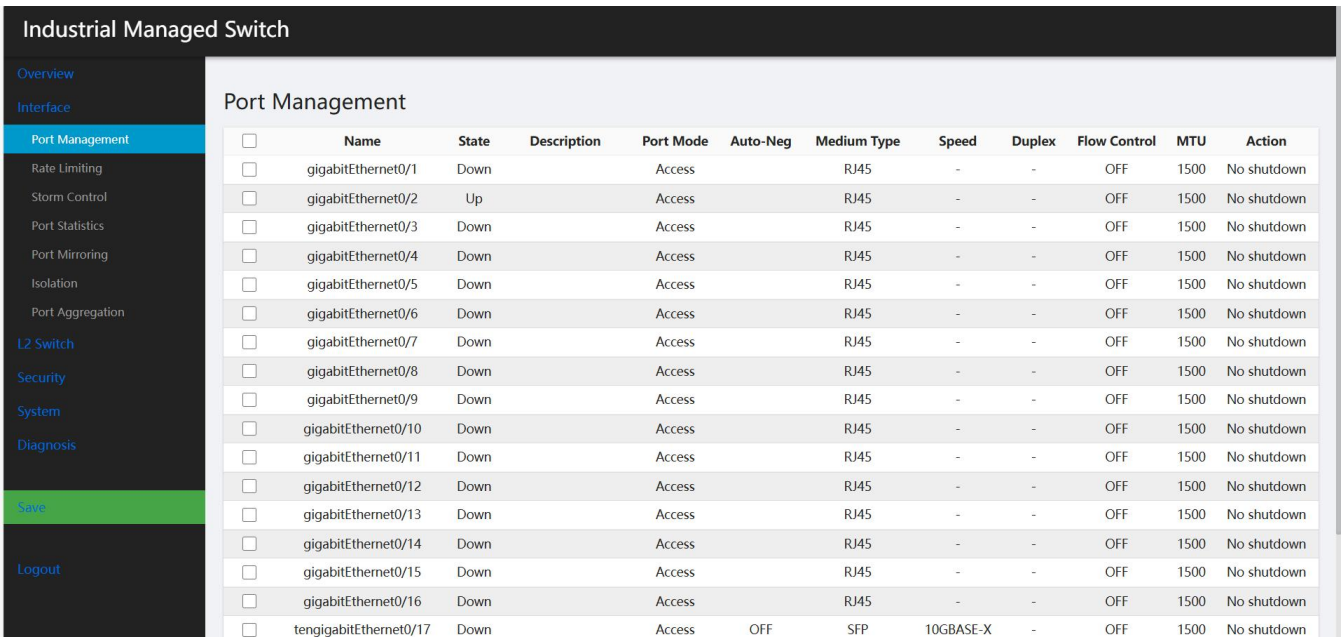
illustrate

- Due to the different parameters of the electrical port and optical port, it is recommended to configure the electrical port and optical port separately when selecting a multi-port configuration.

The port management module is used to configure and view the working parameters of the Ethernet interface, including: name, description, port mode, media type, rate,

Duplex state, flow control, MTU, and state, as shown in Figure 3-1.

Interface status diagram 3-1



Name	State	Description	Port Mode	Auto-Neg	Medium Type	Speed	Duplex	Flow Control	MTU	Action
gigabitEthernet0/1	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/2	Up		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/3	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/4	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/5	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/6	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/7	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/8	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/9	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/10	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/11	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/12	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/13	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/14	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/15	Down		Access		RJ45	-	-	OFF	1500	No shutdown
gigabitEthernet0/16	Down		Access		RJ45	-	-	OFF	1500	No shutdown
tengigabitEthernet0/17	Down		Access	OFF	SFP	10GBASE-X	-	OFF	1500	No shutdown

Operation steps:

（1）Select [Interface] [Port Management] in the navigation bar, as shown in Figure 3-1.

（2）Check the port you want to configure (support multiple ports), click the [Edit] button to enter the page shown in Figure 3-2.

（3）The working parameters of the configuration port are shown in Table 3-3.

（4）Click the [Apply] button to complete the operation.

（5）Click the [Save] button in the navigation bar to save the configuration.

Go to the interface configuration table 3-2 page.

Table 3-3 Interface working parameters description

Configuration	Item Description
Description	Sets the description information of the port, you can use a combination of letters and numbers.
Media Type	• The media type that configures the multiplexed port is valid only for ports that support photoelectric multiplexing (Combo). • RJ45: Set the port to operate in electrical port mode. • SFP: Set the port to work in optical port mode. • Does light spot adaptive need to be added here?
rate	• Set the port rate • 10M：10Mbps • 100M：100Mbps • 1000M：1000Mbps • AUTO：Automatic negotiation port speed
Duplex Status	• Set the duplex status of the port • AUTO：Self-negotiation duplex status • FULL：Full duplex state • HALF：Half Duplex state
Port mode (Applicable to optical ports only)	• Set the port's working mode to support different working modes, and different modes require corresponding optical modules to support them. • 100BASE-FX：Set the port to operate in 100M optical mode. • 1000BASE-X：Set the port to operate in Gigabit optical mode. • SGMII：Set the port to operate in SGMII mode. When the module inserted in the optical port is a Gigabit to 100 Gigabit optical (SFP GE-FX) or an optical to power

	module (Mini-GBIC-GT), it needs to be configured in this mode. • 2500BASE-X：Set the port to work in 2.5G optical port mode. • 10G BASE-X:Set the port to operate in 10G optical port mode.  hint • 2500BASE-Xmode, it may be incompatible with the port interconnection of other manufacturers. • The optical port capabilities of different models of equipment are different. Please refer to the instructions corresponding to the specific product model for details.
Self-negotiation(Applicable to optical ports only)	Turn on/off the self-negotiation function of optical ports. OFF：The optical port is turned off and the work is in a mandatory state. ON：The optical port opens self-negotiation.
Flow control	Set the Enable or Disable port flow control function When both the local and the peer device enable the flow control function, if the local device is congested, it will send a message to the peer device, notifying the peer device to temporarily stop sending messages; the peer device will temporarily stop sending messages to the home device after receiving the message; and vice versa. This avoids the occurrence of message loss  hint Only when the flow control function is enabled on the local and peer ports can flow control be realized
MTU	MTU sets the frame length that is allowed to forward, and the supported frame length range is 46-10222 bytes, and the default is 1500 bytes.
Management Status	• Set the on/off status of the port. • No shutdown：Set the port to work in normal working state. • Shutdown：Set the port to work in a closed state.

Configuration example:

Case requirements: Configure port GigabitEthernet0/1 to 1G working mode, turn off flow control, set MTU to 10000 bytes, and port description is abc.

Step 1: Select [Interface] and [Port Management] in the navigation bar to enter the port management interface.

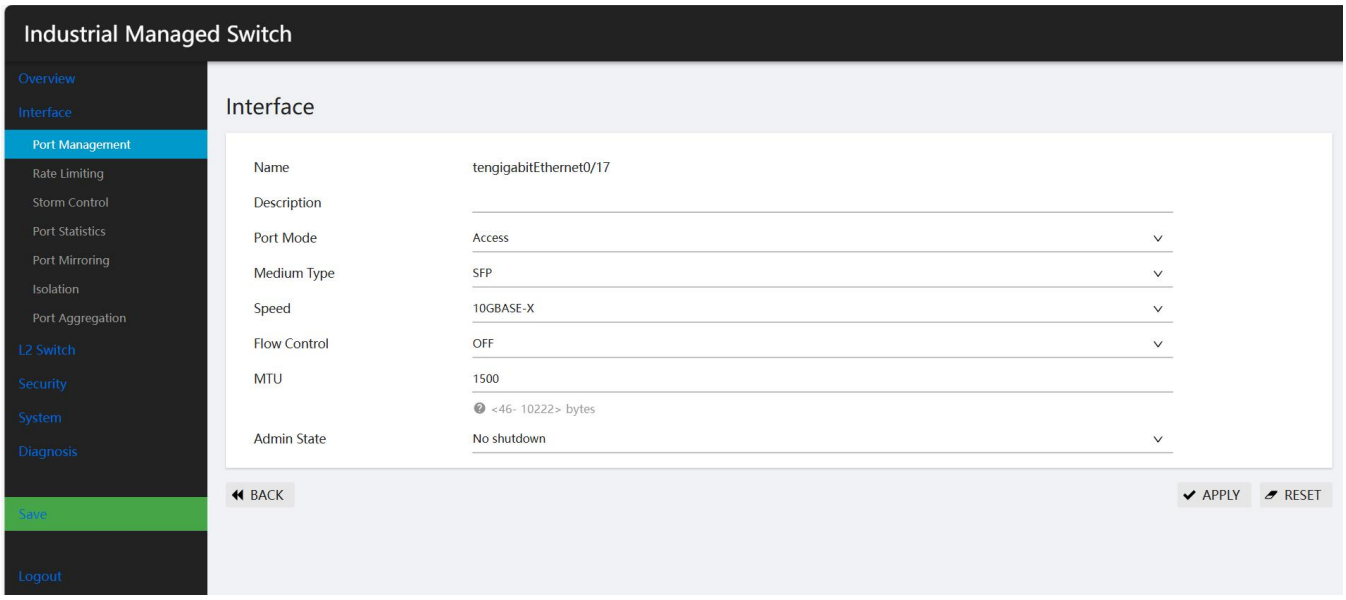
Step 2: Select the port GigabitEthernet 0/9, click the [Edit] button to enter the port configuration interface, as shown in Figure 3-4.

Step 3: As shown in Figure 3-4, follow the description "abc", media type "SFP", port mode "1000BASE-X", flow control "OFF", MTU "1500", management status "No shutdown", and configure the parameters.

Step 4: Click the [Confirm] button to complete the operation.

Step 5: Click the [Save] button in the auxiliary bar to save the configuration.

Figure 3-4 Example of interface configuration



3.2 Port speed limit

Port speed limit is based on the port's rate limit, which limits the total rate of port input and output packets. Before the traffic is sent from the interface, speed limit is configured in the outgoing direction of the interface to control all outgoing packets. Before the traffic is received from the interface, a speed limit is configured in the inlet direction of the interface to control all incoming packets.

Operation steps:

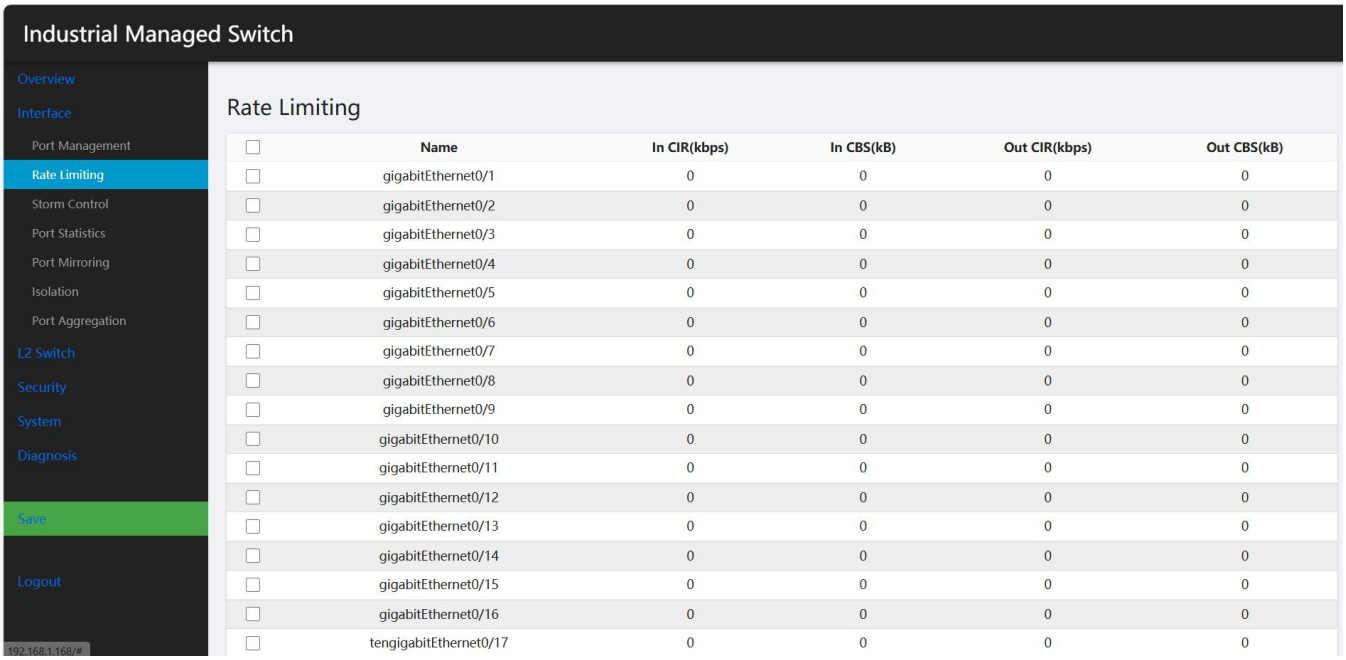
(1) Select [Interface] [Port Speed Limit] [Select Port] in the navigation bar to enter the port speed limit configuration interface, as shown in Figure 3-5.

(2) For ports that need to be configured with speed limit, enter the corresponding value in the dialog box. The specific parameter definitions are shown in Table 3-6.

(3) Click the [Apply] button on the corresponding port to complete the operation.

(4) Click the [Save] button in the navigation bar to save the configuration.

Figure 3-5 Port speed limit interface



illustrate

•The limit value is determinable. For example, if the speed limit is 1M, then the limit value is 1024, but the burst value is taken from the empirical value. When burst

The numerical value is large, the flow spike is higher, the speed limit is relatively stable, but the average rate may be higher than the speed limit; when the burst value is small, the flow spike is lower, the speed limit

The fluctuates greatly and the average rate may be less than the speed limit value. It is recommended that the burst configuration take a 4-fold limit value and a small value of 16384.

Table 3-6 Parameter Description

Configuration Item	Description
Name	Port Name
Input rate (kbps)	Bandwidth limit per second in the input direction (KBits)
Input burst traffic (KB)	Burst traffic limit value in input direction (Kbytes)
Output rate (kbps)	Bandwidth limit per second in the output direction (KBits)
Output burst flow (KB)	Burst flow limit value in the output direction (Kbytes)
Action	Edit or delete this regulation

Configuration example:

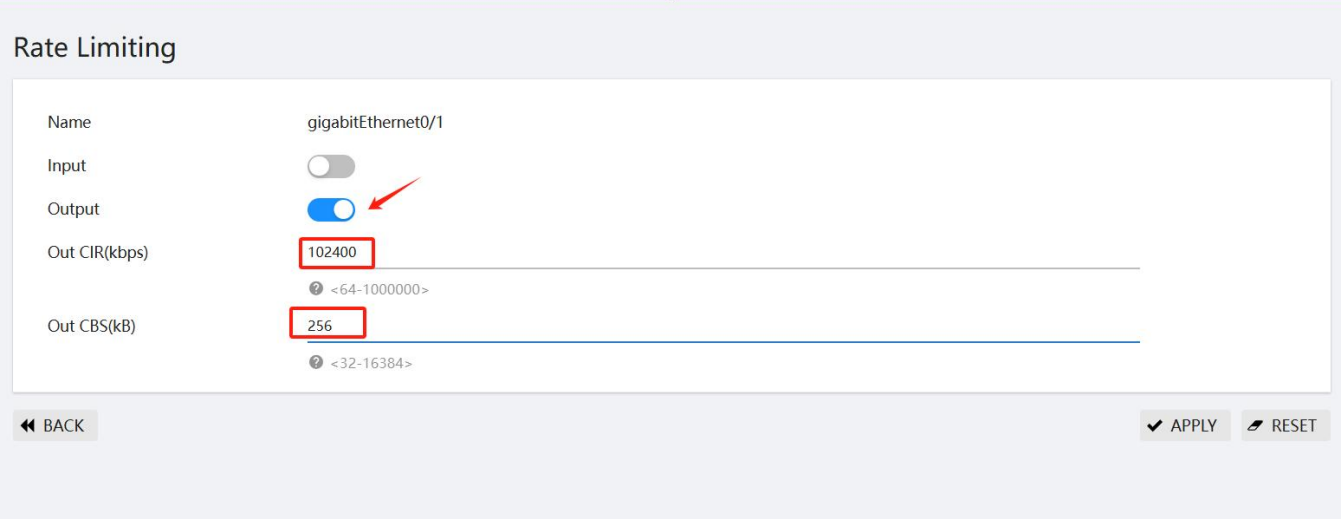
Case requirements: Assuming that the switch's port GigabitEthernet0/1 is connected to the Internet, the traffic limit on the port GigabitEthernet0/1 is required to exit the traffic limit, the bandwidth limit is 102400KBits per second, and the burst traffic limit is 256Kbytes per second.

Step 1: Select [Interface] [Port Speed Limit] [Select Port 1] [Edit] in the navigation bar to enter the port speed limit configuration interface.

Step 2: Click the Close input speed limit button and enter the corresponding value in the output speed limit dialog box, as shown in Figure 3-7.

Step 3: Click the [Apply] button to complete the configuration.

Figure 3-7 port speed limit configuration interface



(4) Click the [Save] button in the navigation bar to save the configuration.

3.3 Storm Control

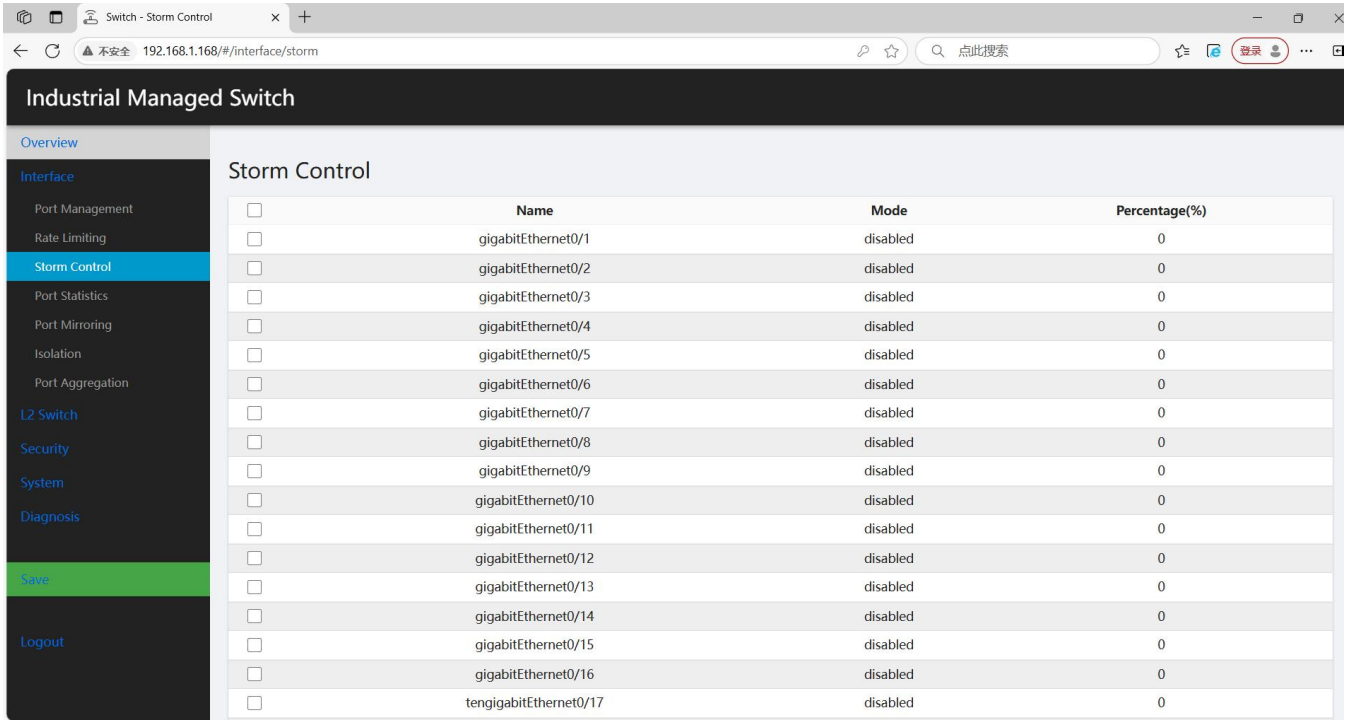
When there are excessive broadcast, multicast or unknown unicast data streams in the LAN, the network performance will decline and even the network is paralyzed, which is called a broadcast storm. Storm control limits the speed of broadcast, multicast and unknown unicast data streams. When the rate of broadcast, unknown multicast or unknown unicast data streams received by the switch port exceeds the set bandwidth, the device will only allow data streams through the set bandwidth, and data streams beyond the bandwidth will be discarded, thus avoiding excessive flooding data streams entering the LAN to form storms.

The storm control module is used to set the port's suppression ratio for broadcast, multicast, and unknown list messages. The storm control mode is adopted based on the bandwidth percentage. When the rate of data stream received by the device port exceeds the set bandwidth, the device will only allow data streams through the set bandwidth, and the data streams beyond the bandwidth will be discarded until the data stream returns to normal.

Configuration steps:

(1) Select [Interface] [Storm Control] [Select Port] [Edit] in the navigation bar to enter the storm control interface, as shown in Figure 3-8.

Figure 3-8 Storm Control Status Interface



(2) Click the "Storm Control" button to enter the port to set storm control. The detailed configuration is shown in Table 3-9

(3) Configure the storm suppression type and bandwidth suppression ratio of the port. The detailed configuration is shown in Table 3-10.

(4) Click the [Confirm] button to complete the operation.

(5) Click the [Save] button in the navigation bar to save the configuration.

Figure 3-9 Port configuration interface

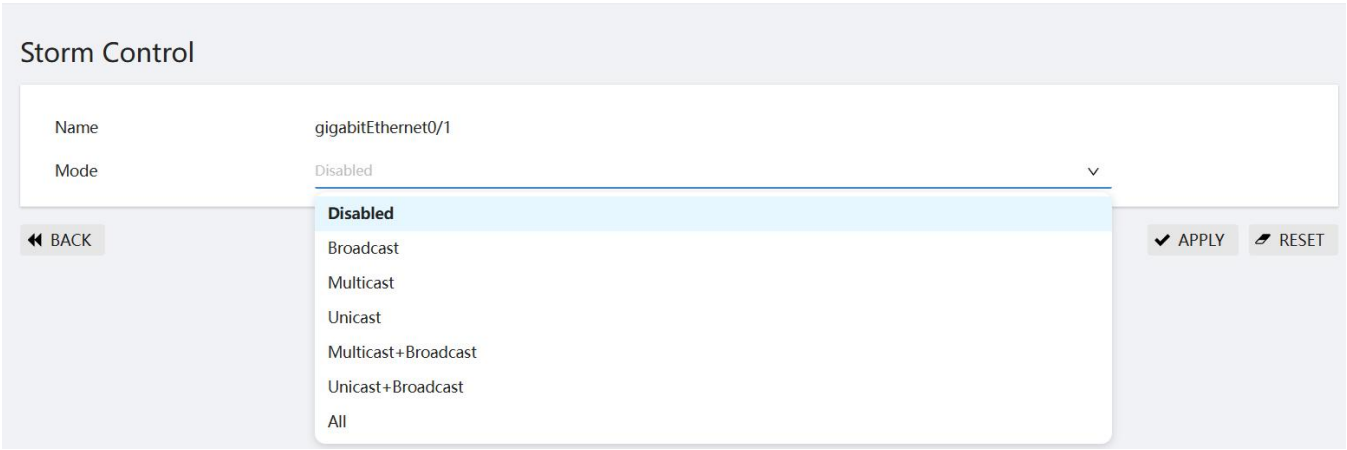


Table 3-10 Parameter Description

Configuration Items		illustrate
name		Selected port
Type	disabled	Turn off this feature.
	broadcast	Turn on the broadcast message storm suppression function to achieve traffic limit on broadcast messages.
	multicast	Turn on the storm suppression function of unknown multicast messages, which can limit traffic on unknown multicast messages.
	unicast	Turn on the unknown list message storm suppression function, which can limit traffic

		on unknown list messages.
	multicast – broadcast	Turn on the multicast message + broadcast message storm suppression function, which can limit traffic to unknown multicast messages and broadcast messages.
	unicast-broadcast	Turn on the unknown list message + broadcast message storm suppression function, which can limit traffic of unknown list message and broadcast message.
	all	Select Suppress Broadcast, Multicast, Unknown List
Bandwidth ratio (%)		The maximum allowed broadcast traffic account for a percentage of the port's transmission capacity. After selecting this item, you need to enter the specific percentage.

Configuration example:

Case requirements: Open storm control of port gigabitGigabitEthernet ernet 0/1, and set the suppression ratio of broadcast packets to 10%.

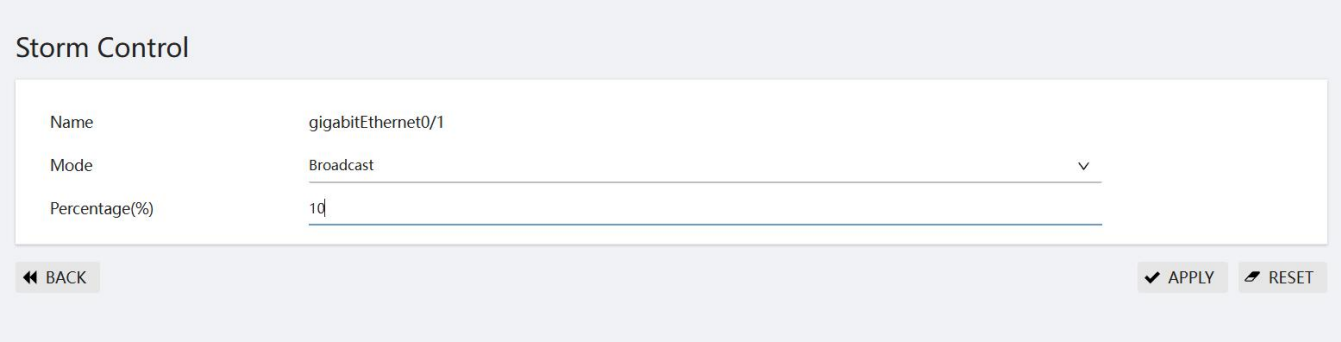
Step 1: Select [Interface] [Storm Control] in the navigation bar to enter the storm control interface.

Step 2: Select the port gigabitGigabitEthernet ernet 0/1, and click the [Edit] button to enter the configuration interface.

Step 3: Select the type broadcast and set the bandwidth ratio to 10, as shown in Figure 3-11.

Step 4: Click the [Apply] button to complete the operation.

Figure 3-11 Storm Control Configuration Interface



Step 5: Click the [Save] button in the navigation bar to save the configuration.

3.4 Port statistics

The "Port Statistics" page is used to display statistics about the number of messages received and sent by the port.

(1) Select [Interface] [Port Statistics] in the navigation bar and enter the port statistics page, as shown in Figure 3-12.

(2) Check the load and port speed of the device port receiving and sending, and the statistics of error packets on the page. The specific parameter description is as described in Table 3-13.

(3) Click the [Clear] button at the end of the port to clear the port count.

Figure 3-12 Port statistics page

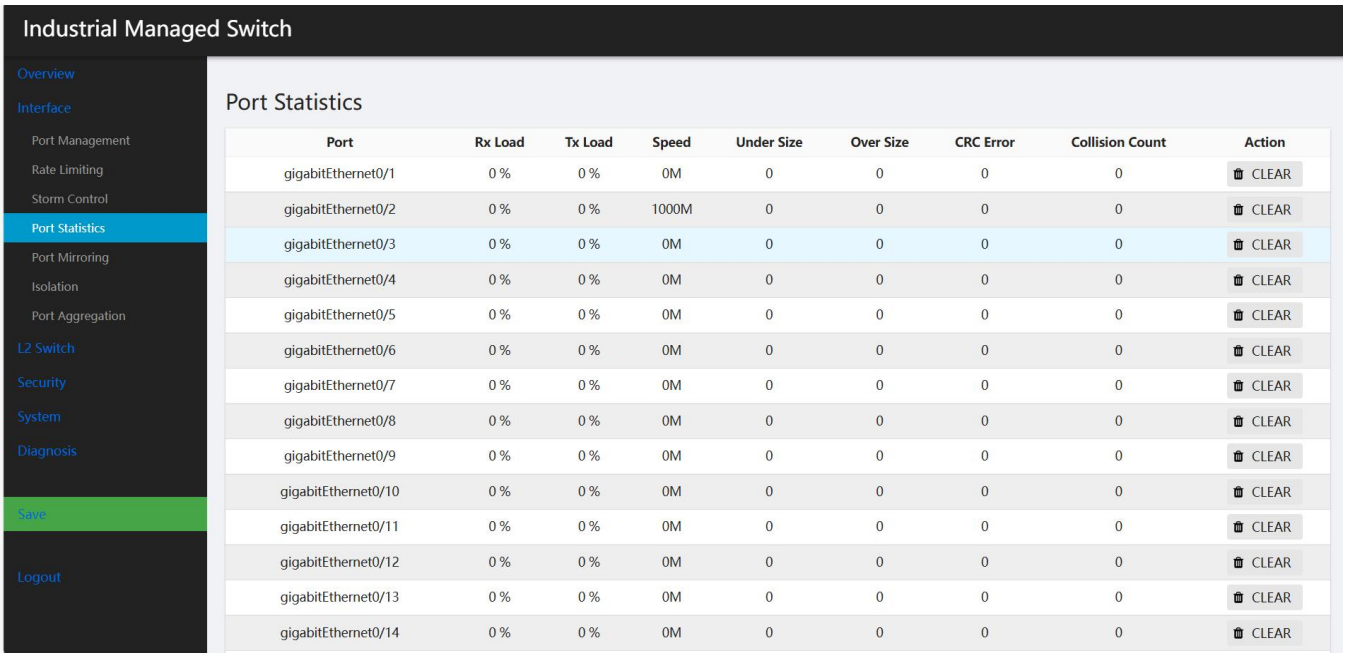


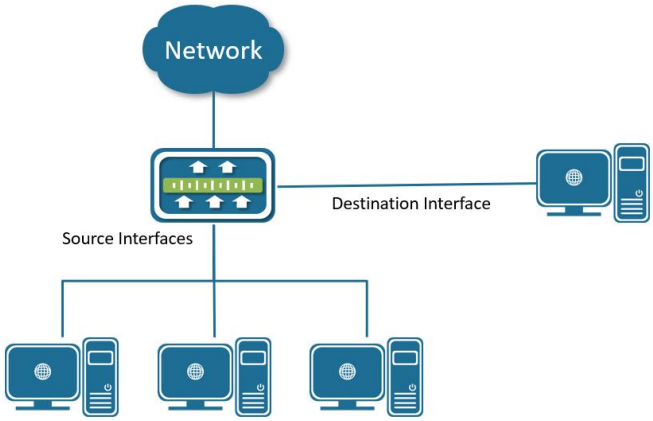
Table 3-13 Parameter Description

Configuration Items	illustrate
port	Switch port
Receive load	Port receiving load rate
Send load	Port send load rate
rate	Port operating rate
Incomplete packet	The number of messages received by the port is less than 64 bytes
Excessive data package	The number of messages received by the port is greater than the upper limit of the MTU configuration
CRC Error	Number of CRC verification error messages received by the port
Number of conflicts	Number of conflicting messages received by the port
Clear	Clear message

3.5 Port mirroring

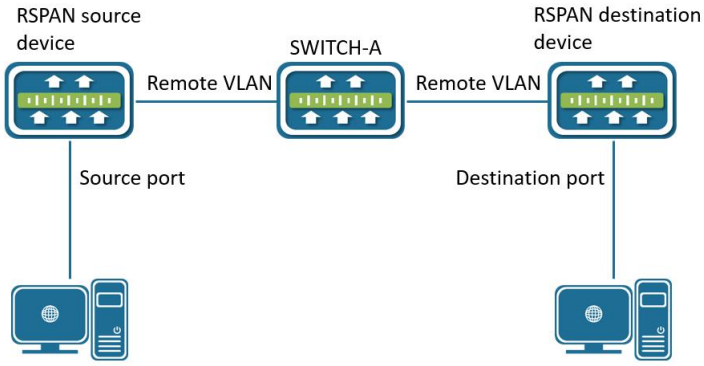
SPAN (Local Switched Port Analyzer) is a local mirroring function. The SPAN function copies the packets from the specified port to the destination port. Generally, the SPAN destination port will be connected to the data detection device. Users use these devices to analyze the messages received by the destination port to perform network monitoring and troubleshooting. The source port and destination port of the SPAN are on the same device, as shown in Figure 3-14.

Figure 3-14 Port mirroring



RSPAN (Remote Switch Port Analyzer, Remote Port Mirror) is an extension of SPAN. Multiple network devices can be spanned between the remote mirror source port and the destination port. The principle of remote mirroring is that the original device, intermediate device and destination device create a Remote VLAN, and all ports participating in the session must be added to the Remote VLAN. The mirrored packets are broadcasted within the Remote VLAN, so that the mirrored packets are transmitted from the source port of the source device to the destination port of the destination device, as shown in Figure 3-15.。

Figure 3-15 Remote port mirroring



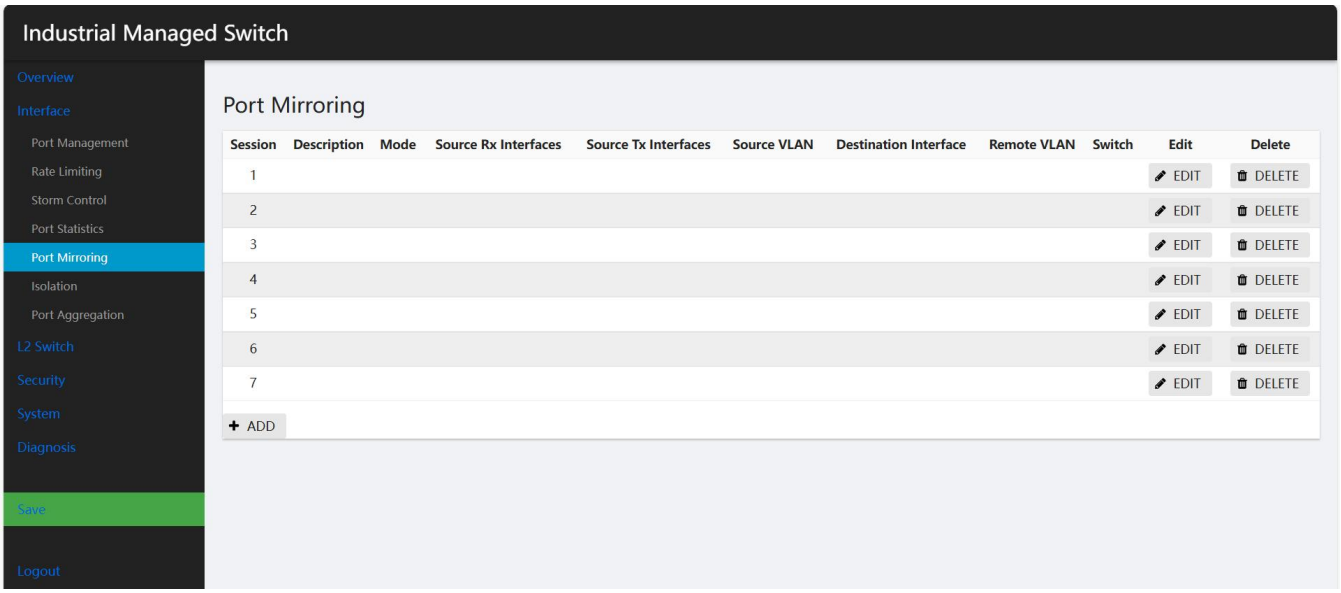
SPAN/RSPAN does not affect the packet exchange of the source port, but only copies all incoming and output packets on the source port to the destination port as it is. When the mirrored traffic of the source port exceeds the bandwidth of the destination port, for example, the destination port monitors the traffic of the 1000Mbps source port, which may cause the packet to be discarded.

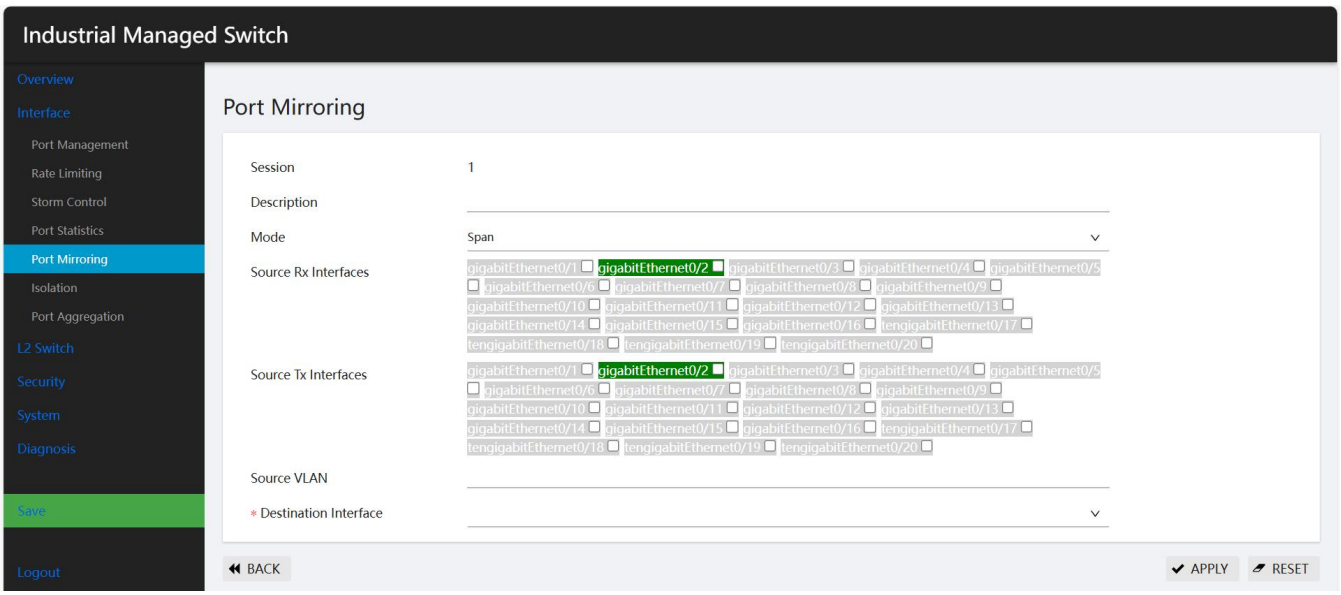
SPAN/RSPAN is based on session management and configures the source and destination ports of SPAN in the session. In a session, there can only be one destination port, but multiple source ports can be configured at the same time.

Configuration example:

(1) Select [Interface] [Port Mirroring] [Edit] in the navigation bar to enter the page as shown in Figure 3-16.

Figure 3-16 port mirror interface





(2) Select the session, destination interface, and source interface. The specific parameters are described in Table 3-17.

(3) Click the [Apply] button to complete the operation.

(4) Click the [Save] button in the navigation bar to save the configuration.

Table 3-17 Parameter Description

Configuration Items	illustrate
port	Switch port
Receive load	Port receiving load rate
Send load	Port send load rate

Configuration example:

Case requirements: Use port gigabitGigabitEthernet ernet 0/3 to monitor gigabitGigabitEthernet ernet 0/1 port and gigabitGigabitEthernet ernet 0/2 exit packet.

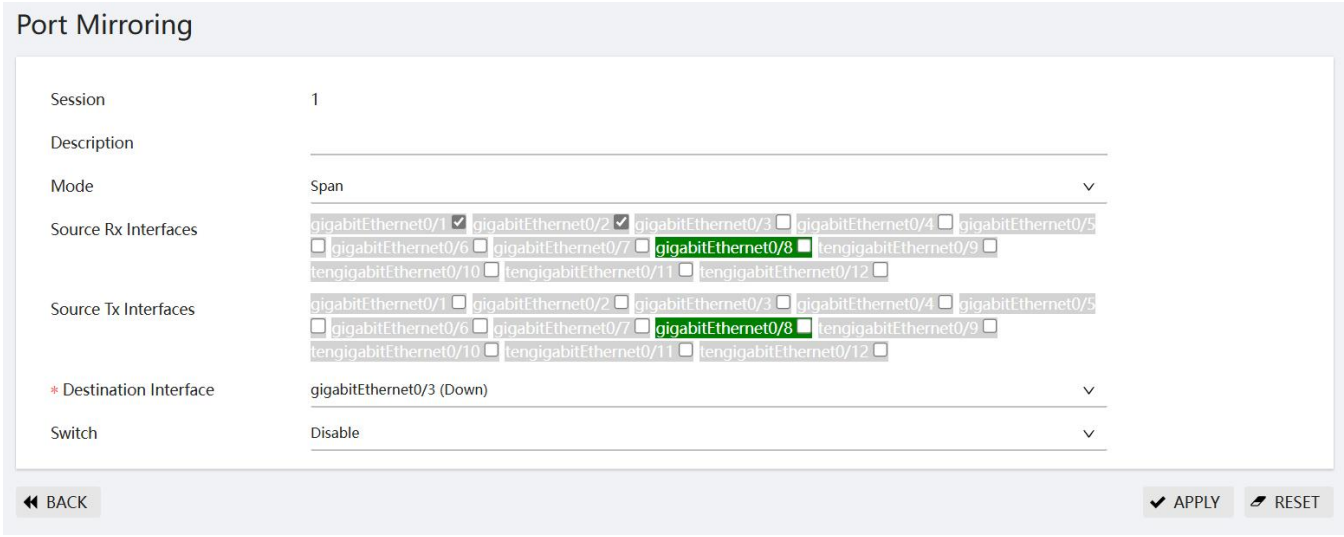
Step 1: Select [Interface] [Port Mirroring] in the navigation bar to enter the port mirroring configuration interface.

Step 2: Click the [Edit] button to enter the port mirror configuration interface.

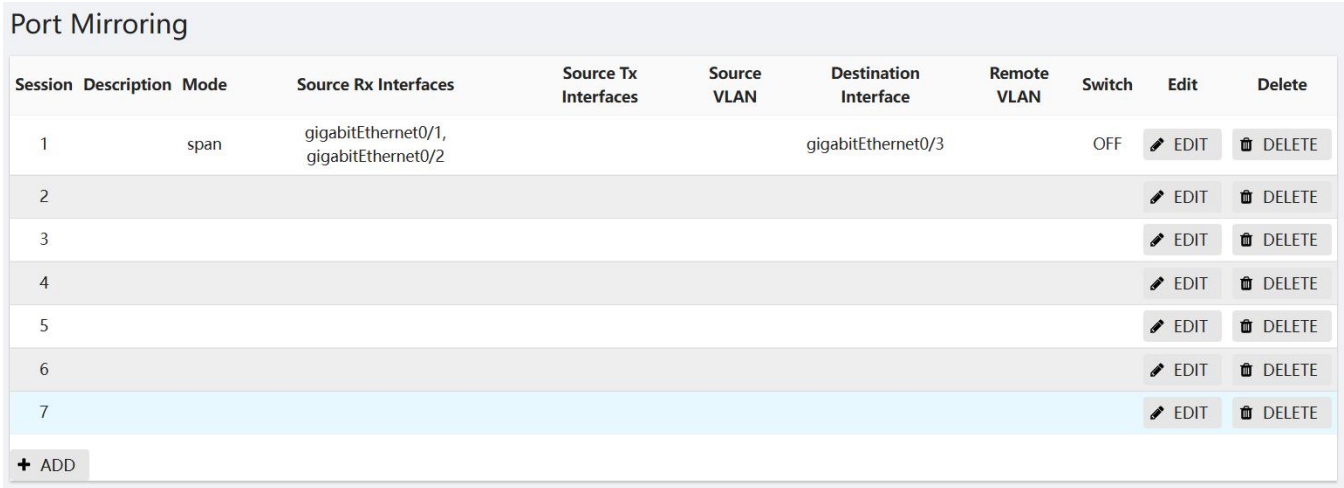
Step 3: As shown in Figure 3-18, select Session 1, select GigabitEthernet 0/3 in the destination interface, and select GigabitEthernet in the source interface.

0/1 and GigabitEthernet 0/2.

Figure 3-18 port mirror configuration interface



Step 4: Click the [Apply] button to complete the configuration and automatically return to the port mirroring interface. You can see the successfully created mirror group 1, as shown in Figure 3-19. Figure 3-19 Port mirror display



3.6 Port isolation

In order to achieve layer 2 isolation between packets, different ports can be added to different VLANs, but limited VLAN resources will be wasted. Using port isolation feature, isolation between ports within the same VLAN can be achieved. Users only need to add the port to the isolation group to achieve the isolation layer two data isolation between ports in the isolation group. The port isolation function provides users with a safer and more flexible networking solution. The port isolation feature has nothing to do with the VLAN to which the

port belongs. Devices that do not support uplink ports, the ports in the isolation group and the ports outside the isolation group have two-way interconnection.

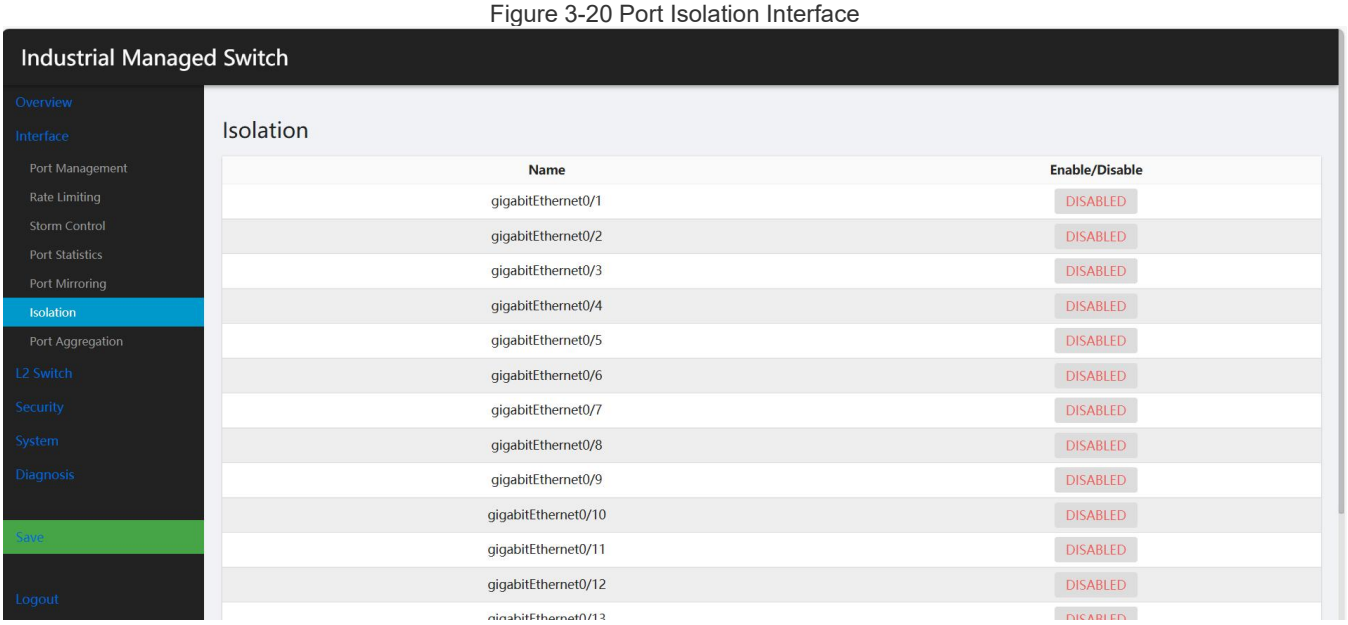
Configuration steps:

(1) Select [Interface] [Port Isolation] in the navigation bar to enter the port isolation interface, as shown in Figure 3-20.

(2) Click the [Enable/Disable] button to the right of "Port Isolation".

(3) Click the [Save] button of the navigation bar to save the configuration.

Figure 3-20 Port Isolation Interface

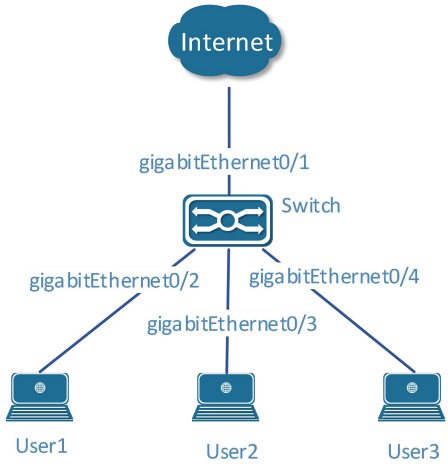


Configuration example:

The networking requirements are shown in Figure 3-21:

- The cell users User1, User2, and User3 are connected to the Switch ports GigabitEthernet 0/2, GigabitEthernet 0/3, and GigabitEthernet 0/4 respectively.
- The device is connected to the external network through the gigabitGigabitEthernet port 0/1.
- GigabitEthernet0/1, GigabitEthernet 0/2, GigabitEthernet 0/3, GigabitEthernet 0/4 belongs to the same VLAN; it realizes that the layer 2 packets between cell users User1, User2 and User3 cannot communicate with each other, but can communicate with external networks.

Figure 3-21 Network Topology



Step 1: Select [Configuration] [Port] in the navigation bar to enter the port isolation interface.

Step 2: Select GigabitEthernet 0/2, GigabitEthernet 0/3, and GigabitEthernet 0/4 in the port panel to complete the configuration, as shown in Figure 3-22.

Figure 3-22 Port isolation configuration interface

Isolation

Name	Enable/Disable
gigabitEthernet0/1	DISABLED
gigabitEthernet0/2	ENABLED
gigabitEthernet0/3	ENABLED
gigabitEthernet0/4	ENABLED
gigabitEthernet0/5	DISABLED
gigabitEthernet0/6	DISABLED

3.7 Aggregation port

3.7.1 Overview

Bundle multiple physical links together to create a logical link. We call this logical link aggregation port (port-channel, hereinafter referred to as
PO port). This feature complies with the IEEE802.3ad standard, it can be used to extend link bandwidth, provide higher connection reliability, and is commonly used in ports
Top link
The polymer port has the following characteristics:
(1) High bandwidth, the total bandwidth of the aggregation port is the sum of the bandwidth of the physical member port;
(2) Support traffic equalization strategy, and traffic can be allocated to each member link according to the strategy;
(3) Support link backup. When a member link in the aggregation port is disconnected, the system will automatically allocate the traffic of the member link to the aggregation port.
on other valid members links

Configuration steps:

(1) Select [Interface] [Port Aggregation] in the navigation bar, enter the port aggregation configuration interface, and select the load balancing algorithm in the global configuration interface, as shown in Figure 3-23, and the parameter description is shown in Table 3-24.

Figure 3-23 Aggregation configuration interface

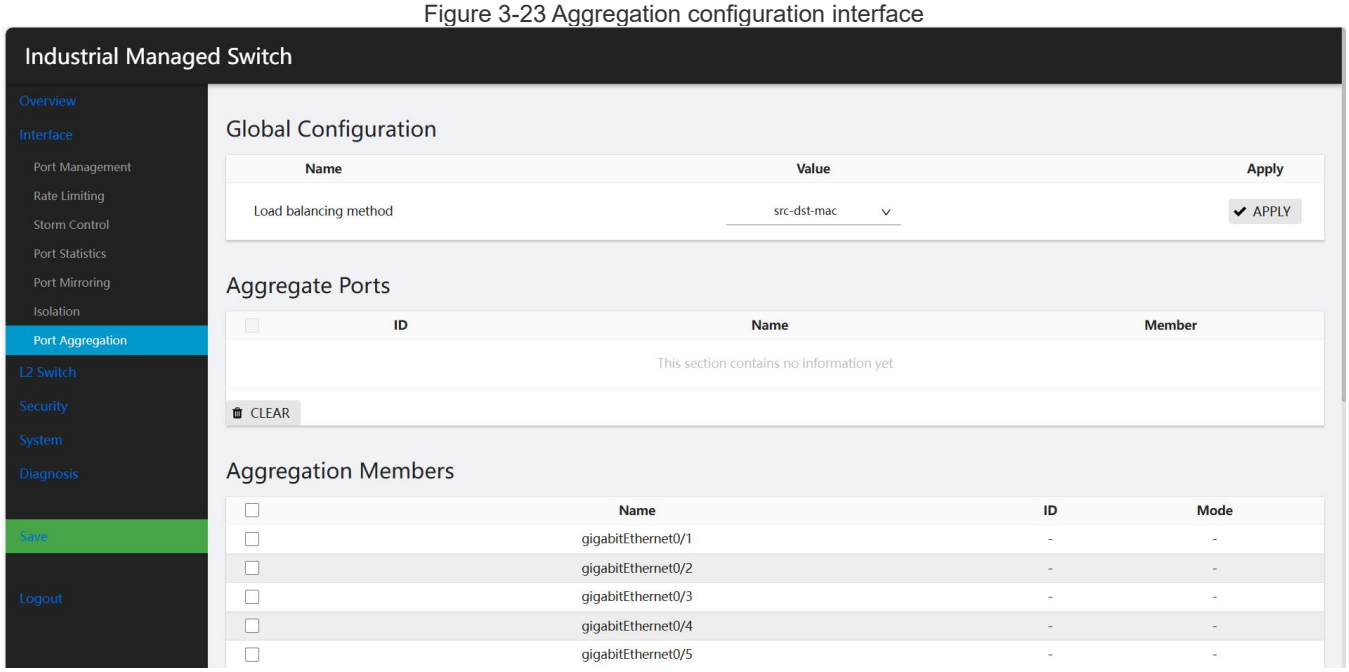


Table 3-24 Global Configuration Parameter Description

Configuration Items		illustrate	
Global configuration	balanced algorithm	dst-mac	Equalize according to the destination MAC address.
		src-mac	Equalize according to the source MAC address.
		src-dst-mac	Equalize according to the source MAC address and the destination MAC.
		dst-ip	Equalize according to the destination IP address.
		srt-ip	Equalize according to the source IP address.
		src-dst-ip	Equalize according to the source IP address and the destination IP address.
		dst-port	Equalize according to the L4 TCP/UDP destination port number.
		src-port	Equalize according to the L4 TCP/UDP source port number.
		src-dst-port	Equalize according to the L4 TCP/UDP source port number and destination port number.

(2) In the aggregation port member, configure the "ID" and "Mode" of the corresponding port, click [Application] to complete the configuration, as shown in Figure 3-25, parameter description Table 3-26 shows.

Figure 3-25 Aggregation port member configuration interface

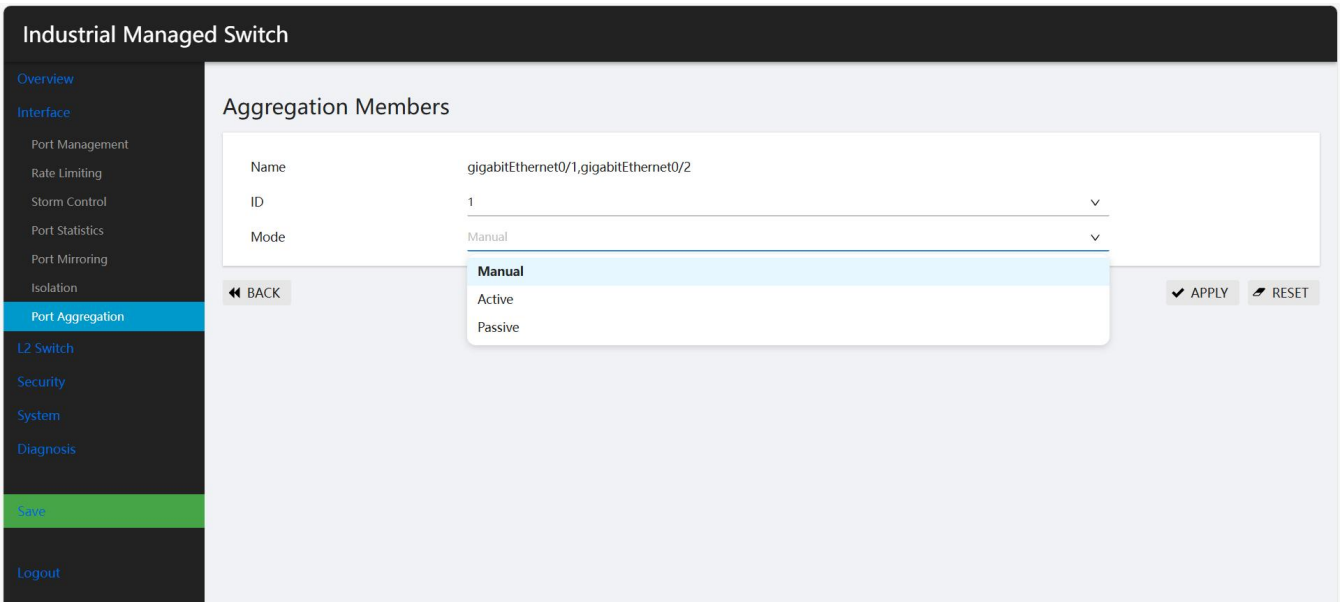


Table 3-26 Description of the configuration parameters of the aggregation member port

Configuration Items		illustrate	
Port configuration	ID	ID of the aggregation port member	
	type	Manual	Set to manual mode
		Active	This port will actively initiate LACP aggregation operation
		Passive	This port will not initiate LACP aggregation operation actively, but will passively participate in LACP calculation after receiving the neighbor's LACP message.

Click [OK] to complete the configuration. The aggregation port ID and member port information that were successfully created will be displayed in the aggregation port interface, as shown in Figure 3-27 and the parameter description table 3-28.

Figure 3-27 Aggregation port display interface

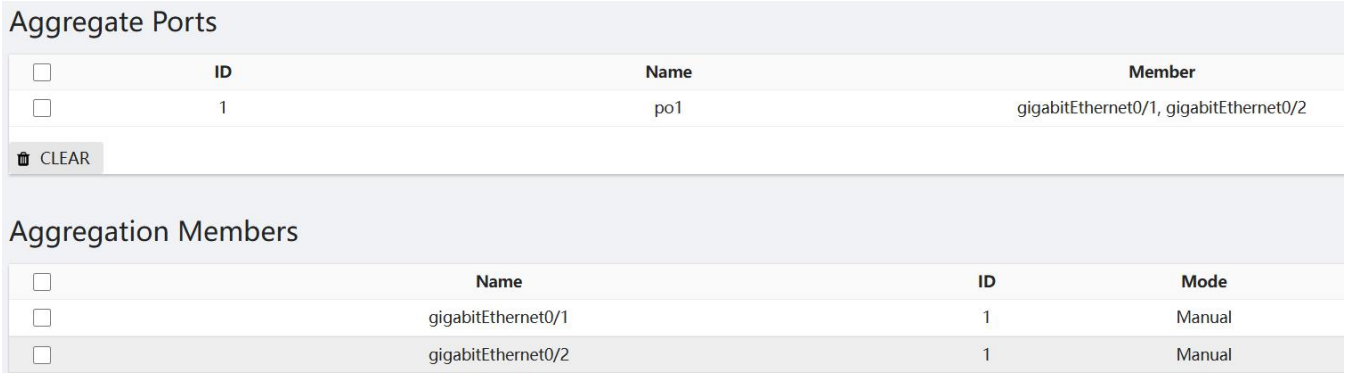


Table 3-28 Aggregation port parameter description

Configuration Items		illustrate
Aggregation port	ID	The ID of the aggregation port.
	name	Aggregation port name
	member	Specific aggregation port member name.

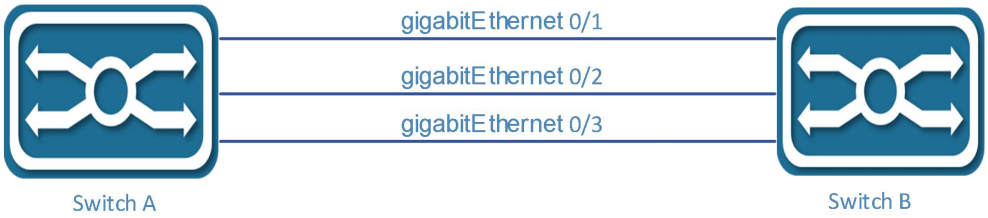
3.2.4.3 Configuration example

1. Networking requirements

• As shown in Figure 3-29, Switch A and Switch B are connected to each other through their respective layer two Ethernet ports GigabitEthernet 0/1~GigabitEthernet /0/3.

• Switch A and Switch B are connected by three physical links. Configure ports into port aggregation groups on Switch A and Switch B, so as to share out/income loads in each member port.

Figure 3-29 Example of port aggregation



2. Configuration steps

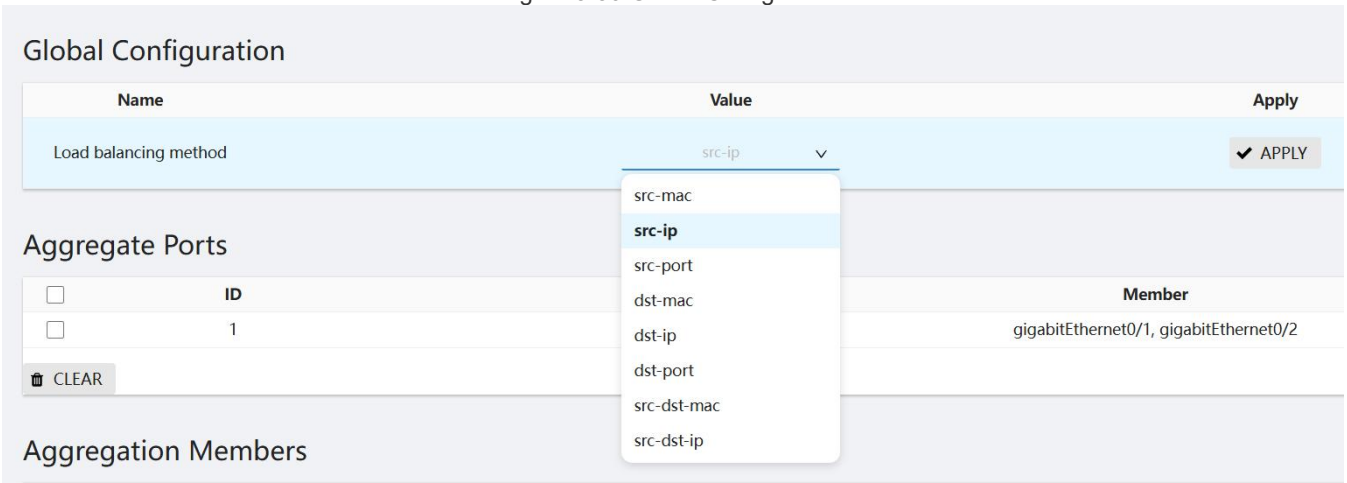
Load sharing can be achieved using both static aggregation ports and dynamic aggregation ports. The configuration methods of these two aggregation ports will be introduced separately below. The requirements can be achieved using either method.

Method 1: Configure the static aggregation port

Step 1: Select [Interface] and [Port Aggregation] in the navigation bar to enter the port aggregation configuration interface.

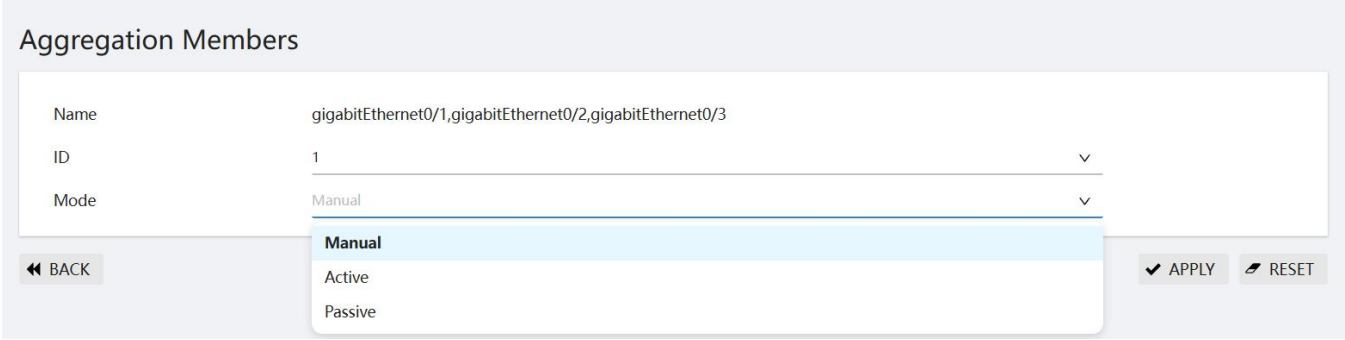
Step 2: In the global configuration item, select "Load Balancing Algorithm" as src-ip, as shown in Figure 3-30.

Figure 3-30 Global Configuration



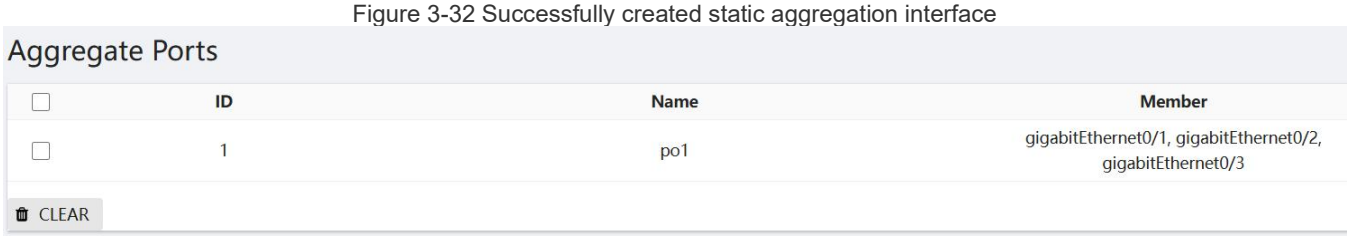
Step 3: Click the [Add] button below the "Aggregation Port", select GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3 in the port panel, set the ID to "1", and select "Manual" in the mode, as shown in Figure 3-31.

Figure 3-31 Static configuration of aggregation member port



Click Apply to complete the configuration. On the Aggregation Port interface, you can see the successfully created aggregation port po1, as shown in Figure 3-32.

Figure 3-32 Successfully created static aggregation interface

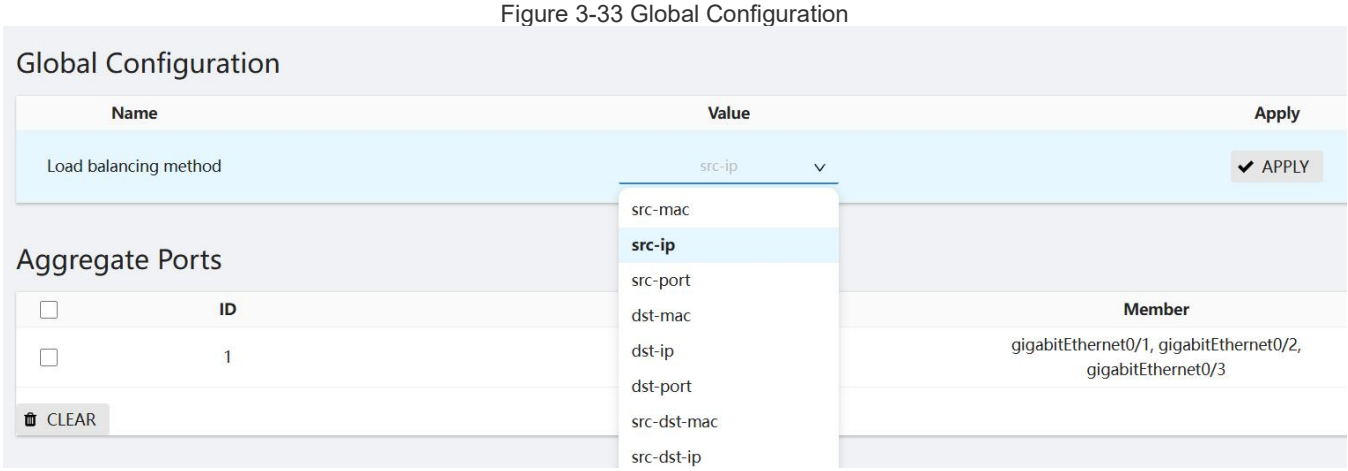


Method 2: Configuring Dynamic Aggregation Groups

Step 1: Select [Interface] [Port Aggregation] in the navigation bar to enter the port aggregation configuration interface.

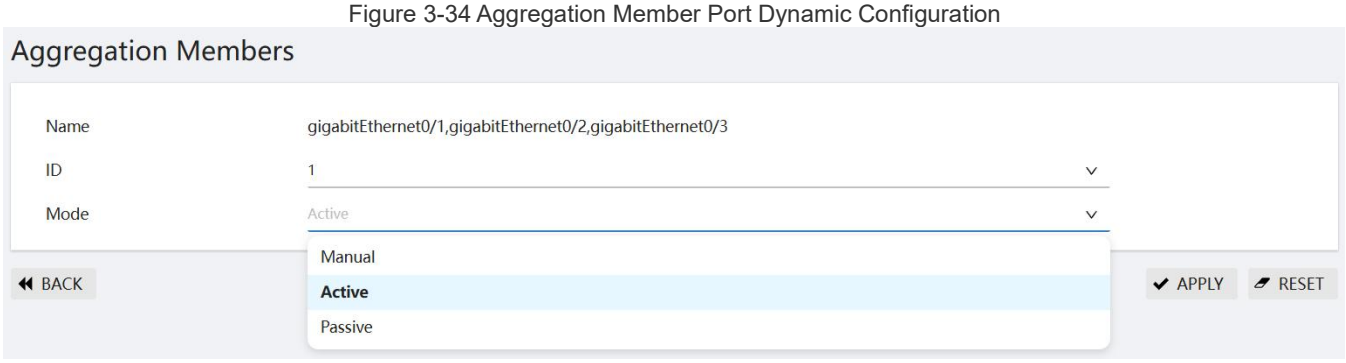
Step 2: In the global configuration item, select "Load balancing algorithm" as src-ip, as shown in Figure 3-33.

Figure 3-33 Global Configuration



Step 3: Click the [Add] button under "Aggregation Port", select GigabitEthernet 0/1, GigabitEthernet 0/2, GigabitEthernet 0/3 for the port panel, and set the ID to "1".", select "Active" mode, as shown in Figure 3-34.

Figure 3-34 Aggregation Member Port Dynamic Configuration



Click [OK] to complete the configuration, and in the Aggregation Port interface, you see the successfully created aggregation port po1, as shown in Figure 3-35.

Figure 3-35 Dynamic Aggregation Port Created Successfully

Step 4: Click the [Save] button on the navigation bar to save the current configuration.

4.1 VLAN

4.1.1 outlined

VLAN stands for Virtual Local Area Network, which is a logical network divided on a physical network.This network corresponds to the Layer 2 network of the ISO model.The division of a VLAN is not limited by the actual physical location of the network ports.A VLAN has the same attributes as a normal physical network, except that it has no physical location limitation, which makes it the same as a normal LAN.Layer 2 unicast, broadcast, and multicast frames are forwarded and propagated within a VLAN and not directly into other VLANs.

Port-based VLANs are the simplest method of VLAN segmentation.Users can divide the ports on the device into different VLANs, and then the messages received from a certain port will only be transmitted in the corresponding VLAN, thus realising the isolation of broadcast domains and the division of virtual workgroups.

4.1.1.1 Link Type

The link connection type of a port can be categorized into two types based on how the port handles VLAN Tag differently when forwarding messages:

Access :

The port sends out messages without VLAN Tag, which is generally used to connect with end devices that cannot recognize VLAN Tag, or when there is no need to distinguish between different VLAN members.

Trunk:

Port outgoing messages, port default VLAN messages without Tag, other VLAN messages must be with Tag, usually used for interconnection between network transmission equipment.

Hybrid :

The messages sent out from the port can be set according to the needs of certain VLANs with Tag and certain VLANs without Tag. Hybrid type ports can be used for interconnecting network transmission devices as well as directly connecting terminal devices.

4.1.1.2 Default VLAN (PVID)

In addition to setting the VLANs that a port is allowed to pass through, you can also set the default VLAN of the port. by default, the default VLAN of all ports is VLAN 1, but users can configure it according to their needs.

- The default VLAN of an Access port is the VLAN to which it belongs.

- Trunk ports and Hybrid ports can allow multiple VLANs to pass through. able to configure the default VLAN.

- When a VLAN is deleted, if the VLAN is the default VLAN of a certain port, the default VLAN of the port will be restored to VLAN 1 for Access ports; for Trunk ports or Hybrid ports, the default VLAN configuration of the ports will not be changed, i.e., they can use the VLAN that no longer exists as the default VLAN.VLAN.

clarifica

- It is recommended that the default VLAN of the local device port and the default VLAN of the connected peer device port be consistent.
- It is recommended to ensure that the default VLAN of the port is the VLAN that is allowed to pass through the port.

  If the port does not allow a VLAN to pass, but the default VLAN of the port is that VLAN, the port discards the received packets of that VLAN or packets without VLAN Tag.
- Hybrid ports are not supported by WebManager. If you need this feature, please use the CLI configuration method.

4.1.1.3 How the port handles the message

After configuring the port connection type and default VLAN, there are several different scenarios for the port's handling of incoming and outgoing messages, as shown in Table 4-1.

Table 4-1 Processing of Port Sending and Receiving Messages

Port Type	Processing of incoming messages		Processing of sent messages
	When the received message does not have a tag	When the received message has a Tag	
Access	Adding a default VLAN to the message's Tag	• -Receive the message when the VLAN is the same as the default VLAN • Discard the message when the VLAN is different from the default VLAN	Remove the Tag and send the message

Trunk	• -When the default VLAN is in the list of VLANs allowed to pass through the port, it receives the message and adds the Tag of the default VLAN to the message. • table, receive the message and add the Tag of the default VLAN to the message. • When the default VLAN is not in the list of VLANs allowed to pass through the port, discard the message.	• -Receive the packet when the VLAN is in the list of VLANs that the port is allowed to pass through • Discard the message when the VLAN is not in the list of VLANs that the port is allowed to pass through	• -When the VLAN is the same as the default VLAN and is in the list of VLANs that the port is allowed to pass through, remove the Tag and send the message • When the VLAN is different from the default VLAN and is in the list of VLANs that the port is allowed to pass through, keep the original Tag and send the message.
Hybrid			Send the message when the VLAN is in the list of VLANs allowed to pass through the port, whether to remove the Tag can be manually configured by the user

4.1.2 deployed VLAN

4.1.2.1 VLAN Configuration

Configuring Access Port-Based VLAN

Table 4-2 Access port-based VLAN configuration steps

move	Configuration tasks	clarification
1	Configure the connection type of the port	selectable Configure the connection type of the port as Access , by default, the connection type of the port is Access
2	Creating VLANs	Required Create one or more VLANs
3	Configure the default VLAN for the port	Configuring the Default VLAN for Access Ports

Configuring Trunk Port-Based VLANs

Table 4-3 Trunk port-based VLAN configuration steps

move	Configuration tasks	clarification	
1	Configure the connection type of the port	Required Configure the connection type of the port as Trunk By default, the connection type of the port is Access	By default, the Trunk port's Untagged VLAN (i.e., the default VLAN) is VLAN 1 When you change a Trunk port's Untagged VLAN (i.e., its default VLAN), the port's original Untagged VLAN will automatically change to its Tagged VLAN.
2	Create the VLANs that need to be added to this Trunk port	Required Create one or more VLANs	
3	Configure the Trunk to which the VLAN belongs	Select the corresponding Trunk port and add the VLAN to the	compulsory The Trunk port has only one Untagged VLAN, its default VLAN。

4.1.2.2 Configuring Ports in a VLAN

VLAN The configuration interface is shown in Figure 4-4, and the detailed description of each parameter is shown in Table 4-5.

Figure 4-4 VLAN placement interface

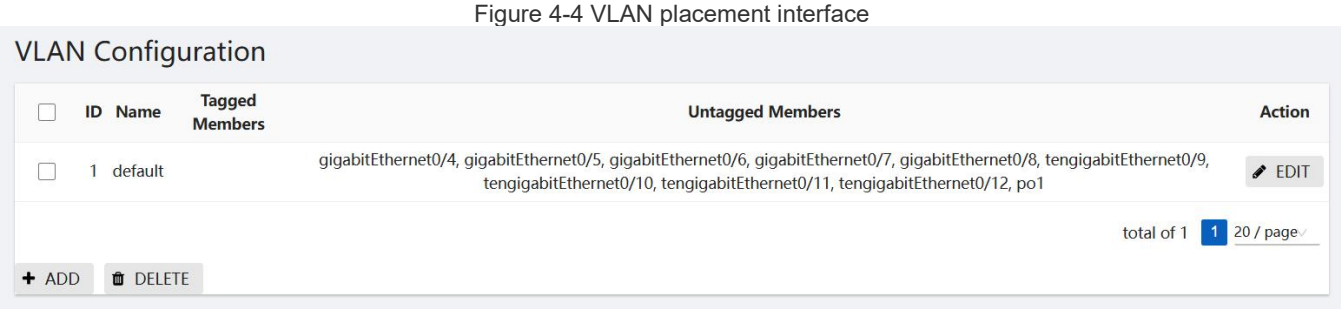


Table 4-5 Description of VLAN configuration-related parameters

configuration item	clarification
ID	VLANserial number
name	VLAN name, configuration is not supported. default VLAN 1 is default and VLAN 2 is VLAN0002.
typology	Static\Dynamic, current version only supports Static
Tagged member port	Port Tagged Member List
Untagged member port	Port Untagged Member List
compiler	Select the VLAN ID to be edited and click this button to enter the editing interface.
increase	Click this button to enter the VLAN Add screen.
removing	Select the VLAN ID to be edited and click this button to delete the VLAN.

Configuration steps:

(1) Select [Switching] [VLAN] in the navigation bar to enter the VLAN configuration interface, as shown in Figure 4-6.

(2) Click the [Add] button to enter the page shown in Figure 4-7.

(3) In the ID box, enter the VLAN to be created.

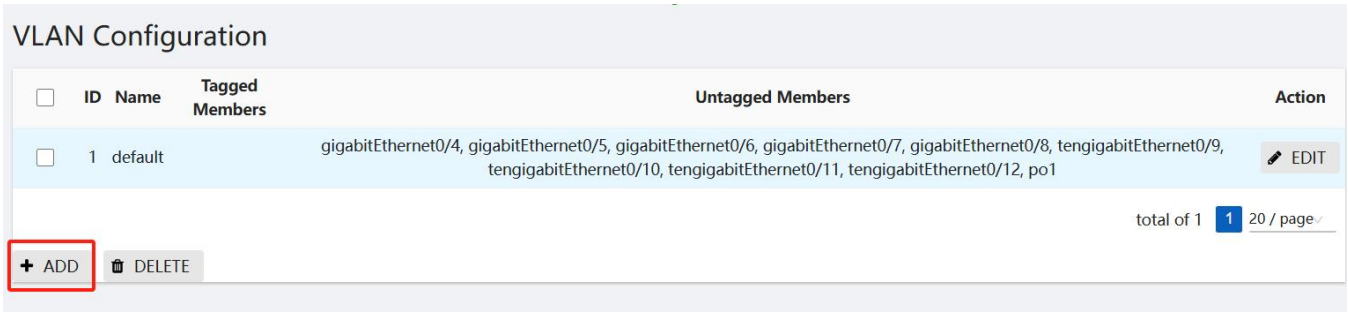
(4) Enter the VLAN name and click the [Confirm] button to complete the operation.

(5) Click the [Save] button on the navigation bar to save the configuration.

(6) When you need to configure VLAN port members, click the [Edit] button, select the port members that need to be added to this VLAN in the port panel, and click the [Apply] button to complete the operation.

(7) When multiple VLANs need to be created at the same time, you can use the "n-m" method, such as "2-10".When the number of VLANs to be created at one time is greater than 100, use the CLI command line to configure.

Figure 4-6 Port Configuration Interface



端 The port configuration interface is shown in Figure 4-7, and the detailed description of each parameter is shown in Table 4-8.

Figure 4-7 Creating a VLAN

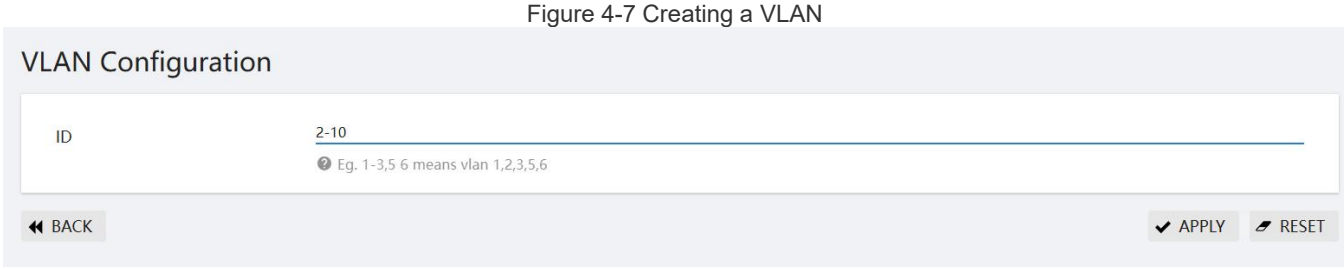


Table 4-8 Description of Interface Configuration Related Parameters

configuration item		clarification
paradigm	Access	Configure the port type as an Access port
	Trunk	Configure the port type as a Trunk port
PVID/Native VLAN		Configure the PORT-BASE VLAN ID of the Access port or the Native VLAN of the Trunk port
Allow VLANs		Select port VLAN for Trunk ports

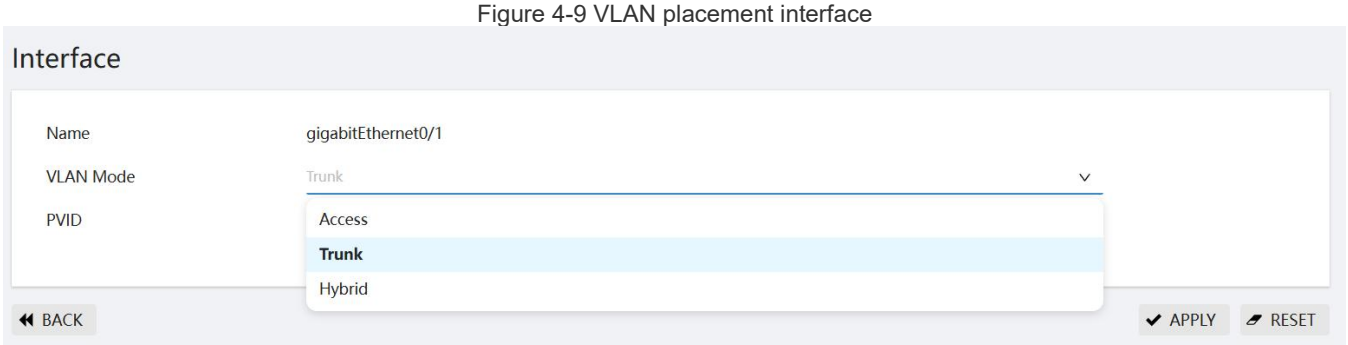
Configuration steps:

(1) Select [Switching] [VLAN] in the navigation bar to enter the interface configuration interface, as shown in Figure 4-9.

(2) Click the [Bulk Edit] button below the Trunk port configuration to enter the interface configuration page.

(3) Configure the VLAN mode of the port, as well as the PVID or Native Vlan. In general, it is recommended that the Native VLAN of the Trunk port be configured as "1" and the Allow VLANs as "all".The configuration interface is shown in Figure 4-9, click the [Apply] button to complete the configuration.

Figure 4-9 VLAN placement interface



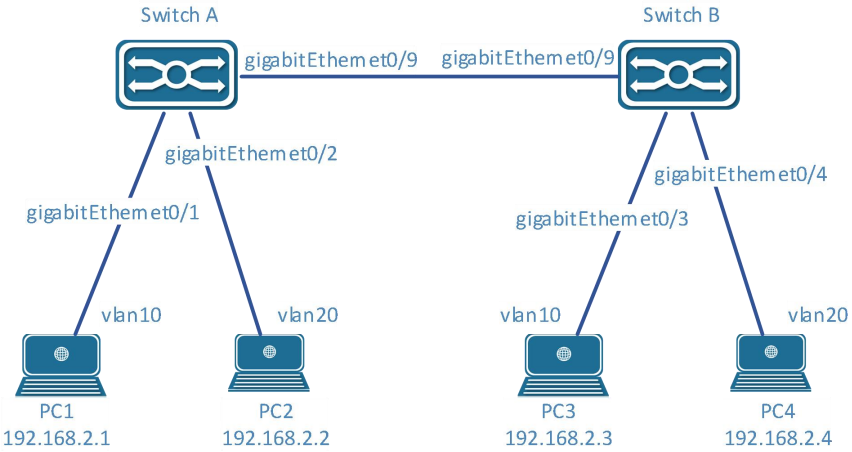
（4) Click the [Apply] button in the lower right corner to save the configuration.

4.1.2.4 VLAN Configuration Example

Configuration Example:

Case Requirements:Switch A and Switch B are interconnected through trunk ports. PCs in the same VLAN can access each other and PCs in different VLANs are prohibited from accessing each other. the network topology is shown in Figure 4-10;

Figure 4-10 Network Topology Diagram



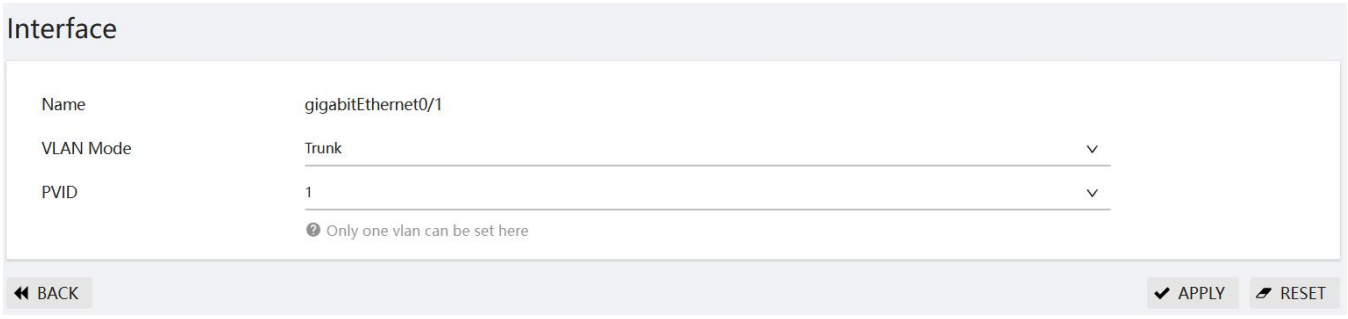
Switch A configuration:

Step 1: Configure GigabitEthernet 0/9 as a Trunk port, and the Native Vlan is 1 by default.

Select [VLAN] in the navigation bar [Switching] to enter the interface configuration interface. Select port GigabitEthernet 0/9 and click the [Edit] button.

Enter the configuration mode, as shown in Figure 4-11, select Trunk for VLAN mode, and Native Vlan is 1 by default.

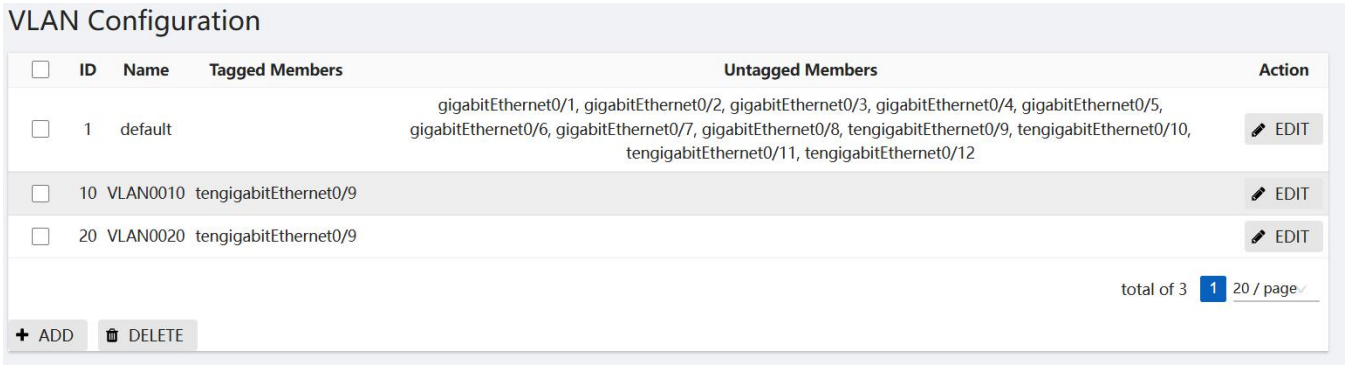
Figure 4-11 Interface Configuration Interface



Step 2: Create VLAN 10 and VLAN 20, and add VLAN 10 and VLAN 20 to the Trunk port GigabitEthernet 0/9. Under the VLAN interface, click the [Add] button to enter the VLAN editing interface, as shown in Figure 4-12, and enter "10,20" in the dialog box.

Port GigabitEthernet 0/9 is set as Trunk default to release all configured VLANs, click [Apply] button to complete the configuration.

Figure 4-12 Add VLAN Interface

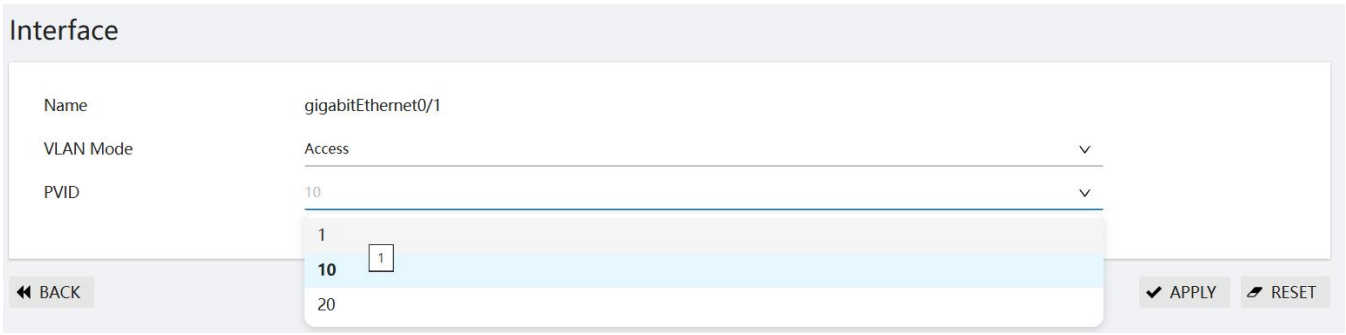


Step 3: Configure port GigabitEthernet 0/1 VLAN mode as Access and PVID as 10.

In the interface interface, select GigabitEthernet 0/1 and click the [Edit] button to enter the interface configuration interface, as shown in Figure 4-13.

The VLAN mode is Access by default and the PVID is 10. click the [Apply] button to complete the configuration.

Figure 4-13 Port VLAN Configuration Interface

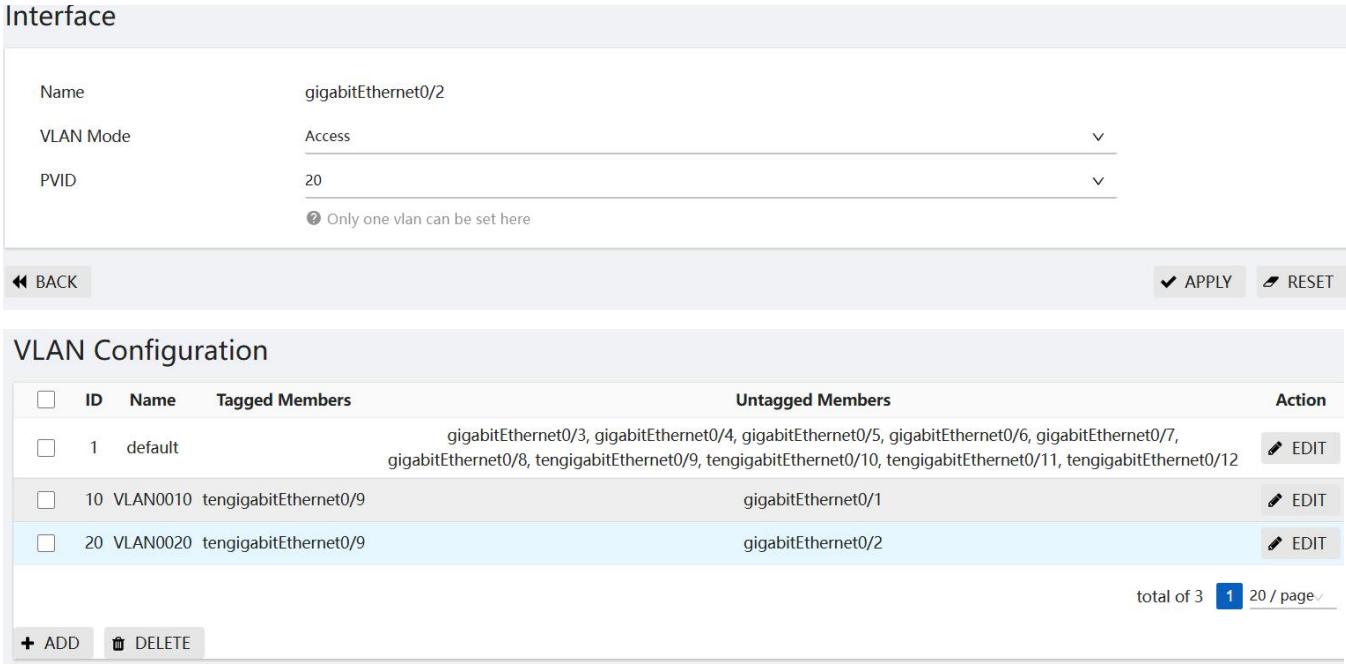


Step 4: Configure the VLAN mode of port GigabitEthernet 0/2 as Access and PVID as 20.

Same as step 3, set the VLAN mode of GigabitEthernet 0/2 to Access and the PVID to 20. click [Apply] to complete the configuration.

After clicking [Apply] to complete the configuration, the VLAN interface is shown in Figure 4-14.

Figure 4-14 Successfully Created VLAN Interface



Step 5: Click the [Save] button on the navigation bar to save the configuration.

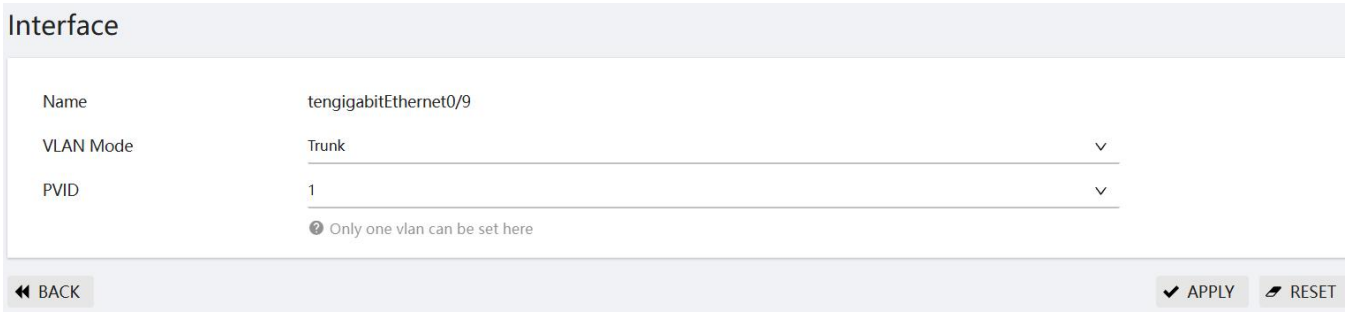
Switch B configuration:

Step 1: Configure GigabitEthernet 0/9 as a Trunk port and Native Vlan as default value 1.

Select [VLAN] in the navigation bar [Switching] to enter the interface configuration interface. Select port GigabitEthernet 0/9 and click the [Edit] button.

Enter the configuration mode, as shown in Figure 4-15, select Trunk as VLAN mode, and Native Vlan is 1 by default.

Figure 4-15 Interface Configuration Interface

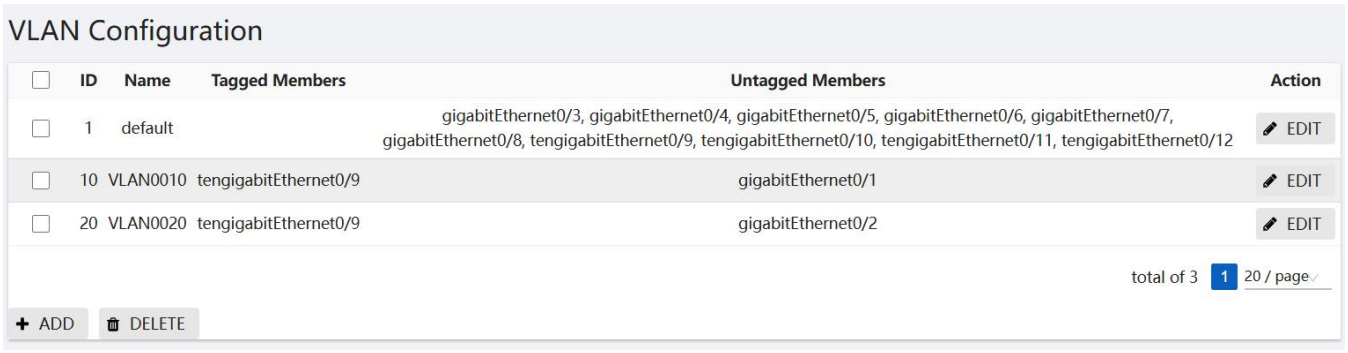


Step 2: Create VLAN 10 and VLAN 20, and add VLAN 10 and VLAN 20 to the Trunk port GigabitEthernet 0/9.

Under the VLAN interface, click the [Add] button to enter the VLAN editing interface, as shown in Figure 4-16, and enter "10,20" in the dialog box.

Enter "10,20" in the dialog box to set port GigabitEthernet 0/9 as the default Trunk to release all configured VLANs, and click the [Apply] button to complete the configuration.

Figure 4-16 Add VLAN Interface

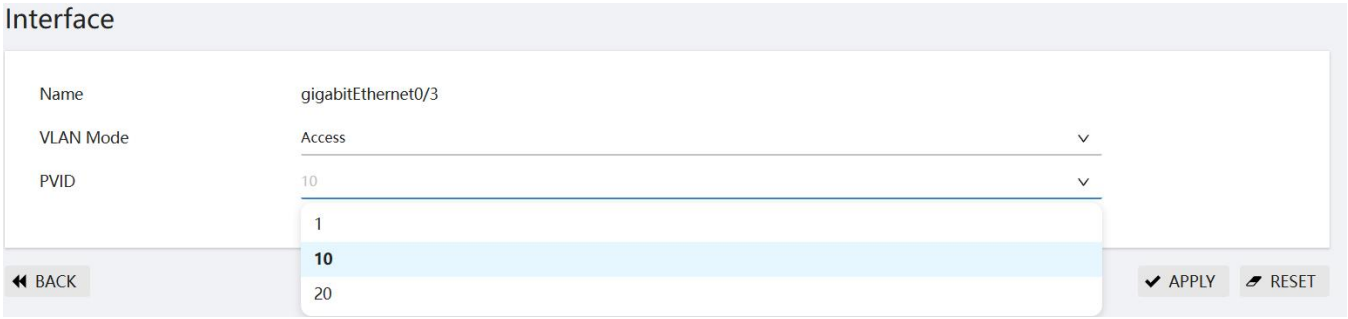


Step 3: Configure port GigabitEthernet 0/3 VLAN mode as Access and PVID as 10.

In the interface interface, select GigabitEthernet 0/3 and click the [Edit] button to enter the interface configuration interface, as shown in Figure 4-17.

The VLAN mode is Access by default and the PVID is 10. Click the [Apply] button to complete the configuration.

Figure 4-17 Port VLAN Configuration Interface

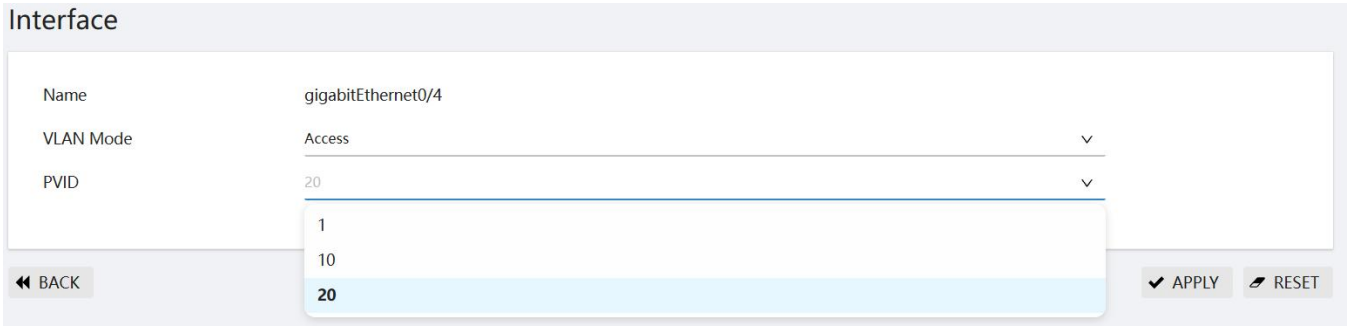


Step 4: Configure the VLAN mode of port GigabitEthernet 0/4 as Access and PVID as 20.

Same as step 3, set the VLAN mode of GigabitEthernet 0/4 to Access and the PVID to 20. click [Apply] to complete the configuration.

The VLAN interface is shown in Figure 4-18.

Figure 4-18 Successfully Created VLAN Interface



Step 5: Click the [Save] button on the navigation bar to save the configuration.

4.2 QinQ

4.2.1 summarize

QinQ is short for 802.1Q in 802.1Q, which is a Layer 2 tunneling protocol based on the IEEE 802.1Q technology. By encapsulating the user's private network message with an outer VLAN Tag, it enables it to traverse the carrier's backbone network (also known as the public network) carrying a two-layer VLAN Tag, thus providing a relatively simple Layer 2 VPN tunneling technology for the user, and making it possible for theThis provides a relatively simple Layer 2 VPN tunneling technology for users, and also makes it possible for carriers to utilize one VLAN to provide services for subscriber networks that contain multiple VLANs.

Background and Advantages of QinQ

In the VLAN Tag field defined by IEEE 802.1Q, only 12 bits are used to represent VLAN IDs, and a maximum of 4094 VLANs can be represented; however, in practice, especially in metropolitan area networks (MANs), where a large number of VLANs are needed to segregate subscribers, 4094 VLANs are not enough to satisfy the demand.4094 VLANs, thus meeting the demand for the number of VLANs in MANs.It has the following advantages:

Relieves the problem of increasingly scarce VLAN ID resources in the public network.

Users can plan their own private network VLAN IDs, which will not lead to conflicts with public network VLAN IDs.

Provides a simple and flexible Layer 2 VPN solution for small metro and enterprise networks.

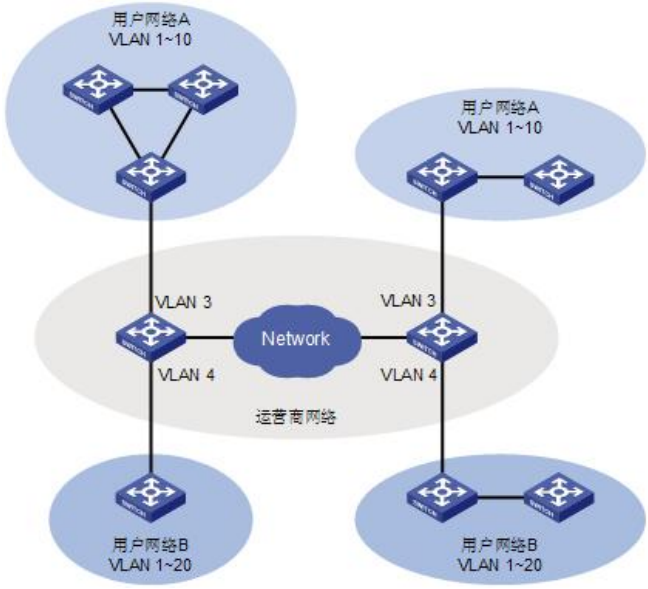
When the operator upgrades the network, the subscriber network does not have to change the original configuration, which makes the subscriber network more independent.

Principle of QinQ realization

During transmission in the public network, the device forwards the message only according to the outer VLAN Tag and learns the source MAC address table entry of the message into the MAC address table of the VLAN in which the outer VLAN Tag is located, while the user's private VLAN Tag will be transmitted as the data part of the message.

As shown in Figure 4-19, the private VLANs of subscriber networks A and B are VLANs 1 to 10 and VLANs 1 to 20, respectively, and the VLANs assigned by the operator to subscriber networks A and B are VLANs 3 and 4, respectively, and the VLANs of subscriber networks A and B are VLANs 3 and 4, respectively. When the messages with VLAN tags in subscriber networks A and B enter the operator's network, the outer part of the message is encapsulated with the VLANs of VLANs 3 and 4, respectively.In this way, messages from different subscriber networks are completely separated when they are transmitted in the carrier network, and even if the VLAN ranges of these subscriber networks overlap, there is no conflict when they are transmitted in the carrier network.

Figure 4-19 QinQ Typical Application Networking Diagram



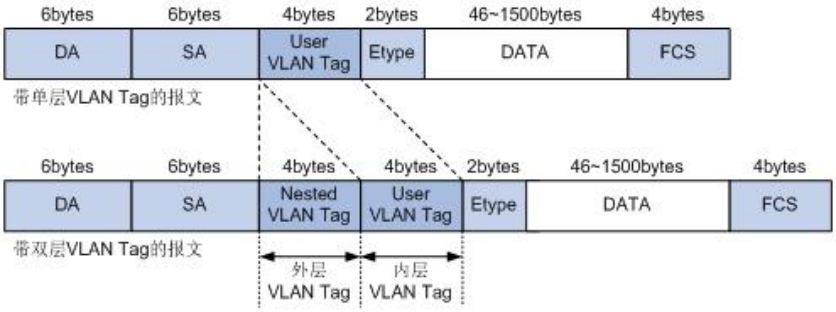
QinQ Message Structure

As shown in Figure 4-20, QinQ messages are transmitted in the carrier network with a two-layer VLAN Tag:

Inner VLAN Tag: is the user's private VLAN Tag;

Outer VLAN Tag: the public VLAN Tag assigned to the subscriber by the operator.

Figure 4-20 QinQ Message Structure



QinQ implementation

The implementation of QinQ can be categorized into the following two ways:

1. Basic QinQ

Basic QinQ is implemented based on the port method.When the basic QinQ function is configured on a port, the device tags the message with the default VLAN of this port regardless of whether the message received from the port is with a VLAN Tag or not:

If a message is received with a VLAN Tag, the message becomes a message with a double Tag;

If a message is received without a VLAN Tag, the message becomes a message with the default VLAN Tag of this port.

2. Flexible QinQ

Flexible QinQ is realized based on the combination of ports and VLANs, which extends the function of QinQ and is a more flexible implementation of QinQ.In addition to realizing all the functions of basic QinQ, Flexible QinQ can perform different operations based on VLANs for messages received from the same port, including:

Adding different outer VLAN Tag to messages with different inner VLAN IDs.

Tag the 802.1p priority of the outer VLAN based on the 802.1p priority of the inner VLAN of the message.

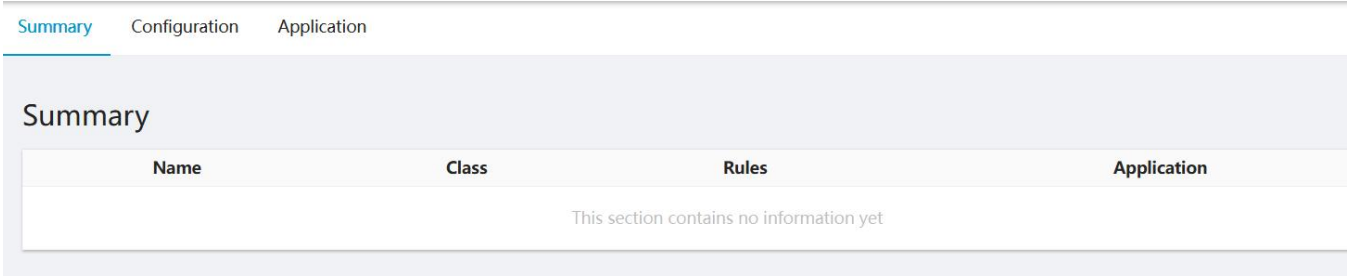
By using the flexible QinQ technology, it can isolate the carrier network and the subscriber network and at the same time provide rich service characteristics and more flexible networking capabilities.

4.2.2 QinQ Layout

VPN Deployment

Select [Switching] [QinQ Configuration] in the navigation bar to enter the QinQ Configuration Overview interface, as shown in Figure 4-21。

Figure 4-21 Configuration Overview



Click the [Add] button under "QinQ Configuration" to enter the interface for creating QinQ rules, as shown in Figure 4-22, and the description of each parameter is shown in Table 4-23.

Figure 4-22 VPN Creation Screen

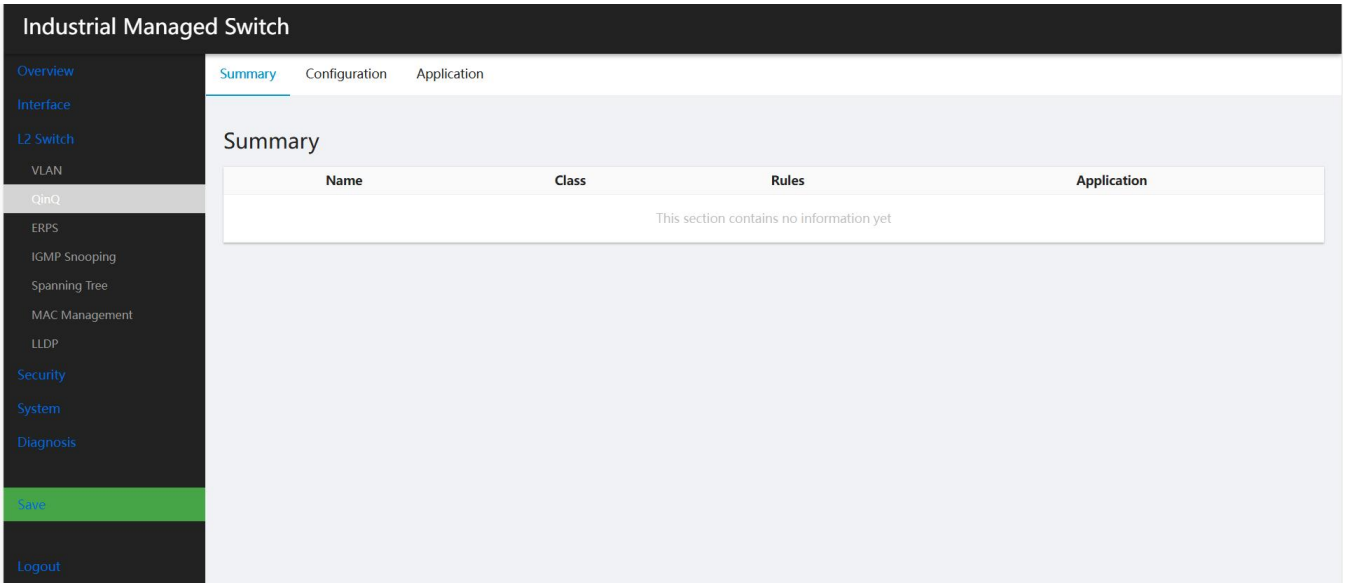


Table 4-23 Description of VPN Configuration Parameters

configuration item	clarification
name	QinQ Rule Name
CVID	Client VLAN ID
SVID	Server VLAN ID

Port Configuration

In the current interface, click the [Edit] button of the corresponding port or click the [Batch Edit] button above the "Port Configuration" to enter the port configuration interface, as shown in Figure 4-24, and the description of each parameter is shown in Table 4-25.

Figure 4-24 Port Configuration Interface

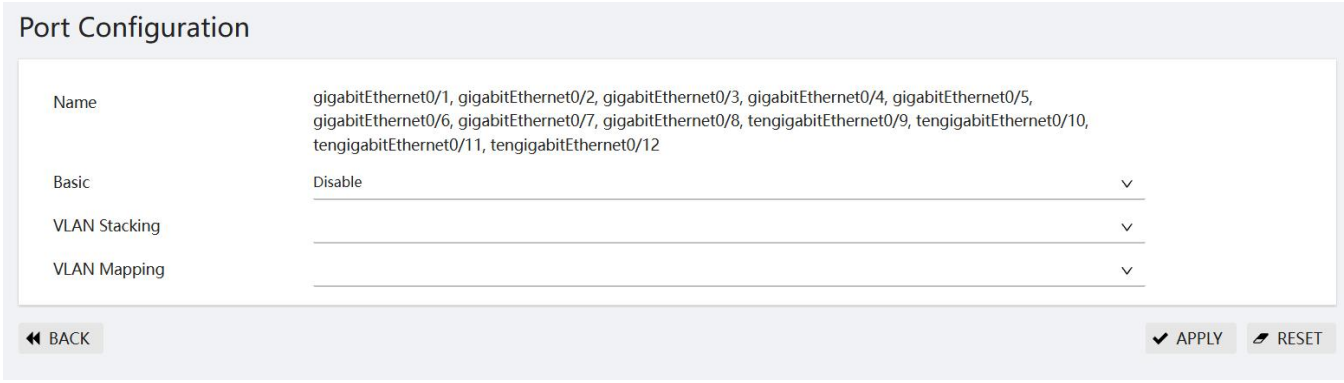


Table 4-25 Description of Port Configuration Parameters

configuration item	clarification
name	interface name
Basic	Basic QinQ rule application status
VLAN Stacking	Multilayer QinQ rule application state
VLAN Mapping	Replacement QinQ Rule Application Status

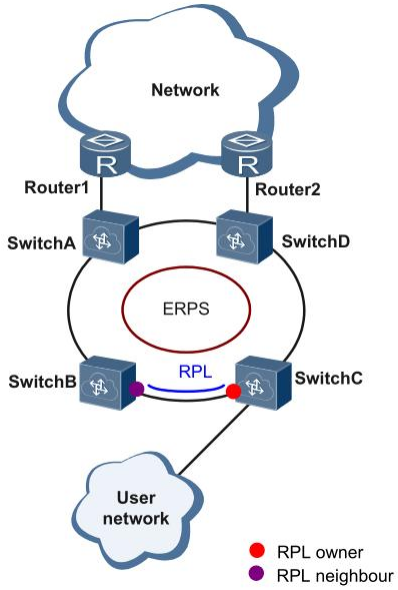
4.3 ERPS

4.3.1 ERPS Functional overview

ERPS（GigabitEthernet ernet Ring Protection Switching，The Ethernet Ring Protection Switching Protocol (ERPSP) is a ring protection protocol developed by the ITU, also known as G.8032, which is a link-layer protocol specialized for Ethernet ring networks.It prevents broadcast storms caused by data loops when the Ethernet ring is intact, and quickly restores communication between nodes on the ring when a link on the Ethernet ring is broken, as shown in Figure 4-26.

Currently, there are other technologies to solve the loop problem in Layer 2 networks, such as STP, which is more mature in application but has a longer convergence time (in seconds.) ERPS is a link-layer protocol that is specifically applied to Ethernet ring networks, and its Layer 2 convergence performance reaches less than 50 ms, which is faster than that of STP.

Figure 4-26 ERPS Typical Networking



4.3.2 Introduction to the ERPS Principle

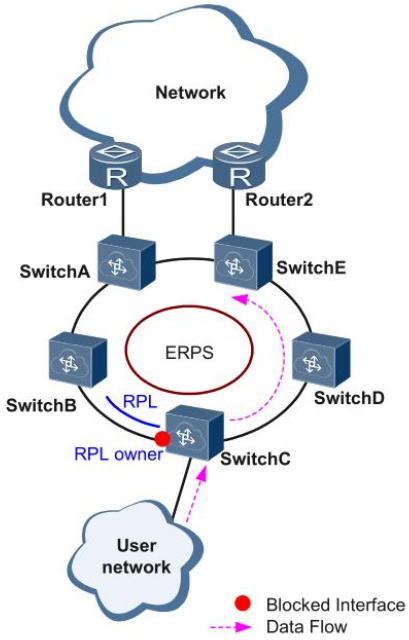
ERPS is a standard ring network protocol dedicated to the Ethernet link layer, with the ERPS ring as the basic unit.Only two ports on each Layer 2 switching device can join the same ERPS ring.In an ERPS ring, in order to prevent a loop from occurring, you can activate the loop-breaking mechanism to block the RPL owner port and eliminate the loop.When a link failure occurs in the ring, the device running the ERPS protocol can quickly release the blocking port, perform a link protection inversion, and restore link communication between nodes on the ring.This section introduces the implementation principle of ERPS in a basic single-ring network in the form of an

example according to the process of link normal->link failure->link recovery (including protection inversion operation).

4.3.2.1 The link is working.

As shown in Figure 4-27, the devices on the loop consisting of Switch A to Switch E communicate normally.

Figure 4-27 ERPS link is normal

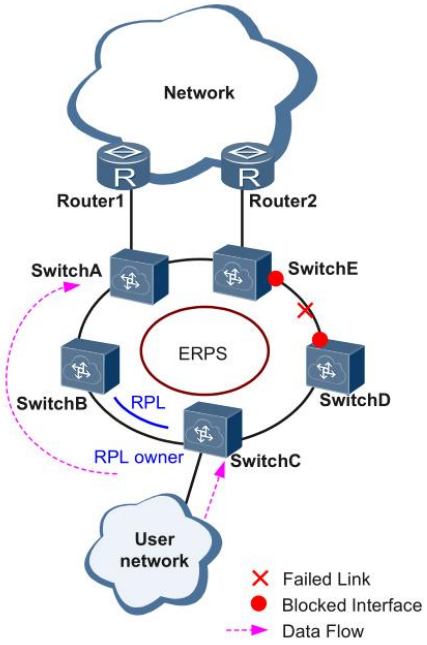


To prevent loops from being generated, ERPS first blocks the RPL owner port. If an RPL neighbor port is configured, the port is also blocked and other ports can forward service traffic normally.

4.3.2.2 link failure

As shown in Figure 4-28, when the link between Switch D and Switch E fails, the ERPS protocol activates the protection inversion mechanism, which blocks the ports at both ends of the failed link and then releases the RPL owner port, and these two ports resume receiving and transmitting user traffic again, thus ensuring that the traffic is not interrupted.

Figure 4-28 ERPS Link Failure



4.3.2.3 Link Recovery

After the link is restored to normal. by default. the ERPS ring is configured in cutback mode. the device on which the RPL owner port is located re-blocks traffic on the RPL link. the original faulty link is reused to complete the delivery of user traffic.

4.3.2.4 ERPS Ring Types

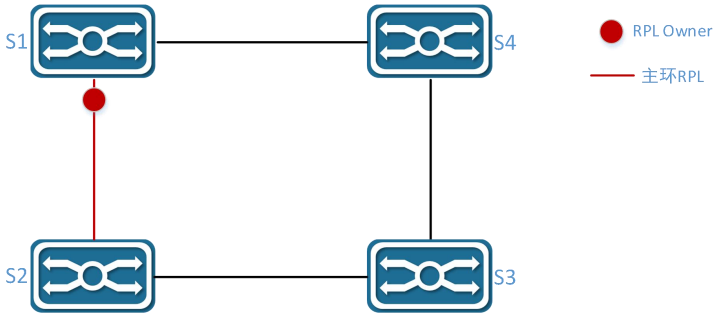
Single ring:

Take Figure 4-29 as an example, there is only one ring in the network topology; there is one RPL Owner; there is one RPL link; all nodes need to have the same RAPS management VLANs

All devices in the ring network need to support the ERPS function.

The links between the devices in the ring network must be directly connected, and there can be no intermediate devices.

Figure 4-29 ERPS single-loop model



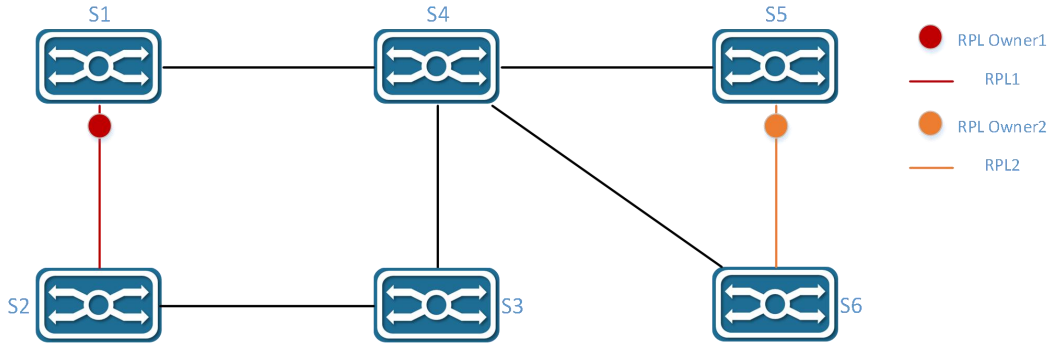
相切环:

Application scenarios in which two or more rings in a network topology share a single device that needs to be protected.Take Figure 4-30 as an example, two rings in the network topology share one device; each ring has one and only one blocking point, and each ring has one and only one RPL link; different rings need to have different RAPS management VLANs.

All devices in the ring network need to support the ERPS function.

The links between devices in the ring network must be directly connected, with no intermediate devices.

Figure 4-30 ERPS tangent ring modeling



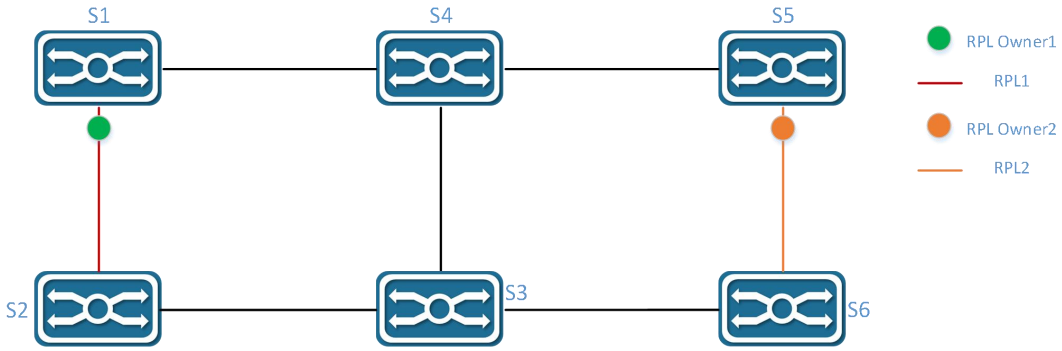
Intersecting rings:

There are two or more rings in the network topology sharing a common link (the two intersecting nodes must be directly connected to each other, and there can be no other nodes).Take Figure 4-31 as an example, there are 2 rings in the network topology; each ring has one and only one RPL owner node, and each ring has one and only one RPL link; different rings need to have different RAPS management Alan.

All devices in the ring network need to support ERPS function.

The links between the devices in the ring network must be directly connected, no intermediate devices.

Figure 4-31 ERPS intersecting ring model



4.3.3 Introduction to ERPS Configuration

attention (heed)

c-The Spanning Tree Protocol and the ERPS protocol cannot be turned on at the same time.

4.3.3.1 ERPS ring configuration

Click the navigation bar to select [Switching] [ERPS] [Configuration] to enter the ERPS ring configuration interface, as shown in Figure 4-32, and the specific description of parameter information is shown in Table 4-33.

Figure 4-32 ERPS Ring Configuration Screen

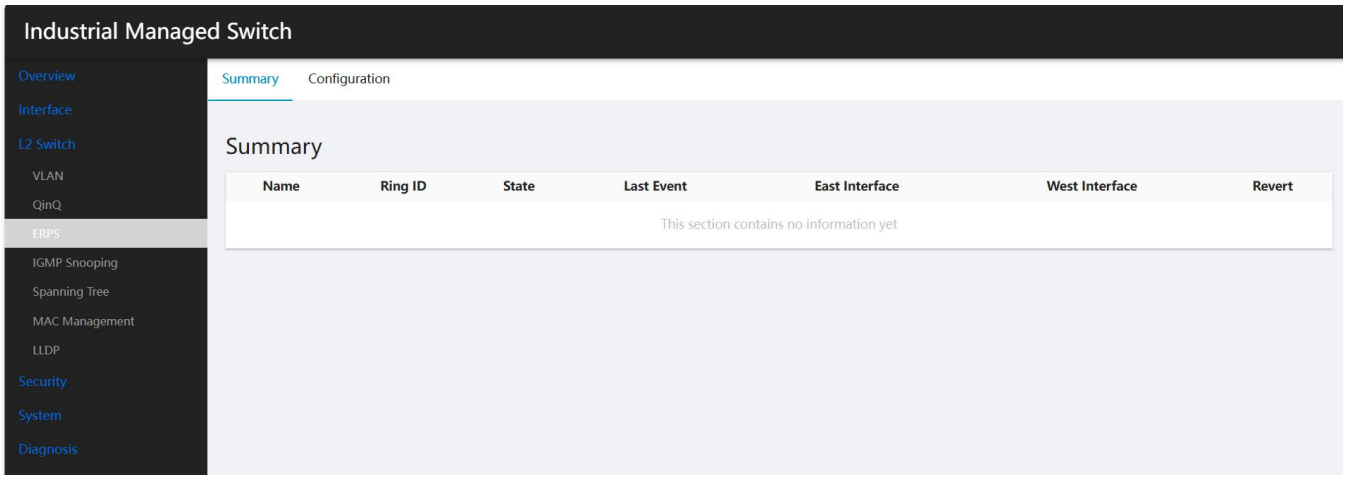


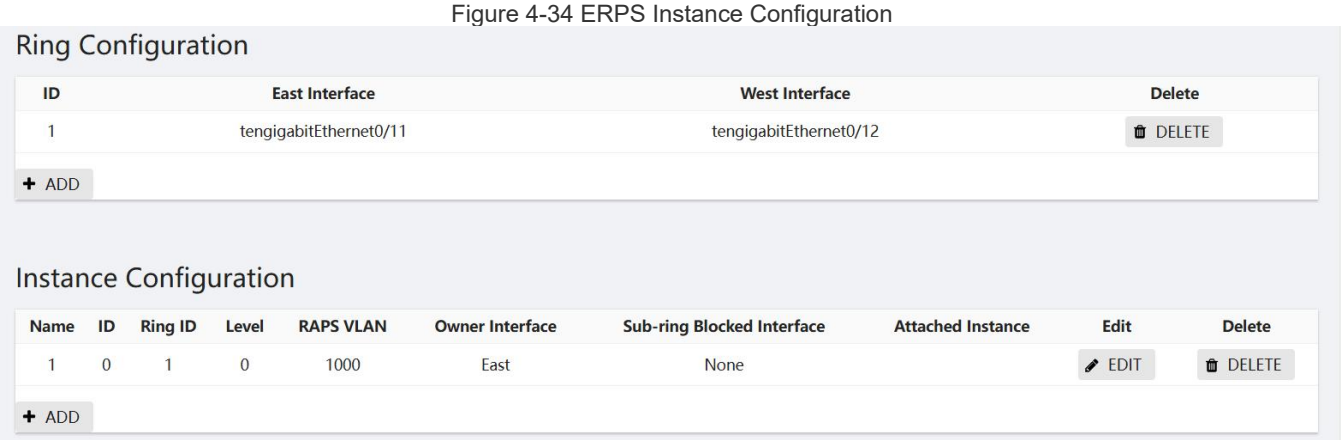
Table 4-33 Description of Ring Configuration Parameters

configuration item	clarification
ring number	ERPS ring ID, which can be any number.The ring number must be unique for each ERPS ring.
East Interface	Eastbound interface of the ERPS ring
western interface	Westbound interface of the ERPS ring
manipulate	Deleting an ERPS instance

4.3.3.2 ERPS Instance Configuration

Click on the navigation bar and select [Configuration] [ERPS] [Instance Configuration] to enter the ERPS Instance Configuration interface, as shown in Figure 4-34.

Figure 4-34 ERPS Instance Configuration



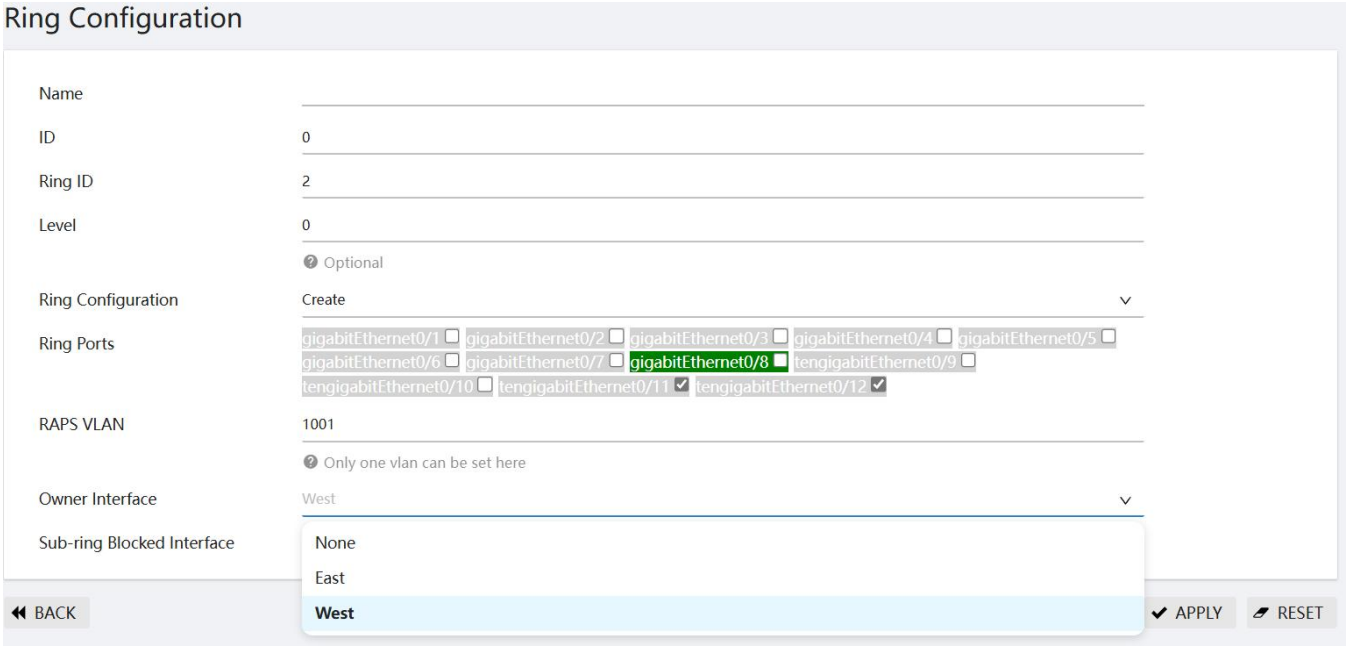
Click the [+Add] button under ERPS "Instance Configuration" to enter the ERPS instance configuration interface, as shown in Figure 4-35, and the specific parameters of the instance configuration are described in Table 4-36.

Table 4-35 Description of Ring Configuration Parameters

configuration item	clarification
name	Instance name, in string format, need to ensure uniqueness, e.g., the number "1", the character "aa".
ID	Configure the VLAN Instance for ERPS instance protection; by default all VLANs belong to Instance 0; the default id is 0.
ring number	Associated ring ID, must be an already created ring

(military) rank	ERPS priority, default is 0
RAPS Management VLAN	Each switch in the same ring must be configured with the same RAPS management VLAN for transmitting ERPS protocol messages. The RAPS management VLAN can be a virtual VLAN, which is required to be just different from the data VLAN and does not need to be physically created.
Data VLAN	ERPS data VLANs, set the VLANs that are allowed to be transmitted in the ERPS ring. must be a VLAN that already exists, if not please add it in the VLAN configuration; Support VLAN Range class configuration, for example, "1-3,5" means VLAN 1,2,3,5;
Owner Interface	The main ring ERPS Owner node, you can select the east interface or the west interface as the Owner node. Each ERPS ring has one and only one device configured as an RPL Owner node, which controls the ports to be blocked.
subring blocking port	Subring blocking port, a subring has only one blocking port, you can choose east or west. This parameter needs to be configured only when the ring is tangent, and the subrings of two devices whose rings are tangent must set the subring blocking port.
Linked Example	This only needs to be set when a subring blocking port needs to be configured, set to the ring ID tangent to the current subring.

Figure 4-36 ERPS Instance Configuration

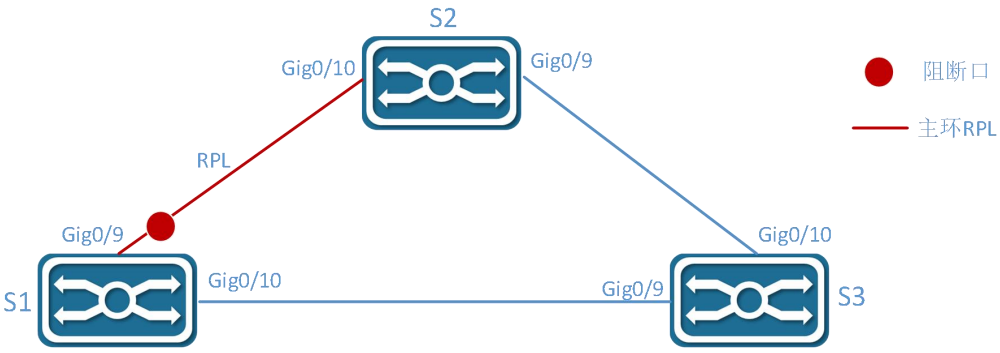


4.3.4 Example of Ring Configuration

Case Requirements:

Three switching groups are ringed, as shown in Figure 4-37, and the default blocking port is configured to be the GigabitEthernet 0/9 port of S1, so that the link can be restored in time to ensure that the network is available in the event of a failure.

Figure 4-37 ERPS Network Topology

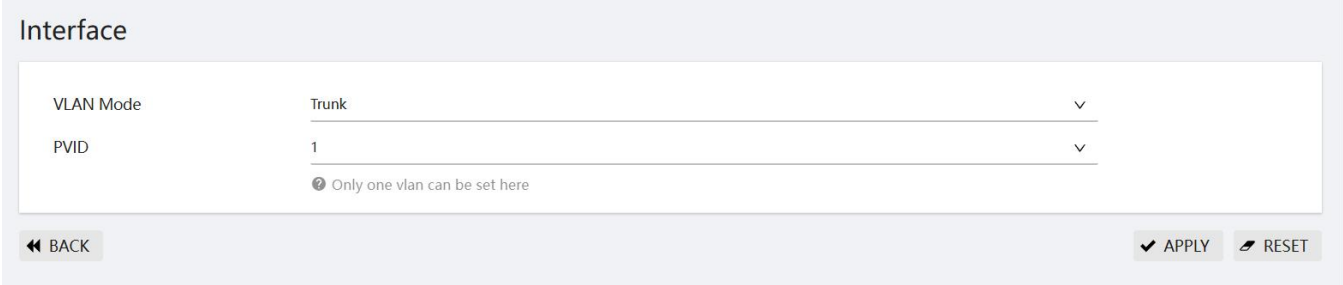


4.3.4.1 Configuring Switch S1

Step 1: Configure ports 9 and 10 as trunk ports with a Native Vlan of default 1.

Select [Configuration] [Port] [Port Configuration] in the navigation bar to enter the interface configuration interface, click the [Bulk Edit] button, as shown in Figure 4-38, select ports GigabitEthernet 0/9 and GigabitEthernet 0/10, and select "Trunk" for the port mode.

Figure 4-38 Port Configuration Interface



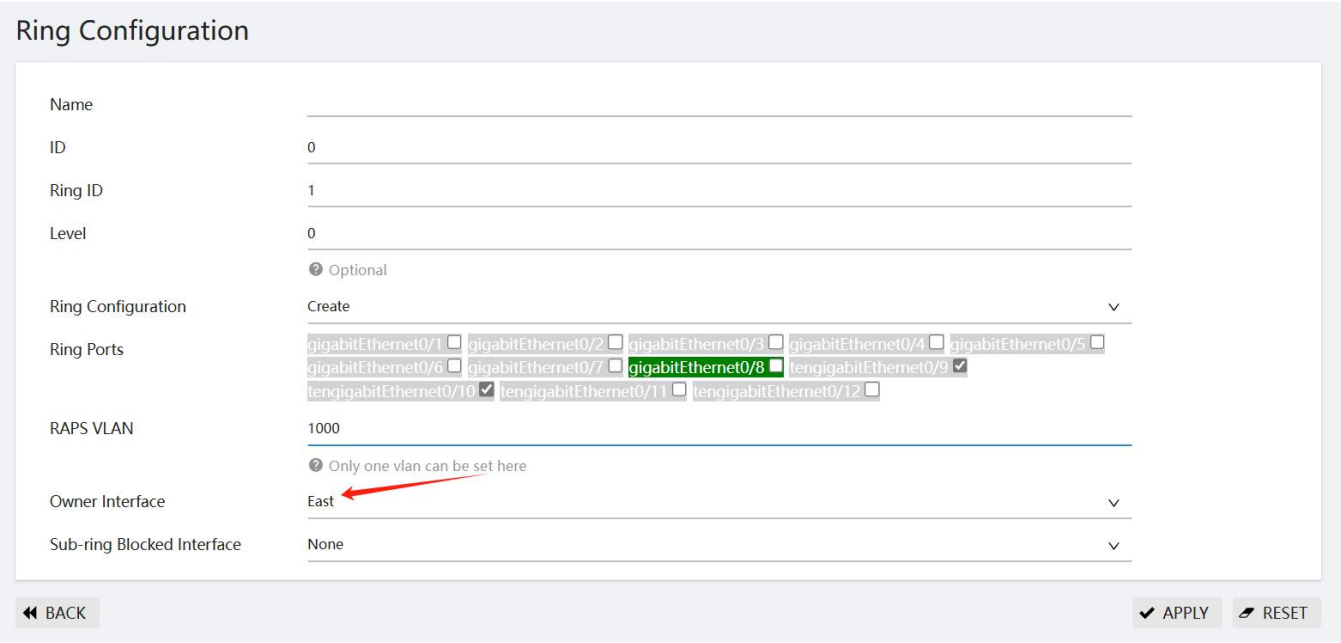
Click the [Confirm] button to return to the interface as shown in Figure 4-39.

Figure 4-39 Port Status Display Screen

Step 2: Create ERPS Ring。

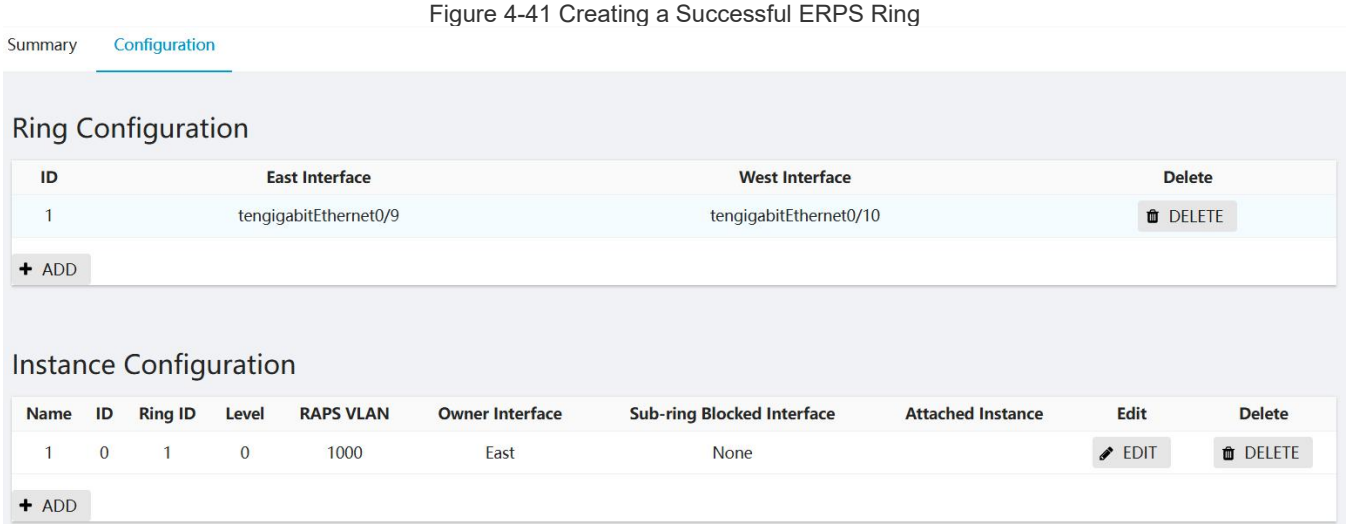
Select [Configuration] [ERPS] in the navigation bar to enter the ERPS configuration interface, click the [+ Add] button below the change configuration to enter the ERPS ring configuration interface, as shown in Figure 4-40.The ring number is set to "1", the east interface is set to "GigabitEthernet 0/9", and the west interface is set to "GigabitEthernet 0/10".The RAPS VLAN defaults to "1000", the ID defaults to "0", the level defaults to "0", and the Owner interface defaults to "0"."East", subring blocking port "None".

Figure 4-40 ERPS Ring Configuration Screen



Click the [Confirm] button to return to the following page, as shown in Figure 4-41。

Figure 4-41 Creating a Successful ERPS Ring



Step 3: Click the [Save] button in the auxiliary area to save the configuration。

clarification

- In the case of a single ring, only one blocking point is required, and the selection of the blocking point is generally considered to be in the middle of the ring。

4.3.4.2 Configure switches S2 and S3

Step 1: Configure ports 9 and 10 as trunk ports, and Native Alan as default value 1.

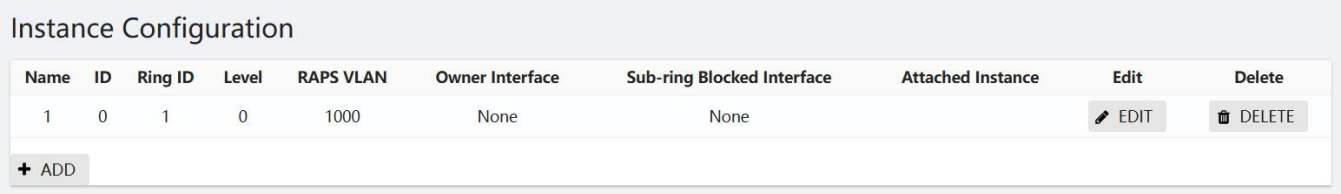
Select [Configuration] [Port] [Port Configuration] in the navigation bar to enter the interface configuration interface, click [Bulk Edit] to select ports GigabitEthernet 0/9 and GigabitEthernet 0/10, and select "Trunk" for

the port mode and "Native Vlan" for the port mode.Default is "1", Allows VLANs is "all", click [OK] button to complete the configuration.

Step 2: Create ERPS Instance

Select [Configuration][ERPS] in the navigation bar to enter the ERPS configuration interface, click the [+Add] button under "Ring Configuration" to enter the ERPS ring configuration interface, set the ring number to "1", the east interface to "GigabitEthernet 0/9", and the west interface to "GigabitEthernet 0/10".The ring number is set to "1", the east interface is set to "GigabitEthernet 0/9", and the west interface is set to "GigabitEthernet 0/10"; the RAPS VLAN is set to "1000" by default, and the ID is set to "1000" by default.", ID default "0", level default "0", Owner interface "None", subring blocking port"None", click the [Confirm] button to complete the configuration.The successfully created ERPS ring is shown in Figure 4-42.

Figure 4-42 Creating a Successful ERPS Ring



Step 3: Select the [Save] button on the navigation bar to save the configuration.

clarific

- Unlike S1, S2 and S3 lie in the blocking point Owner interface = None。

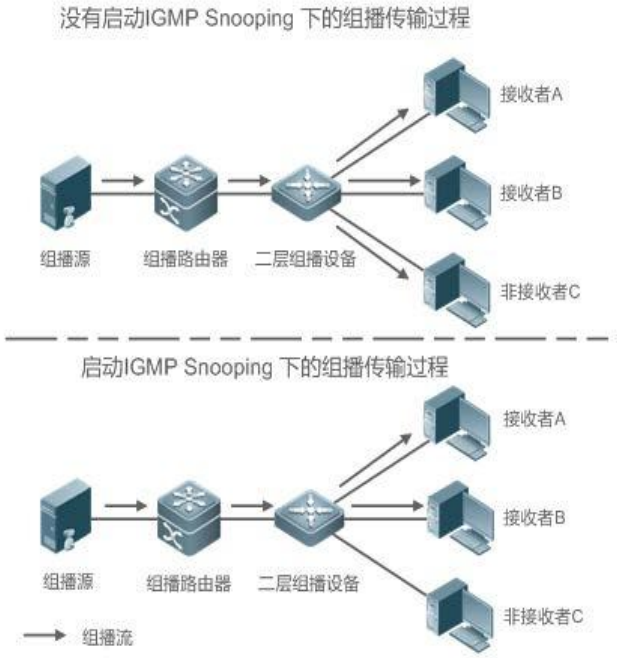
4.4 IGMP Snooping

4.4.1 summarize

IGMP Snooping is Internet Group Management Protocol Snooping(short for Internet Group Management Protocol Snooping), which is a mechanism for multicast constraints running on Layer 2 devices to manage and control multicast groups.

A Layer 2 device running IGMP Snooping establishes a mapping relationship for ports and MAC multicast addresses by analyzing received IGMP messages and forwards multicast data based on such a mapping relationship.When a Layer 2 device is not running IGMP Snooping, multicast data is broadcast at Layer 2; when a Layer 2 device is running IGMP Snooping, multicast data for a known multicast group is not broadcast at Layer 2 but is multicast at Layer 2 to a specified receiver.

Figure 4-43 How IGMP Snooping Works



As shown in Figure 4-43, when a Layer 2 multicast device is not running IGMP Snooping, IP multicast messages are broadcast within the VLAN; when a Layer 2 multicast device is running IGMP Snooping, IP multicast messages are sent only to group member receivers.

4.4.2 IGMP Snooping deployment

4.4.2.1 IGMP Global Configuration Description

(1) Select [Switching] [IGMP Snooping] [Configuration] in the navigation bar to enter the IGMP Snooping interface.

(2) In the current interface, click the "Enable" button to globally enable the IGMP Snooping function, as shown in Figure 4-44.

(3) Click the Discard Unknown Multicast "Disabled" button to enable the Discard Unknown Multicast function, which is optional.

(4) Click the Topology Change Suppression "Disabled" button to enable the Topology Change Suppression function, which is optional.

Figure 4-44 IGMP Global Configuration Interface

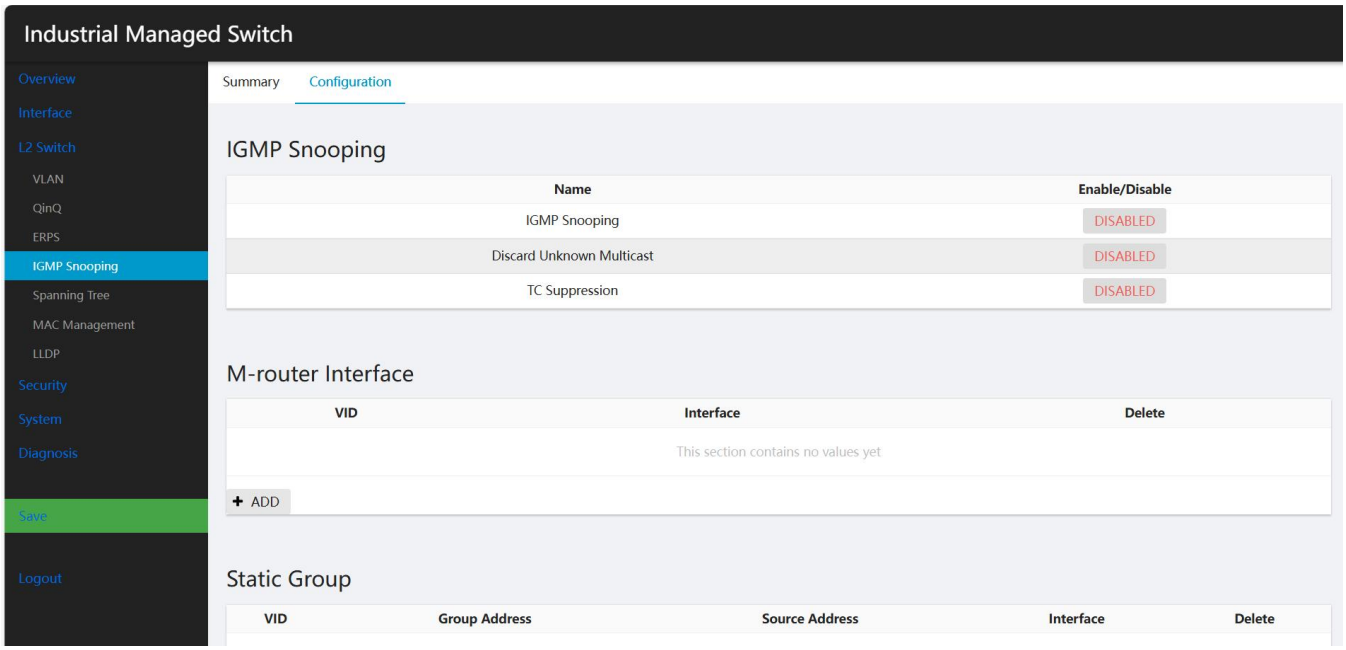


Table 4-45 Description of Global Configuration Parameters

configuration item		clarification
IGMP Snooping	state of affairs	Enable/disable the IGMP Snooping function, the default is off.
	Discard Unknown Multicast	Enable/disable Discard Unknown Multicast feature Unknown multicast data packets are IGMP Snooping forwarding tables that do not have a corresponding forwarding table entry for those multicast data packets: - When the Discard Unknown Multicast Data Messages function is enabled, the switch discards all received unknown multicast Unknown Multicast Data Messages - When discarding unknown multicast data packets is disabled, the switch discards all received unknown multicast data packets in the unknown multicast data packet's forwarding table. When the function of dropping unknown multicast data packets is disabled, the switch will broadcast unknown multicast data packets in the VLAN to which they belong.
	Topology change suppression	Enable/disable topology change suppression

4.4.2.2 IGMP Routing Port Configuration Description

(1) Select [Switching] [IGMP Snooping] [Configuration] in the navigation bar to enter the IGMP Route Port page, as shown in Figure 4-46.

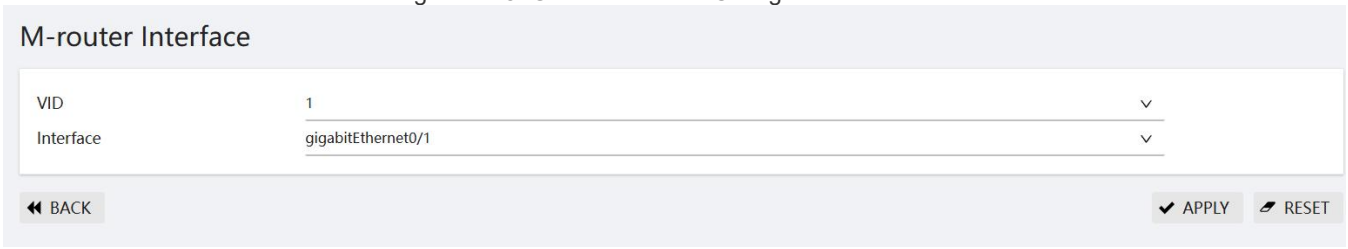
Figure 4-46 IGMP Routing Port Interface

Table 4-47 IGMP Routing Port Parameter Descriptions

configuration item		clarification
IGMP router port	VID	ID of the VLAN to which the multicast table entry belongs
	connector	All member ports
	removing	Delete this IGMP route

(2) Click the [Add] button under "Multicast Routing Port" to enter the IGMP routing port setting interface, as shown in Figure 4-48, configure the VID and select the port to be applied.Click the [Confirm] button to complete the configuration.

Figure 4-48 IGMP Route Port Configuration Interface



4.4.2.3 IGMP Static Group Configuration Description

(1) Select [Switching] [IGMP Snooping] [Configuration] in the navigation bar to enter the IGMP static group display page, as shown in Figure 4-49, and the parameter descriptions are shown in Table 4-50.

Figure 4-49 IGMP static group display screen

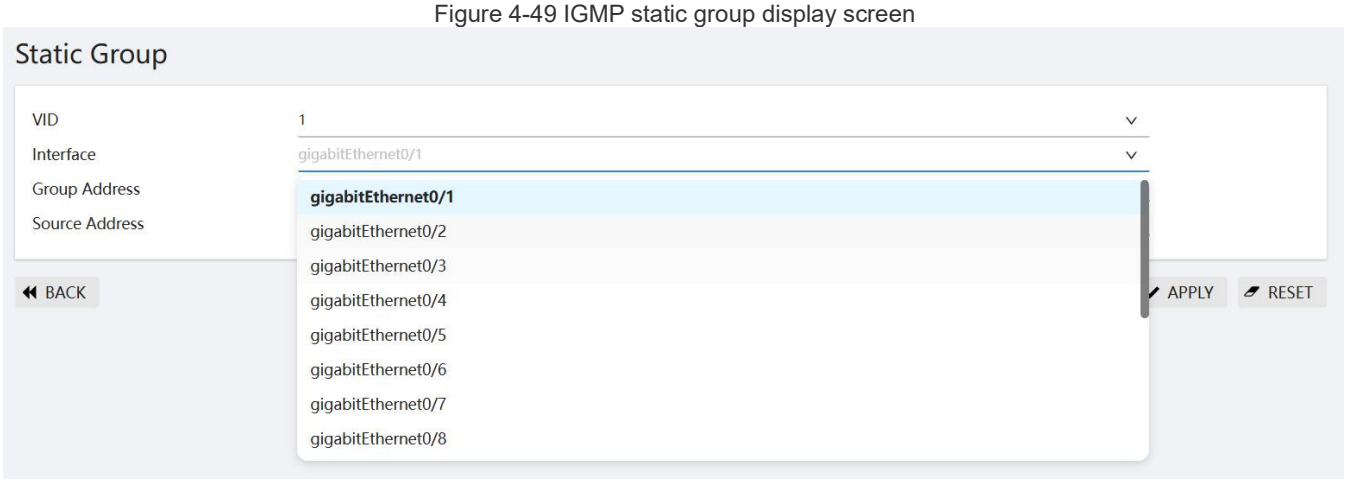


Table 4-50 IGMP static group parameter descriptions

configuration item		clarification
IGMP static group	VID	ID of the VLAN to which the multicast table entry belongs
	group address	multicast group address
	source address	multicast source address
	connector	All member ports
	removing	Delete this IGMP static group

(2) Click the [Add] button under "Static Group" to enter the IGMP static group configuration interface, as shown in Figure 4-51.Configure the VID, group address, source address and interface name in turn.Click the [Confirm] button to complete the configuration.

Figure 4-51 IGMP Static Group Configuration Interface

M-router Interface

VID	Interface	Delete
1	gigabitEthernet0/1	DELETE

+ ADD

Static Group

VID	Group Address	Source Address	Interface	Delete
1	225.0.0.1		gigabitEthernet0/2	DELETE

+ ADD

4.4.2.4 Configuration Example

Configuration Example

Case Requirement:

The video server uses 225.0.0.1 as the multicast source and uses multicast data streams to play videos, so that users can click to play videos on demand and only video packet streams exist in the path from the server to the on-demand clients.

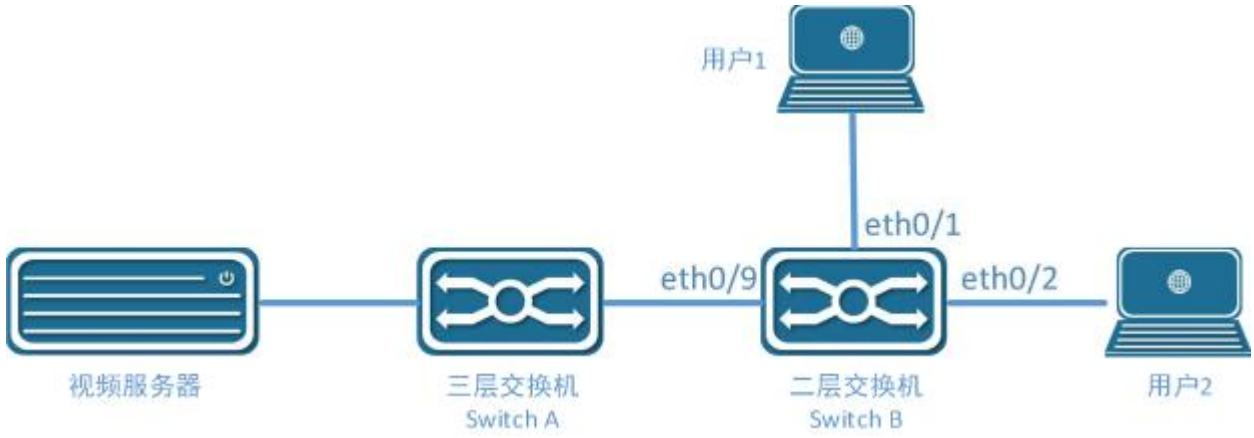
Only the video message stream exists in the path from the server to the on-demand client in the network, and there should be no duplicate or invalid streams to maximize the network bandwidth utilization. The network topology is shown in Figure 4-52.

The network topology is shown in Figure 4-52, in which the Layer 3 switch is directly connected to the multicast source as a multicast routing device, enables the multicast route forwarding function, and configures the multicast routing protocol (see the corresponding Layer 3 switch for details).

(see the configuration manual of the corresponding Layer 3 switch). The Layer 2 access switch acts as a user access device, and the data VLAN is the default VLAN 1.

The uplink port is GigabitEthernet 0/9, and the downlink ports are GigabitEthernet 0/1 and GigabitEthernet 0/2 respectively.

Figure 4-52 IGMP Network Topology

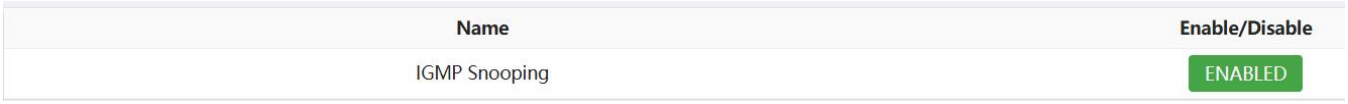


Step 1: Enable the IGMP Snooping function on Switch B.

Select [IGMP Snooping] in the [Switching] subsection of the navigation bar, enter the configuration interface, and click [Disabled] behind [IGMP Snooping].

Click the [Disabled] button after [IGMP Snooping] to enable the IGMP Snooping function, as shown in Figure 4-53.

cFigure 4-53 IGMP Enable Configuration Interface

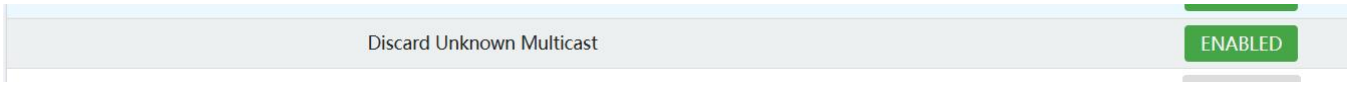


Step 2: Enable Discard Unknown Multicast on Switch B (Optional)

Select [IGMP Snooping] in the [Switching] subsection of the navigation bar, enter the configuration interface, and click [Disabled] behind [Discard Unknown Multicasts].

to enable the Discard Unknown Multicast function, as shown in Figure 4-54.

Figure 4-54 IGMP Drop Unknown Multicast Configuration Interface

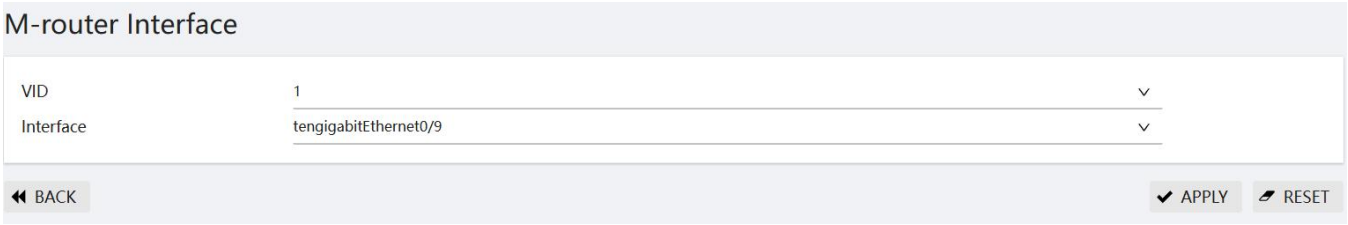


Step 3: Configure an IGMP Routing Port on the Switch B Uplink (optional)

Select [IGMP Snooping] in the [Switching] subsection of the navigation bar, enter the configuration interface, and click [+Add] under [IGMP Route Port].

button under [IGMP Route Port] to enter the Route Port Adding interface, as shown in Figure 4-55.

Figure 4-55 IGMP Routing Port Configuration Interface



Click the [OK] button to return to the interface as shown in Figure 4-56.

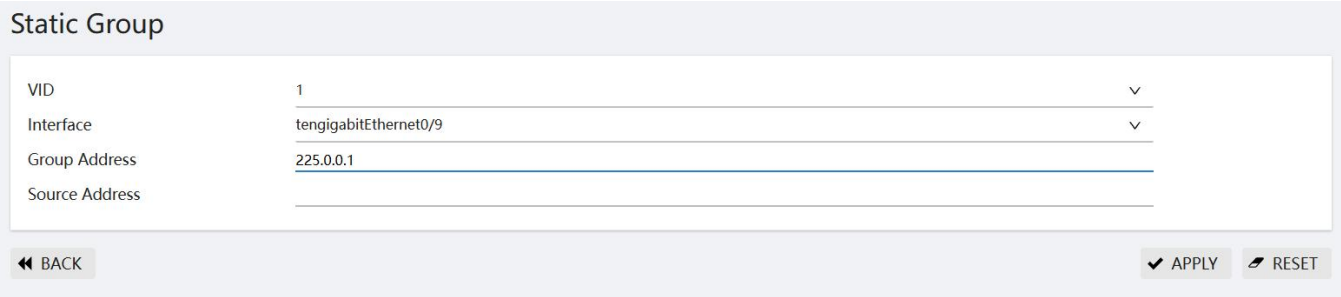
Figure 4-56 IGMP Routing Port Display Interface

Step 4: Configure an IGMP Static Group on the Switch B Downlink Port (Optional)

Select [IGMP Snooping] in the [Switching] subsection of the navigation bar, enter the configuration interface, and click [+Add] under [Static Group].

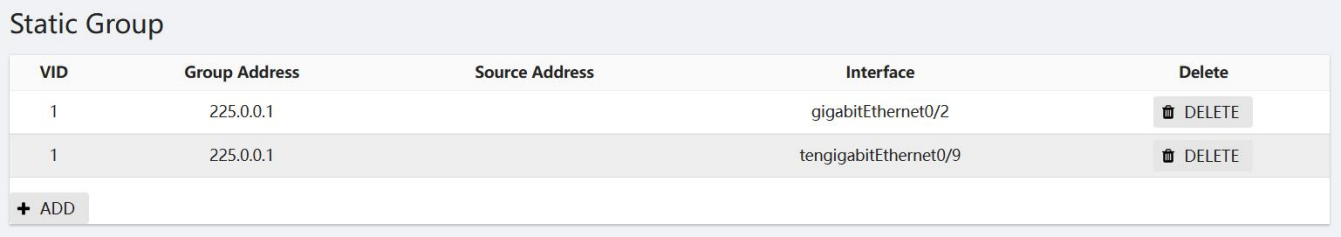
button under [+Add] to enter the Route Port Add interface and create a static group, as shown in Figure 4-57.

cFigure 4-57 IGMP Static Group Configuration Interface



Click the [Apply] button and do the same to add GigabitEthernet 0/2 to the same static group, as shown in Figure 4-58.

Figure 4-58 IGMP Static Group Display Interface



Step 5: Select the [Save] button on the navigation bar to save the configuration.

4.5 spanning tree

4.5.1 summarize

Spanning Tree Protocol is a Layer 2 management protocol that eliminates Layer 2 loops by selectively blocking redundant links in the network, and also has a link backup feature.

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

For Layer 2 Ethernet, there can only be one active path between two LANs, otherwise a broadcast storm will occur.But in order to enhance the reliability of a LAN, it is again necessary to create redundant links, some of which must be in a backup state, and the redundant link must be brought up to an active state if and when the network fails and the other link fails.Manually controlling such a process is obviously a very hard job, and the STP protocol does it automatically.It enables devices in a LAN to do the following:

- Discover and activate an optimal tree topology for the LAN.
- Discover and start an optimal tree topology for the LAN. Discover and recover from faults, automatically updating the network topology so that the best possible tree structure is selected at any given time.

4.5.2 Spanning Tree Configuration

The Spanning Tree module provides global configuration, MST configuration, instances, interfaces, and other configurations for Spanning Tree.

Spanning Tree Global Configuration

Select [Exchange] [Spanning Tree] [Global Configuration] in the navigation bar to enter the Spanning Tree Global Configuration interface, as shown in Figure 4-59.The global configuration parameters are shown in Table 4-60.

Figure 4-59 Spanning Tree Global Configuration

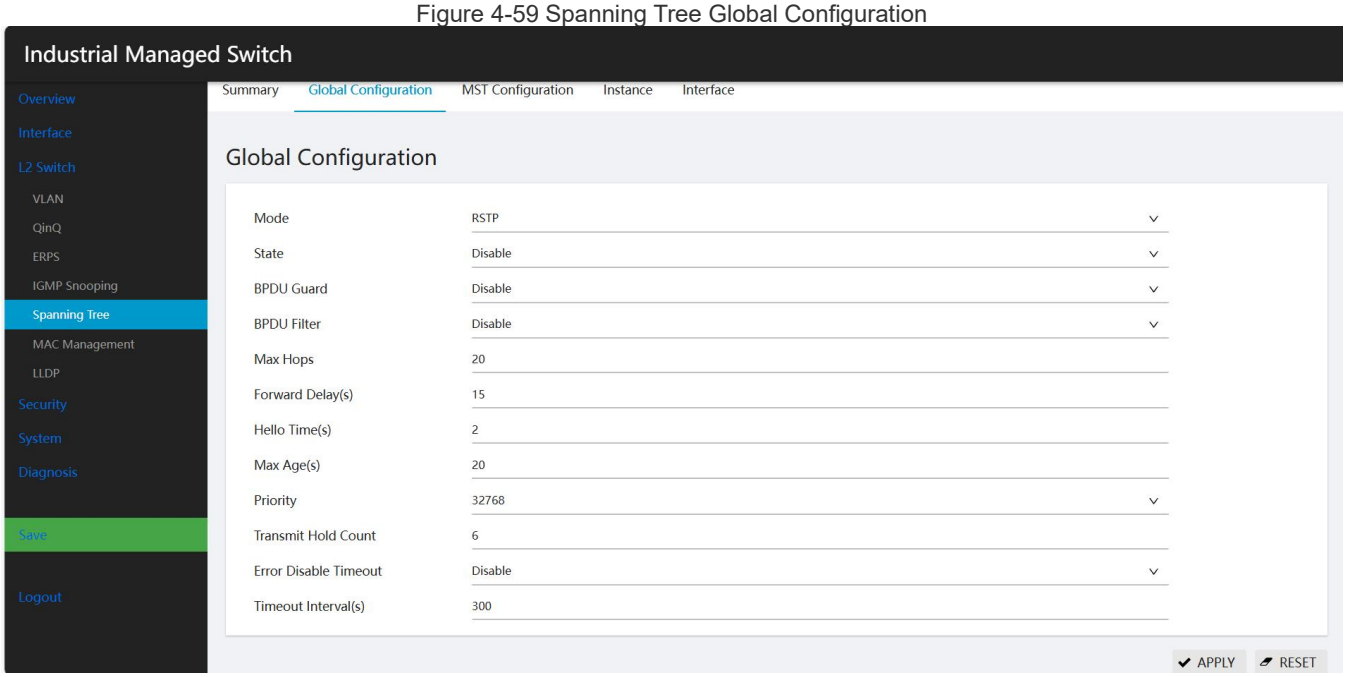


Table 4-60 Description of Spanning Tree Profile Parameters

configuration item		clarification
global configuration	paradigm	Set the working mode of STP, including STP, RSTP and MSTP. STP: In STP mode, each port of the device will send STP BPDU messages outward. RSTP: In RSTP mode, each port of the device will send RSTP BPDU messages outward, and when it is found to be connected to a device running STP, the port will automatically migrate to STP mode. MSTP: In MSTP mode, each port of the device will send MSTP BPDU messages outward, and when it is found to be connected to a device running STP, the port will automatically migrate to STP mode.
	state of affairs	Set whether to enable the global STP function
	Handshake period (seconds)	Set the period for the device to send hello messages to detect link failure
	prioritization	Bridge Priority
	Forwarding delay (seconds)	Setting the delay time for device state migration
	forwarding threshold	Maximum number of BPDU messages sent per second by the bridge
	Aging time (seconds)	Set the maximum length of time a message can be stored in the device
	Error port disable timeout	Configuring Automatic Error Port Disabling
	Error port disable ctimeout time	Configure the timeout to un-disable an error port after it has been automatically disabled

Spanning Tree Instance Configuration

Select [Switching] [Spanning Tree] [Instance Configuration] in the navigation bar to enter the Spanning Tree Instance Configuration interface, as shown in Figure 4-61.The instance configuration parameters are shown in Table 4-62.

Figure 4-61 Spanning Tree Instance Configuration

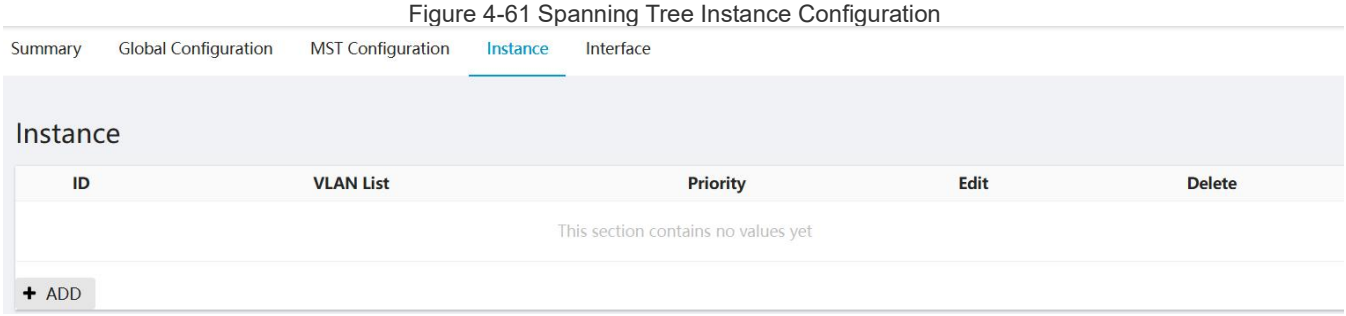


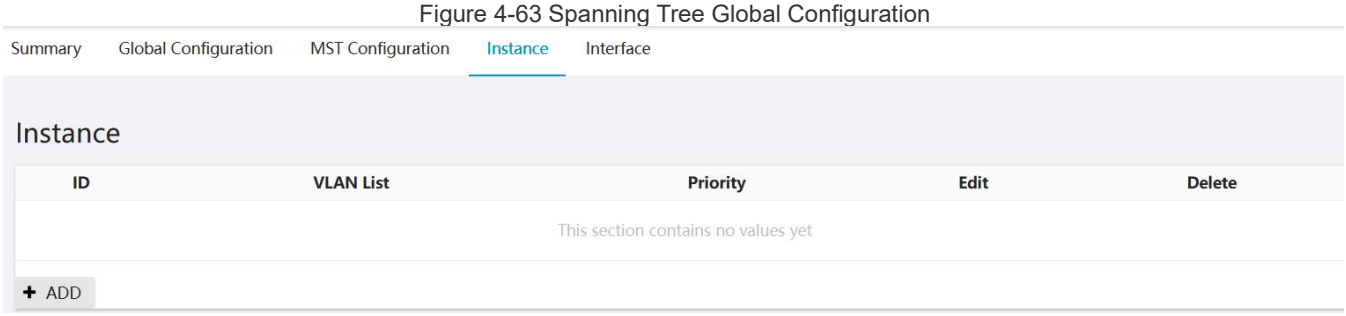
Table 4-62 Spanning Tree Instance Configuration Parameter Descriptions

configuration item		clarification
an actual example	ID	Instance ID
	VLAN List	All VLANs associated with the instance, in list form
	prioritization	Priority of the bridge in the current instance
	compiler	Click to edit the change instance
	removing	Click to delete this instance

Spanning Tree Port Configuration

Select [Switching] [Spanning Tree] [Interface Configuration] in the navigation bar to enter the Spanning Tree Port Configuration interface, as shown in Figure 4-63.The port configuration parameters are shown in Table 4-64.

Figure 4-63 Spanning Tree Global Configuration



cTable 4-64 Description of Spanning Tree Profile Parameters

configuration item		clarification
Port Configuration	cname	interface name
	cstate of affairs	Spanning Tree Switch Status of the Interface
	Link Type	Configure the interface link type
	root protection	Configure the interface to enable root protection
	Auto Edge Port	Configure the interface to automatically recognize edge ports
	edge port	Configure the interface as an edge port
	fast port	Configure the interface as a fast port
	BPDU Filtration	Configure the interface to enable BPDU filtering
	BPDU protection	Configure the interface to enable BPDU protection
	Instance/priority/TCN	Configuring Instance ID, Priority, and Topology Change Announcement

	message limits	Message Suppression

4.5.3 Configuration Example

Configure MSTP so that messages for different VLANs are forwarded according to different spanning-tree instances as shown in Figure 4-66:

- All devices in the network belong to the same MST domain;
- All devices in the network belong to the same MST domain. VLAN 20 is forwarded along instance 0, VLAN 10 messages are forwarded along instance 1, VLAN 30 is forwarded along instance 3, and VLAN 40 is forwarded along instance 3.

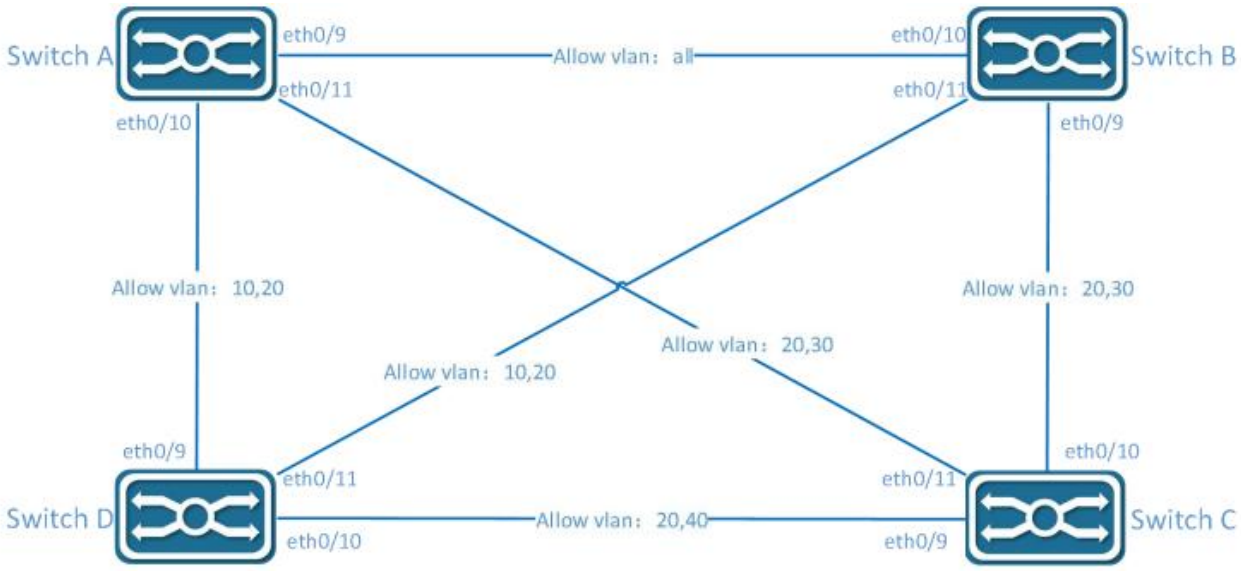
VLAN 30 is forwarded along instance 3, and VLAN 40 is forwarded along instance 4, as shown in Figure 4-65.

The parameters of each device are configured as shown in Table 4-65.

参数 / 设备	VLAN	实例	端口
Switch A	10	1	GigabitEthernet 9, GigabitEthernet 0/10
	20	0	GigabitEthernet 9, GigabitEthernet 0/10, GigabitEthernet 0/11
	30	3	GigabitEthernet 9, GigabitEthernet 0/11
	40	4	GigabitEthernet 9

Switch B	10	1	GigabitEthernet 0/10, GigabitEthernet 0/11
	20	0	GigabitEthernet 9, GigabitEthernet 0/10, GigabitEthernet 0/11
	30	3	GigabitEthernet 9, GigabitEthernet 0/10
	40	4	GigabitEthernet 10
Switch C	10	1	
	20	0	GigabitEthernet 9, GigabitEthernet 0/10, GigabitEthernet 0/11
	30	3	GigabitEthernet 10, GigabitEthernet 0/11
	40	4	GigabitEthernet 9
Switch D	10	1	GigabitEthernet 9, GigabitEthernet 0/11
	20	0	GigabitEthernet 9, GigabitEthernet 0/10, GigabitEthernet 0/11
	30	3	
	40	4	GigabitEthernet 10

配置环网拓扑图 4-66

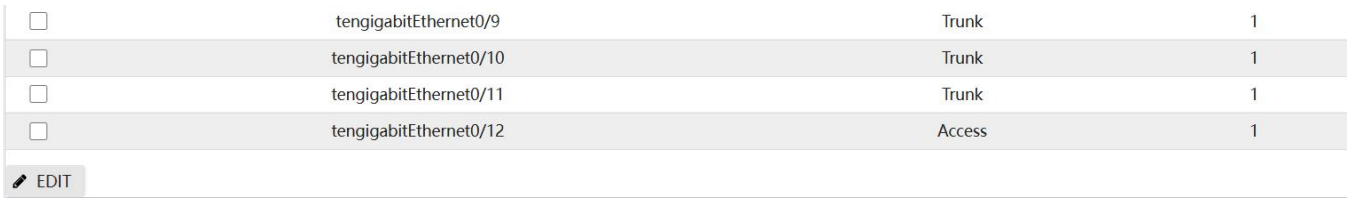


3.4.2.2 Configuring Switch A

Step 1: Select [Switching] ⇨ [VLAN] in the navigation bar, and in the Interface Configuration interface, configure ports 9, 10, and 11 as trunk ports, Native Vlan

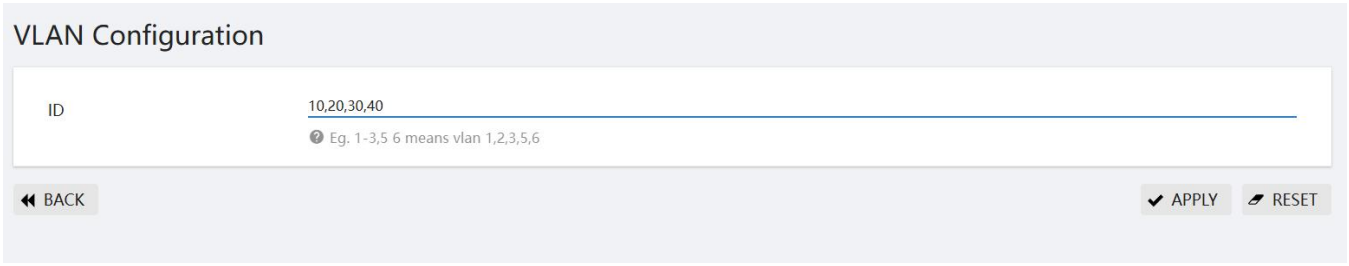
Switch Web Configuration Guide

Figure 4-67 VLAN Mode Configuration Interface



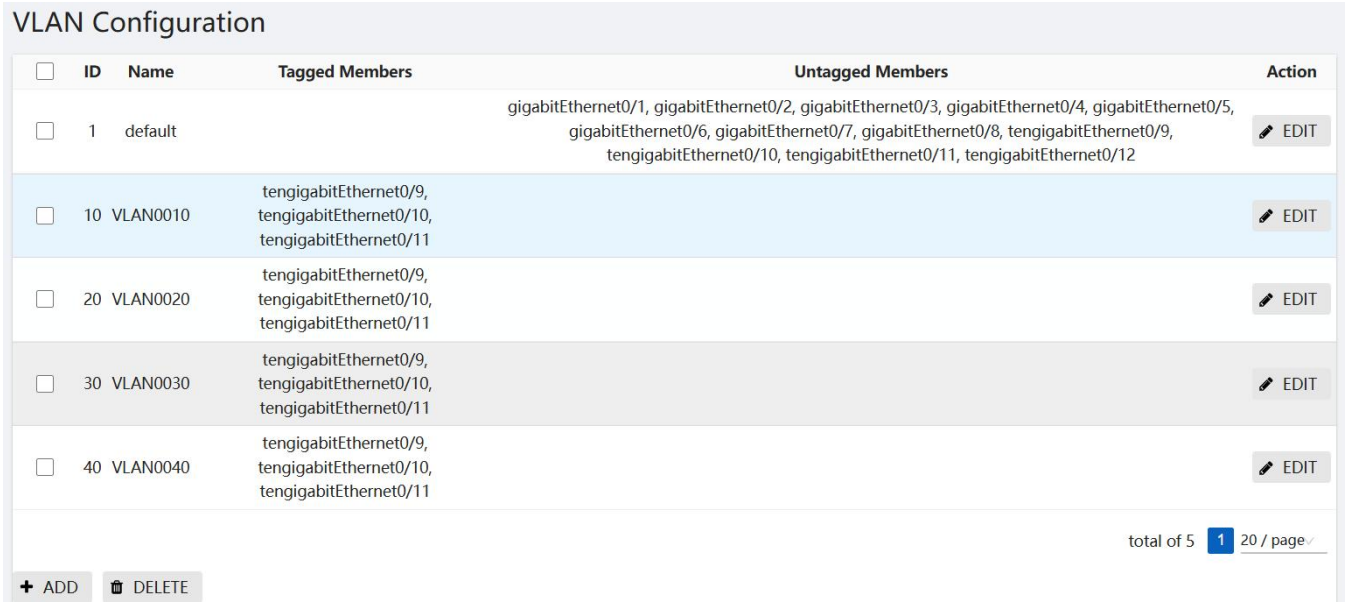
Step 2: In the VLAN interface, click the [Add] button to create VLANs 10, 20, 30, and 40, as shown in Figure 4-68.

Figure 4-68 VLAN Creation Screen



Click the [Apply] button to return to the interface as shown in the figure, at this time the default will add all the ports to the VLAN.

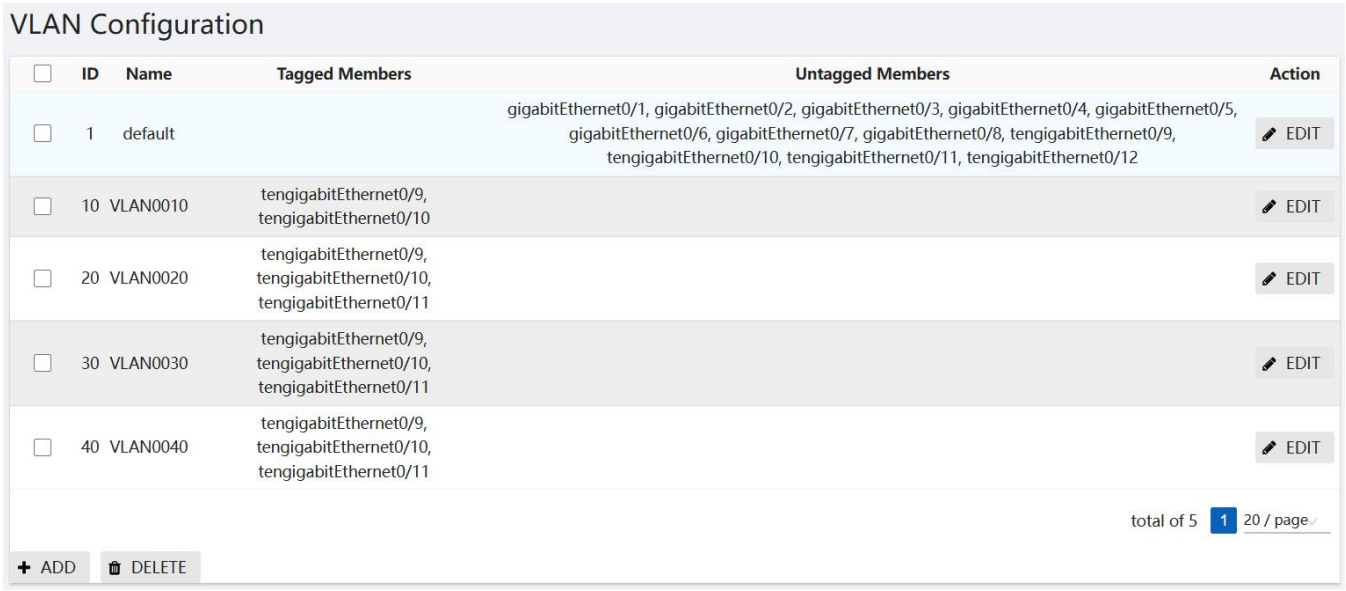
Figure 4-69 VLAN Status Display Interface



Check VLAN 10, click the [Edit] button to enter the editing interface, remove port GigabitEthernet 0/11,click Apply and return to the following interface.

The following interface will be returned after clicking "Apply":

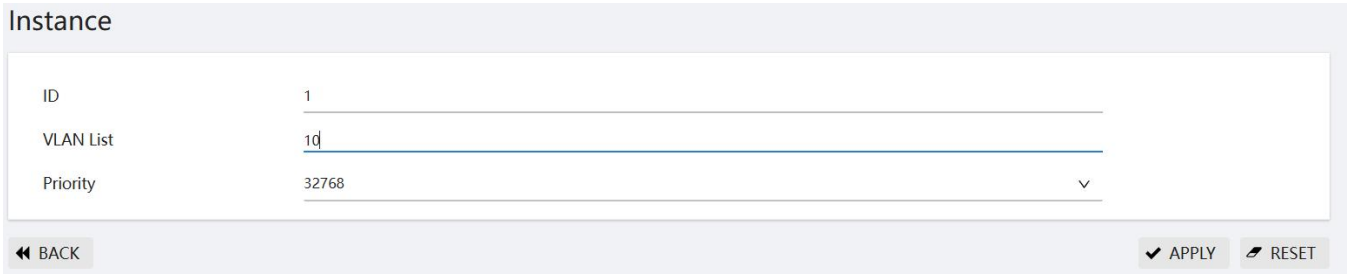
Figure 4-70 VLAN Status Display Interface



Step 3: Select [Exchange] ⇨ [Spanning Tree], click the [Instance] tab, and then click the [Add] button, as shown in the following figure, with ID "1".

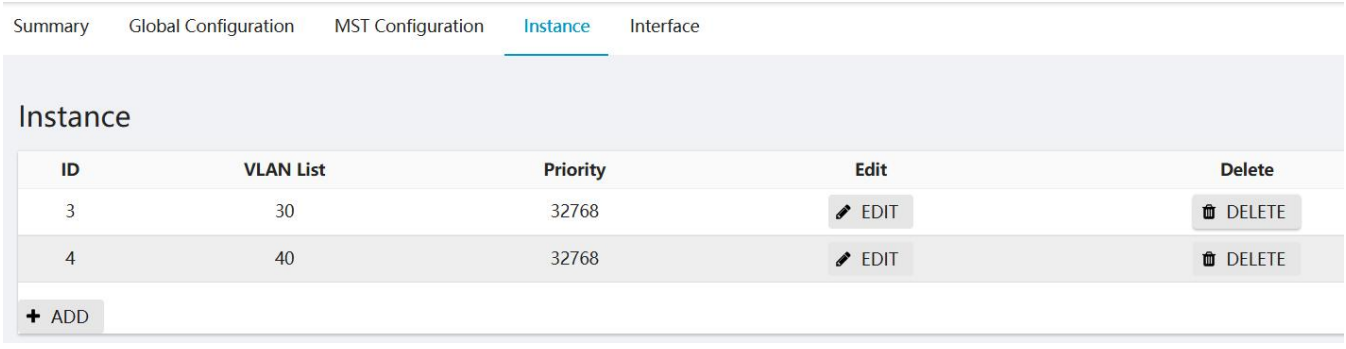
VLAN list is "10", use the default parameters for priority, and click the [Apply] button to save the configuration.

Figure 4-71 Spanning Tree Instance Configuration Screen



Using the same method, create instances 3 and 4 with corresponding VLAN lists of 30 and 40, respectively. The list of successfully created instances is shown in the figure.

Figure 4-72 Spanning Tree Instance Display Screen

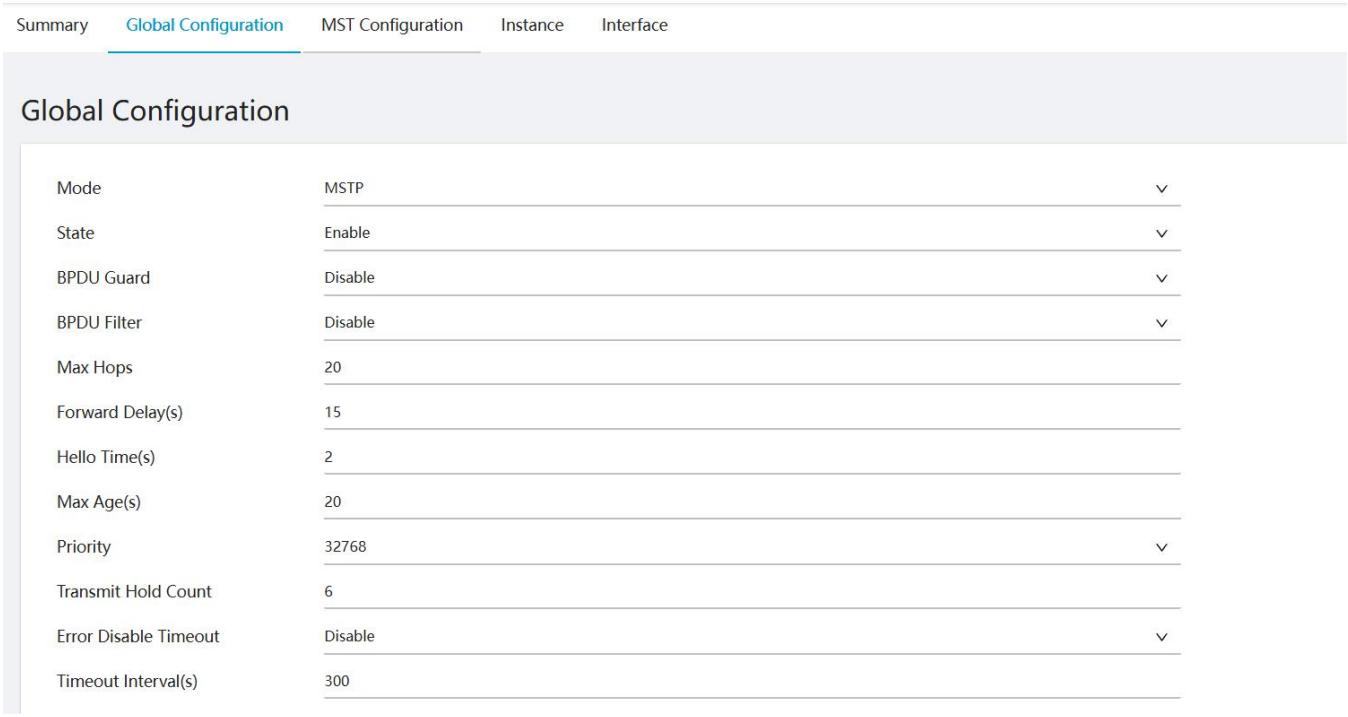


VLANs that are not associated are grouped into instance 0 by default.

Step 4: In the current interface, click on the [Global Configuration] tab, select "MSTP" as the mode, "Enable" as the status, and select the default for other parameters.

Click the [Apply] button to complete the configuration.

Figure 4-73 Spanning Tree Global Configuration Interface Switch Web Configuration Guide



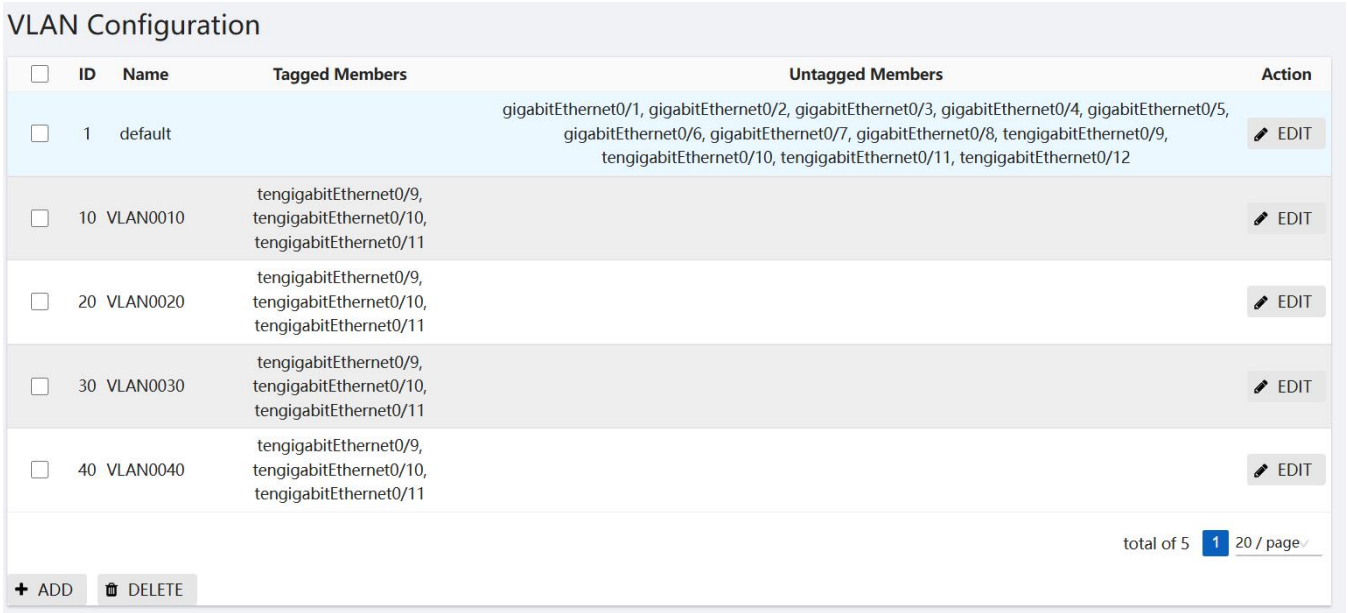
Step 5: Select the [Save] button on the navigation bar to save the configuration.

3.4.2.3 Configure Switch B

Step 1: Referring to Swtich A, configure ports 9, 10, and 11 as trunk ports, and the Native Vlan as default value 1.

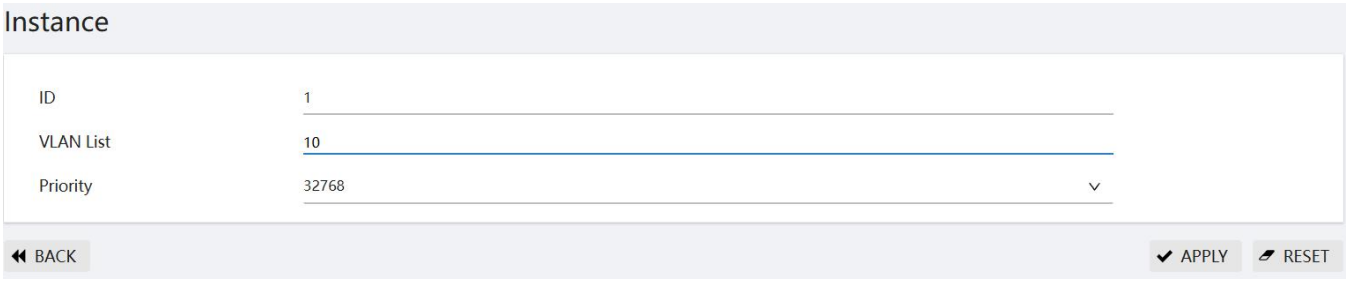
Step 2: Create VLANs 10, 20, 30, and 40, and add the corresponding ports to the VLANs as shown in the figure.

Figure 4-74 VLAN Status Display Screen



步骤 3: 选择【交换】⇨【生成树】，点击【实例】标签，点击【添加】按钮，如下图所示，ID 为“1”，VLAN 列表为“10”，优先级使用默认参数，点击【应用】按钮保存配置。

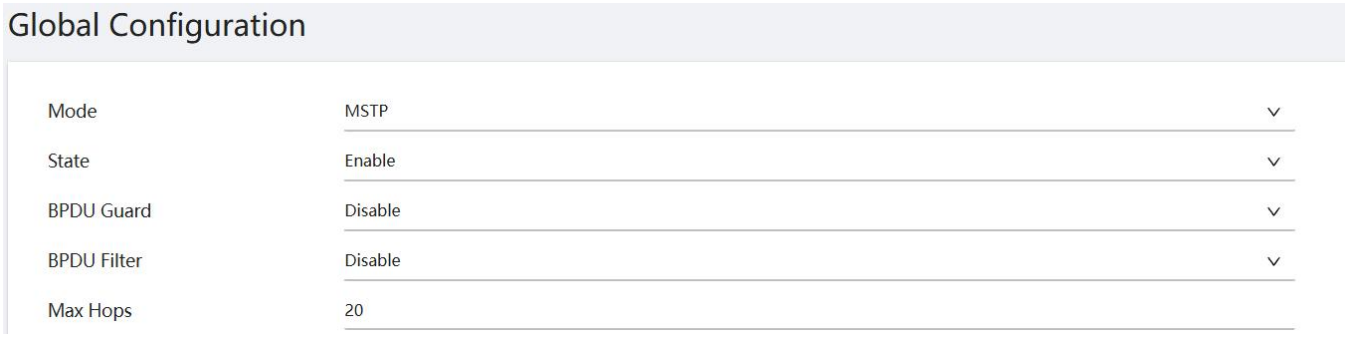
Figure 4-75 Spanning Tree Instance Display Screen



Step 4: In the current interface, click on the [Global Configuration] tab, select "MSTP" as the mode, "Enable" as the status, and select the default for other parameters.

Click the [Apply] button to complete the configuration.

Figure 4-76 Spanning Tree Global Configuration Screen



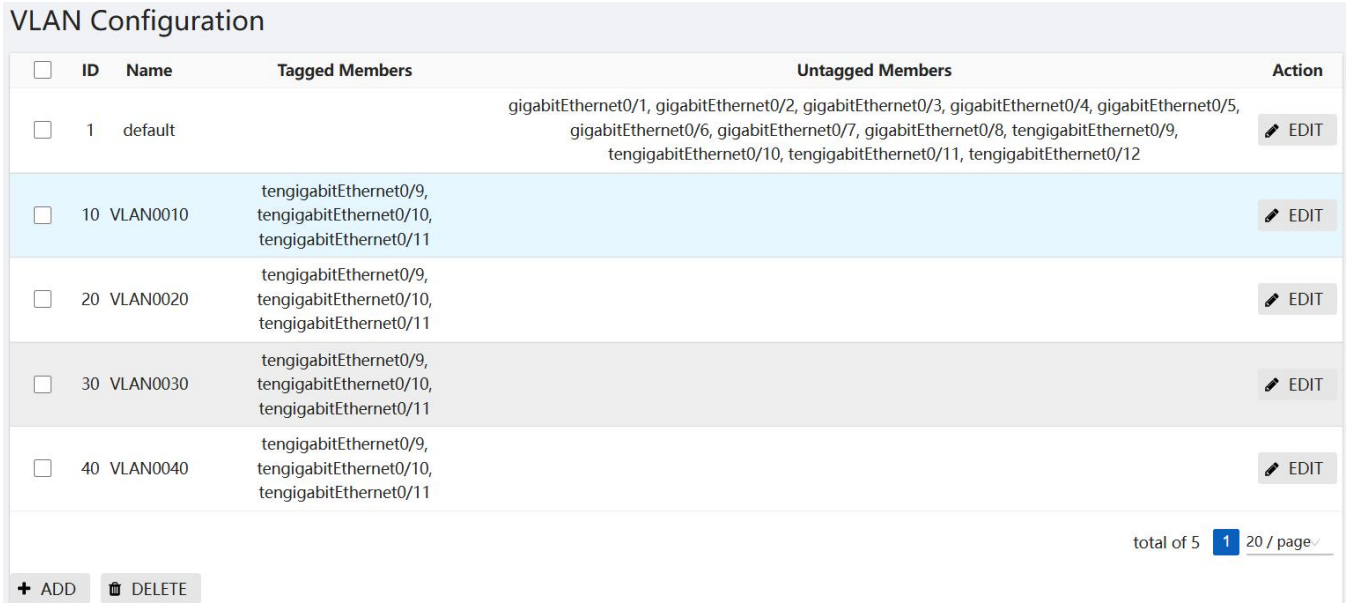
Step 5: Select the [Save] button on the navigation bar to save the configuration.

3.4.2.4 Configuring Switch C

Step 1: Referring to Swtich A, configure ports 9, 10, and 11 as trunk ports, and the Native Vlan as default value 1.

Step 2: Create VLANs 10, 20, 30, and 40, and add the corresponding ports to the VLANs as shown in the figure.

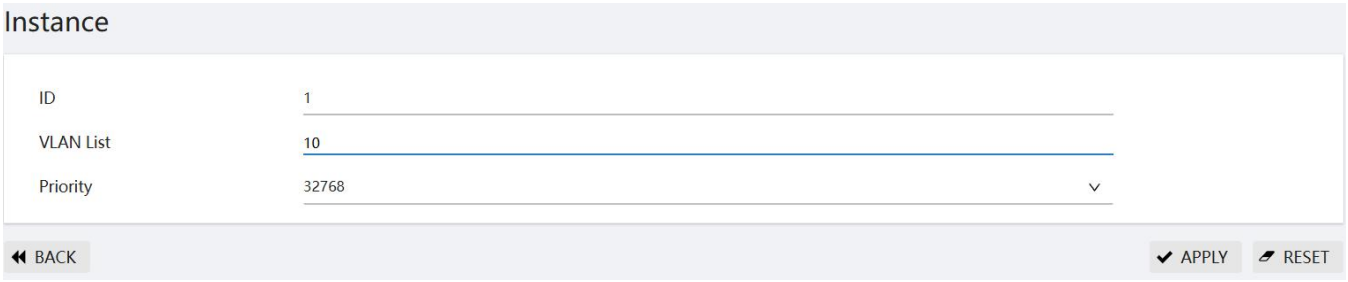
Figure 4-77 VLAN Status Display Screen



Step 3: Select [Exchange] ⇨ [Spanning Tree], click the [Instance] tab, and then click the [Add] button, as shown in the following figure, with ID "1".

VLAN list is "10", use the default parameters for priority, and click the [Apply] button to save the configuration.

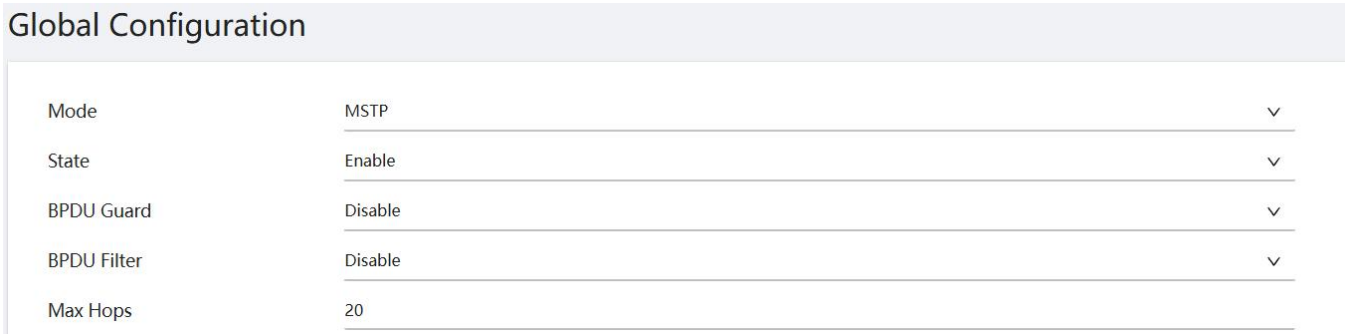
Figure 4-78 Spanning Tree Instance Display Screen



Step 4: In the current interface, click on the [Global Configuration] tab, select "MSTP" as the mode, "Enable" as the status, and select the default for other parameters.

Click the [Apply] button to complete the configuration.

Figure 4-79 Spanning Tree Global Configuration Screen



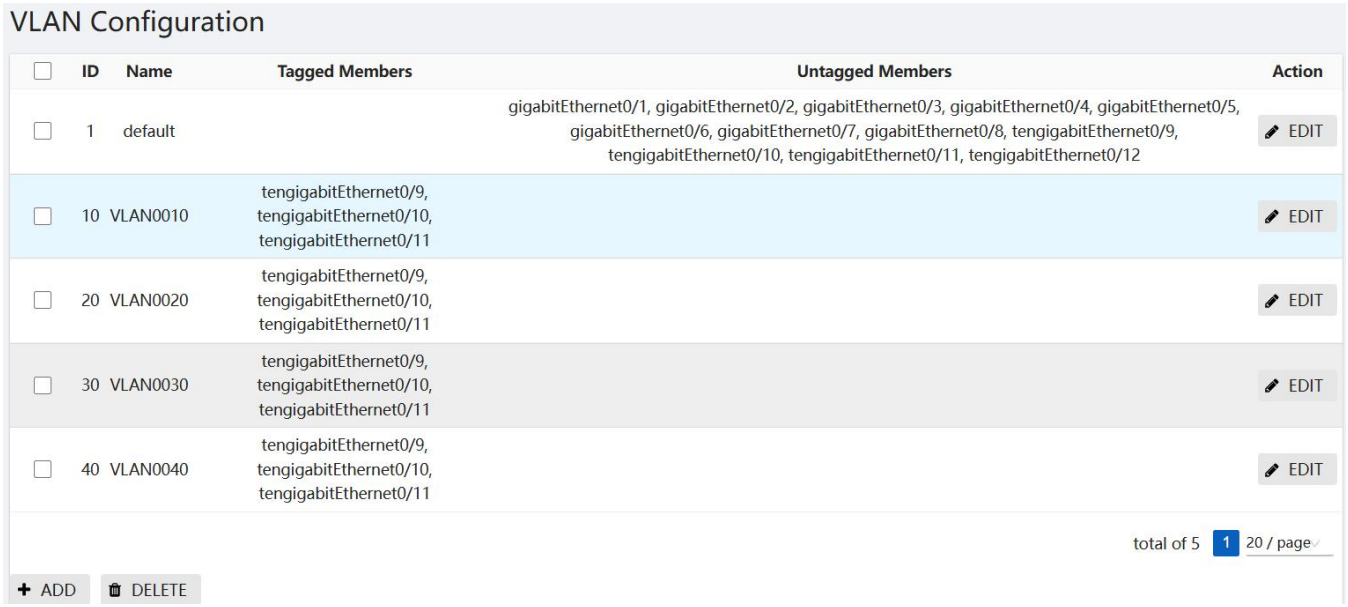
Step 5: Select the [Save] button on the navigation bar to save the configuration.

3.4.2.5 Configuring Switch D

Step 1: Referring to Swtich A, configure ports 9, 10, and 11 as trunk ports, and the Native Vlan as default value 1.

Step 2: Create VLANs 10, 20, 30, and 40, and add the corresponding ports to the VLANs as shown in the figure.

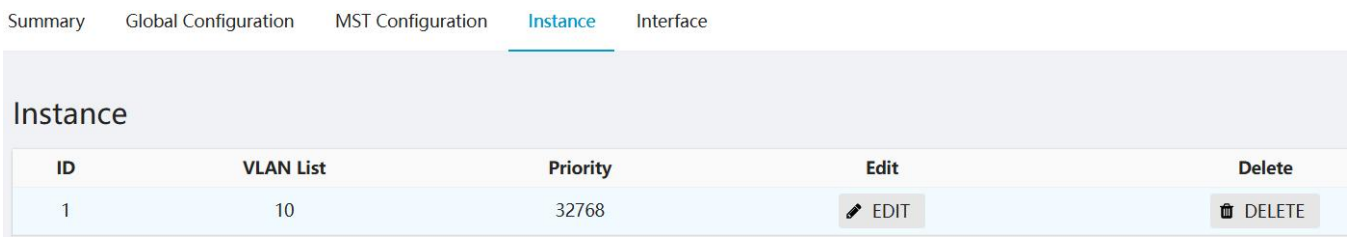
Figure 4-80 VLAN Status Display Screen



Step 3: Select [Exchange] ⇨ [Spanning Tree], click the [Instance] tab, and then click the [Add] button, as shown in the following figure, with ID "1".

VLAN list is "10", use the default parameters for priority, and click the [Apply] button to save the configuration.

Figure 4-81 Spanning Tree Instance Display Screen



Step 5: Select the [Save] button on the navigation bar to save the configuration.

4.6 MAC Management

4.6.1 summarize

The Ethernet switch queries the MAC address table by parsing the destination MAC address carried by the message and sends the message to the corresponding port. the MAC address table records the MAC addresses, interfaces, and VLAN IDs of the devices connected to the device.The Ethernet switch decides whether to use the forwarding method of known-moncast or unknown broadcast according to the result of the MAC address table lookup.

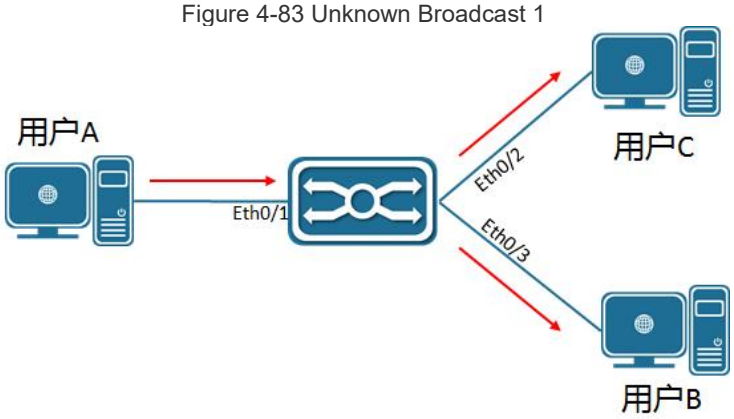
Known-unknown broadcast: The Ethernet switch finds a table entry in the MAC address table that corresponds to the destination MAC address and VLAN ID of the message, and the output port in the table entry is unique, so the message is directly output from the port corresponding to the table entry.

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

The MAC address of the Ethernet switch can be dynamically acquired or statically configured, and it is generally obtained through dynamic acquisition.The following gives the working principle of dynamic learning of MAC address by analyzing the interaction process between user A and user C.

As shown in Figure 4-83, User A sends a message to the port GigabitEthernet 0/1 of the switch, and at this time 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 sends the message to all ports belonging to VLAN 1 except GigabitEthernet 0/1 connecting to user A by broadcasting, including the ports of user B and user C. At this time, user B is able to receive the message sent by user A that does not belong to it.

Figure 4-83 Unknown Broadcast 1



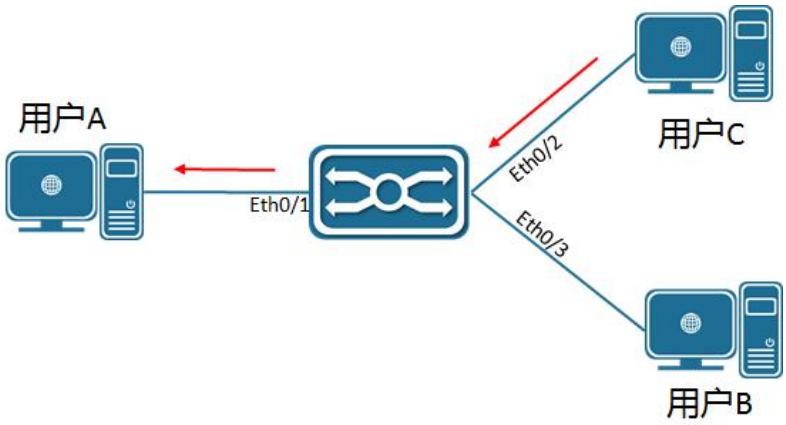
The current dynamic MAC address table information is shown in Table 4-84:

Table 4-84 Device Parameter List

subscribers	VLAN	MAC address	ports
User A	1	000E.C6C1.C8AB	GigabitEthernet 0/1

As shown in Figure 4-85, user B receives the message and sends the response message to user A through the Ethernet switch's port GigabitEthernet 0/2. At this time, user A's MAC address already exists in the Ethernet switch's MAC address table, and the message is forwarded to the GigabitEthernet 0/1 port in a unicast manner, while the Ethernet switch willAt the same time, the Ethernet switch will learn the MAC address of user C. The difference with the previous one is that user B cannot receive the message sent from user C to user A at this time.

Figure 4-85 Unknown Broadcast 2



The current dynamic MAC address table information is shown in Table 4-86:

Table 4-86 Device Parameter List

subscribers	VLAN	MAC address	ports
User A	1	000E.C6C1.C8AB	Gigabit Ethernet 0/1
User C	1	000E.C6C1.C8AD	Gigabit Ethernet 0/2

After an interaction process between user A and user C, the device learns the source MAC addresses of user A and user C. After that, the message interaction between user A and user C is forwarded in unicast mode, and user B will no longer receive the interactive message between user A and user C.

4.6.2 Configure the MAC address

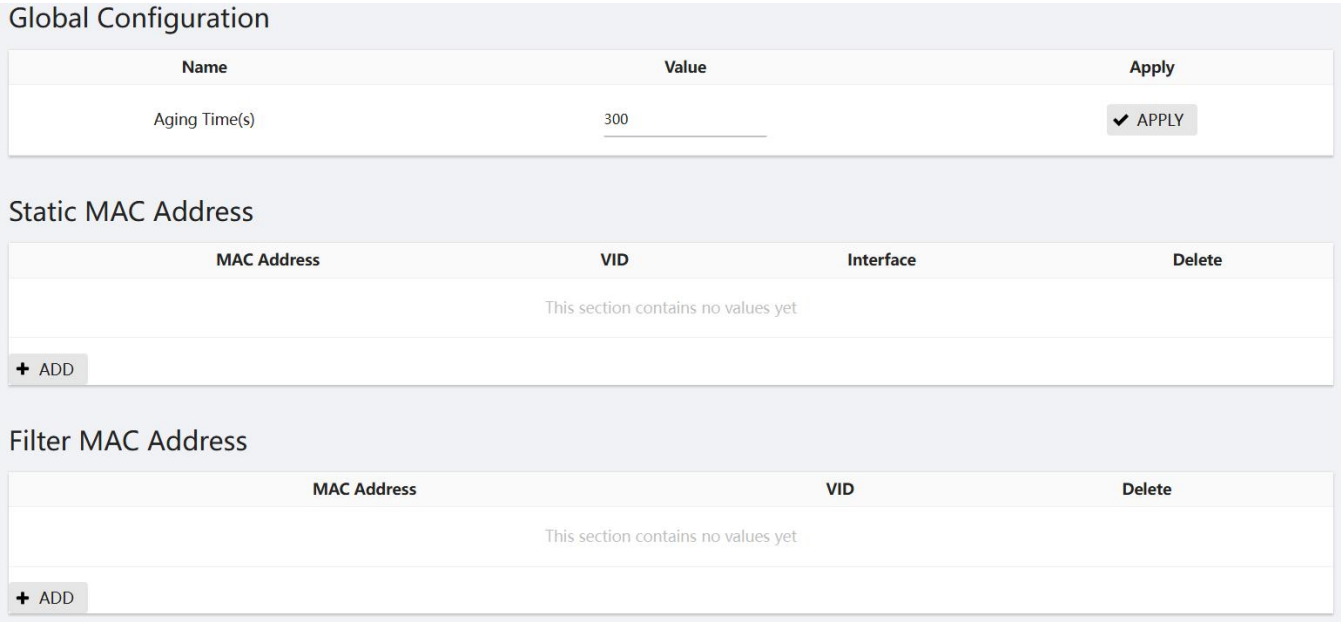
MAC address table entries are categorized into: static MAC address table entries, dynamic MAC address table entries, and filtered MAC address table entries.

Static MAC address table entries: Configured manually by the user, the table entries do not age.

Dynamic MAC address table entries: Including user-configured and those learned by the device through the source MAC address, the table entries have an aging time.

Filter MAC Address Table Entry: Used to discard messages containing a specific MAC address (e.g., a user can be blocked from receiving messages for security reasons), manually configured by the user, and the table entry does not age.

Figure 4-87 MAC placement interface



Select [Switching] [MAC Configuration] in the navigation bar to enter the MAC configuration interface, as shown in Figure 4-87, and each parameter of MAC configuration is shown in Table 4-88.

Table 4-88 Description of MAC Address Management Parameters

configuration item		clarification
global configuration	aging time	<30,1000>, the default aging time is 300 seconds, and the MAC address is systematically aged within the last update time range of 300 to 600 seconds
	appliance	Click Configure to take effect
static address (computing)	MAC address	Configured static MAC address in the format of 00-00-00-00-00-01
	VID	vlan attribute of the MAC address
	connector	Port Attributes for MAC Addresses
	manipulate	Click to delete this static MAC address
filtered address	MAC address	Configure the filtering MAC address in the format such as: 00-00-00-00-00-01
	VID	vlan attribute of the MAC address
	manipulate	Click to remove this filtered MAC address

4.6.3 MAC Address Configuration Example

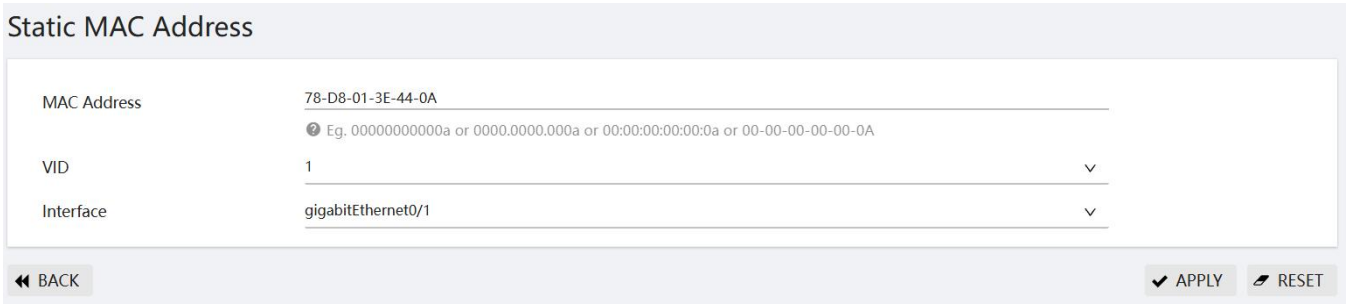
Configuration Example:

Case requirements: All messages with destination MAC address 000E.C6C1.C8AB, VLAN 1 are forwarded from port GigabitEthernet 0/1, while messages with MAC address 000E.C6C1.C8CC, VLAN 10 are filtered.

Step 1: Create a static MAC address, MAC: 000E.C6C1.C8AB, VLAN 1, port GigabitEthernet 0/1.

Select [Switching] [MAC Configuration] in the navigation bar to enter the MAC address configuration interface, click the [Add] button under "Static Address" to enter the static address addition interface, as shown in Figure 4-89, and configure the MAC address, VID, and interface in turn.

Figure 4-89 Static Address Configuration



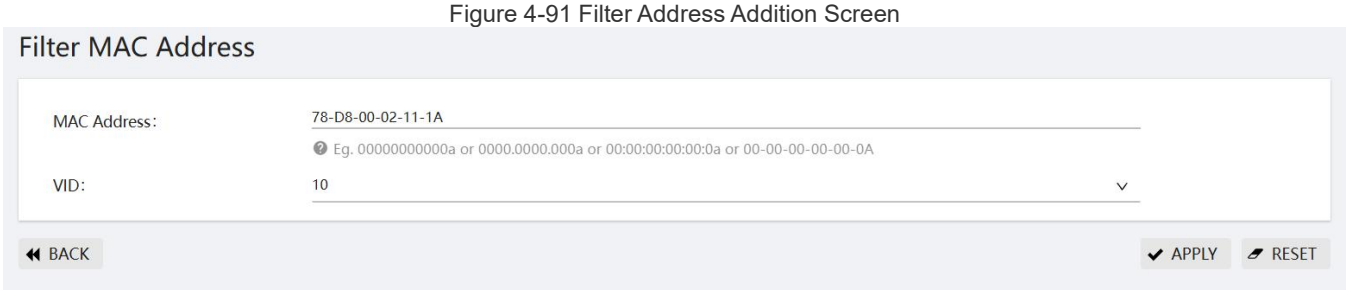
Click the [Confirm] button to complete the configuration and return to the interface as shown in Figure 4-90.

Figure 4-90 Static Address Display

Step 2: Create a filter MAC address, MAC: 000E.C6C1.C8CC,VLAN10

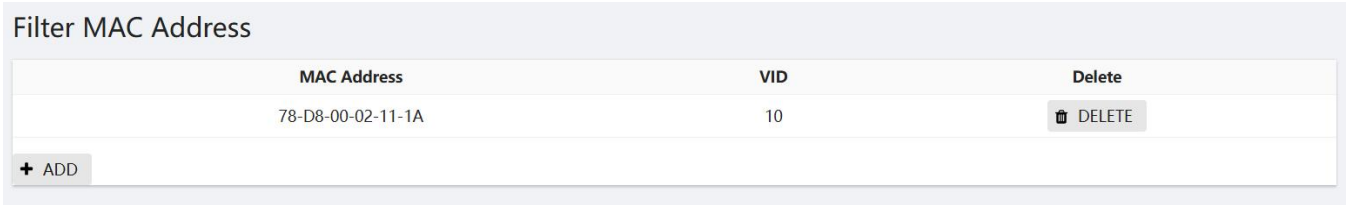
Select [Switching] [MAC Configuration] in the navigation bar to enter the MAC address configuration interface, click the [Add] button under "Filter Address" to enter the filter address addition interface, as shown in Figure 4-91, configure the MAC address and VID in turn.

Figure 4-91 Filter Address Addition Screen



Click the [Confirm] button to complete the configuration, return to the interface as shown in Figure 4-92

Figure 4-92 Static Address Display



Step 3: Click the [Save] button on the navigation bar to save the configuration.

4.7 LLDP

4.7.1 summarize

4.7.1.1 LLDP Context in which it arose

At present, the increasing variety of network devices and their respective configurations are intricate, in order to enable devices from different vendors to discover each other in the network

and interact with each other's system and configuration information, there is a need for a standard information exchange platform.

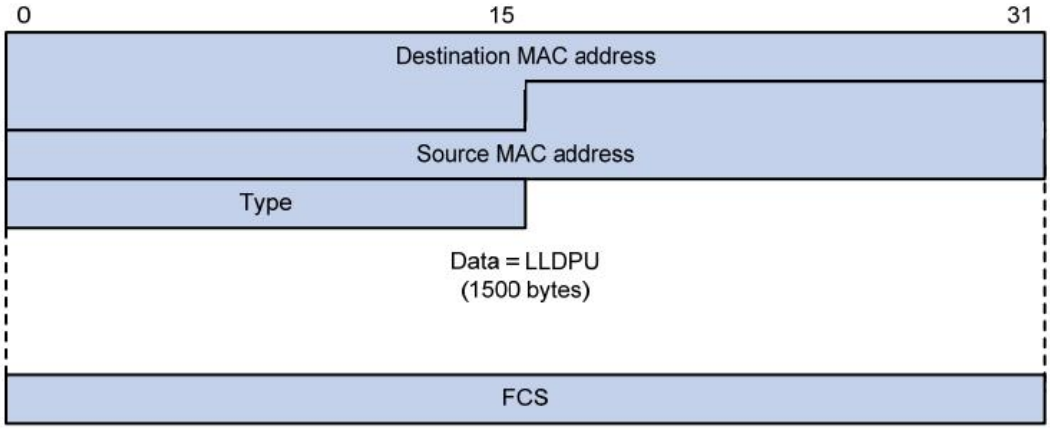
LLDP (Link Layer Discovery Protocol) is produced in such a background, it provides a standard link layer discovery method, can be the end of the device's main capabilities, management address, device identification, interface identification and other information is organized into different TLV (Type/Length/Value), and encapsulated in a TLV (Type/Length/Value)./Length/Value), and encapsulated in LLDPDU (Link Layer Discovery Protocol Data Unit) released to their directly connected neighbors, the neighbors receive this information will be in the standard MIB (Management Information Base) of theThe neighbor receives this information and saves it in the form of a standard MIB (Management Information Base) for the network management system to query and judge the communication status of the link.

4.7.1.2 LLDP basic concept

1. LLDP telegram

A message encapsulated with an LLDPDU is called an LLDP message and has two encapsulation formats: Ethernet II and SNAP (Subnetwork Access Protocol).

Figure 4-93 Ethernet II Format Encapsulated LLDP Message



(1) LLDP Message Encapsulated in Ethernet II Format

As shown in Figure 4-93, it is an LLDP message encapsulated in Ethernet II format, and the meanings of the fields are as follows:

-Destination MAC address: destination MAC address, a fixed multicast MAC address 0x0180-C200-000E.

-Source MAC address: source MAC address, which is the port MAC address.

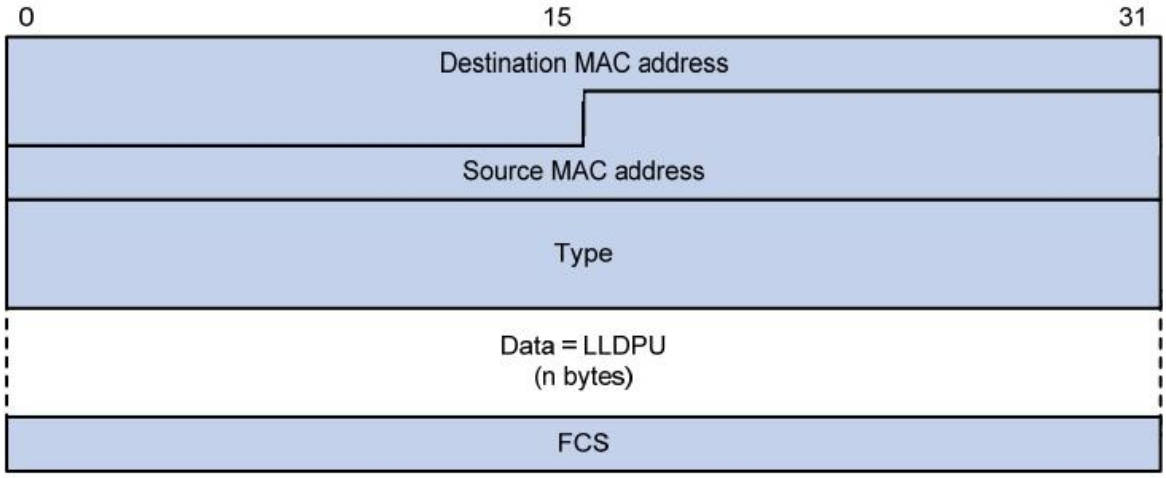
-Type: message type, 0x88CC.

-Data: data content, it is LLDPDU.

-FCS: Frame Check Sequence, used to verify the message.

(2) LLDP message encapsulated in SNAP format

Figure 4-94 LLDP Message Encapsulated in SNAP Format



As shown in Figure 4-94, it is an LLDP message encapsulated in SNAP format, in which the meanings of the fields are as follows:

-Destination MAC address: destination MAC address, which is the fixed multicast MAC address 0x0180-C200-000E.

-Source MAC address: source MAC address, either the port MAC address or the device bridge MAC address (if there is a port address, use the port MAC address, otherwise use the device bridge MAC address).

-Type: message type, 0xAAAA-0300-0000-88CC.

-Data: data content, as LLDPDU.

-FCS: Frame Check Sequence, used to verify the message.

2. LLDPDU

LLDPDU is the data unit encapsulated in the data part of LLDP message.Before forming an LLDPDU, the device encapsulates the local information into TLV format, and then several TLVs are combined to form an LLDPDU encapsulated in the data part of the LLDP message for transmission.

Figure 4-95 Encapsulation Format for LLDPDUs

As shown in Figure 4-95, the four TLVs, Chasis ID TLV, Port ID TLV, Time To Live TLV, and End of LLDPDU TLV, in dark blue, are required to be carried by every LLDPDU, and the remaining TLVs are carried optionally.Each LLDPDU can carry up to 28 TLVs.

2. TLV

TLVs are the units that make up an LLDPDU, and each TLV represents a piece of information.The TLVs that LLDP can encapsulate include basic TLVs,

802.1 organization-defined TLVs, 802.3 organization-defined TLVs, and LLDP-MED (Media Endpoint Discovery) TLVs.

Basic TLVs are a set of TLVs that are the basis of network device management, while 802.1 organization-defined TLVs, 802.3 organization-defined TLVs, and LLDP-MED TLVs are TLVs defined by

standards organizations or other agencies to enhance the management of network devices, which can be sent or not sent in LLDPDUs according to the actual needs.

(1) Basic TLV

Among the basic TLVs, there are several TLVs that are mandatory for the implementation of LLDP functionality, i.e., they must be published in the LLDPDU, as shown in Table 4-1.

Table 4-96 Basic TLVs

TLV Name	clarification	Whether it must be published
Chassis ID	Bridge MAC address of the sending device	yes
Port ID	Identifies the port at the sending end of the LLDPDU. If the LLDPDU carries an LLDP-MED TLV, its content is the MAC address of the port, and the bridge MAC is used when there is no port MAC; otherwise, its content is the Name of the port	yes
Time To Live	Survival time of this device's information on neighboring devices	yes
End of LLDPDU	The end identifier of the LLDPDU, which is the last TLV of the LLDPDU.	yes
Port Description	Description of the port	no
System Name	Name of the equipment	no
System Description	Description of the system	no
System Capabilities	The main functions of the system and the enabled functional items	no
Management Address	Management address, as well as the interface number and OID (Object Identifier) that corresponds to the change of address	no

(2) 802.1 Organizational Definitions TLV

The IEEE 802.1 organization defines TLVs as shown in Table 4-97.

Table 4-97 TLVs defined by the IEEE 802.1 organization

TLV name	clarification
Port VLAN ID	PVID (Port VLAN ID) of the port, one LLDPDU carries more than one TLV of this type.
Port And Protocol VLAN ID	The PPVID (Port and Protocol VLAN ID) of the port, an LLDPDU can carry multiple non-repeating TLVs of this type in a single
VLAN Name	The name of the VLAN to which the port belongs, and an LLDPDU can carry multiple non-duplicated TLVs of this type.
Protocol Identity	The type of protocol supported by the port, an LLDPDU can carry multiple non-duplicated TLVs of this type.

DCBX	（Data Center Bridging Exchange Protocol）

(3) 802.3 Organizational Definitions TLV

The IEEE 802.3 organization defines TLVs as shown in Table 4-98

Table 4-98 TLVs defined by the IEEE 802.3 organization

TLV Name	clarification
MAC/PHY Configuration/Status	Rate and duplex status supported by the port, whether port rate auto-negotiation is supported, whether auto-negotiation is enabled, and current rate and duplex status
Power Via MDI	The power supply capability of the port, including the type of POE (Power over Ethernet) (PSE (Power Sourcing Equipment) or PD (Powered Device)), the remote power mode of the POE port, and whether PSE power is supported, whether PSE power is enabled and whether the power supply method is controllable.
Link Aggregation	Whether the port supports link aggregation and whether link aggregation has been enabled
Maximum Frame Size	The maximum frame length supported by the port is taken from the port's configured MTU (Maximum Transmission Unit.). Maximum Transmission Unit (MTU)
Power Stateful Control	Power state control of the port, including the type of power supply used by the PSE/PD, the priority of supplying/receiving power to the and power supplied/received

clarification

Our products do not support POE-related parts of the TLV for the time being.

(3)LLDP-MED TLV

LLDP-MED TLV provides many advanced applications for VoIP (Voice over IP, transmitting voice over IP networks), including basic configuration, network policy configuration, address information, and directory management, which meets the requirements of different manufacturers of voice equipment in terms of cost-effectiveness, ease of deployment, and ease of management, and solves the problem of deploying voice equipment in Ethernet.It provides convenience for producers, sellers, and users of voice devices.The contents of LLDP-MED TLV are shown in Table 4-99.

4-99 LLDP-MED TLV

TLV Name	clarification
LLDP-MED Capabilities	Types of LLDP-MED TLVs supported by network devices
Network Policy	VLAN type and VLAN ID of the port on the network device or terminal device, as well as Layer 2 and Layer 3 and specific application types, related priorities, etc.
Extended Power-via-MDI	Extended power capability for network devices or end devices to Power Via MDI TLVs

Hardware Revision	Hardware version of the end device
Firmware Revision	Firmware version of the end device
Software Revision	Software version of the terminal device
Serial Number	Serial number of the terminal device
Manufacturer Name	Name of the manufacturer of the terminal equipment
Model Name	Module name of the terminal device
Asset ID	Asset identifiers for end devices for catalog management and asset tracking
Location Identification	Location identification information of network devices for use by end devices in location-based applications

clarification

Our products do not support VoIP-related parts of TLV for the time being.

(4)Management address

An administrative address is an address that is used by the network management system to identify a network device and manage it. A management address clearly identifies a device, which facilitates the drawing of the network topology and facilitates network management. The management address is encapsulated in the Management Address TLV of the LLDP message and released to the public.

4.7.1.3 LLDP Working mechanisms

1. LLDP operating mode

LLDP has the following four modes of operation:

-TxRx: Both sending and receiving LLDP messages.

-Tx: Sends and does not receive LLDP messages.

-Rx: Receive and not send LLDP messages.

-Disable: Neither send nor receive LLDP messages.

When the LLDP operation mode of the port is changed, the port will initialize the protocol state machine. In order to avoid frequent changes in the port operating mode that cause the port to perform initialization operations continuously, you can configure the port initialization delay time, so that the initialization operation is delayed for a certain period of time when the port operating mode is changed.

2.Mechanisms for sending LLDP messages

When the port is operating in TxRx or Tx mode, the device periodically sends LLDP (Link Layer Discovery Protocol) packets to neighboring devices. If there is a change in the device's local configuration, it immediately sends an LLDP packet to notify neighboring devices of the change in local information as soon as possible. However, to prevent a large number of LLDP packets from being sent due to frequent changes in local information, a delay is required after each LLDP packet is sent before the next packet can be transmitted.

When the device's operating mode switches from Disable/Rx to TxRx/Tx, or when a new neighboring device is discovered (i.e., a new LLDP packet is received and the local device has not yet saved information about the device that sent the packet), the device will automatically enable the fast transmission mechanism. This mechanism shortens the LLDP packet transmission cycle to 1 second and sends a specified number of LLDP packets consecutively before restoring the normal transmission cycle.

3. LLDP Mechanisms for receiving messages

When the port is working in TxRx or Rx mode, the device checks the validity of the received LLDP message and the TLV it carries, passes the check and then saves the neighbor information locally, and sets the aging time of the neighbor information on the local device based on the value of the TTL (Time to Live) in the Time To Live TLV, and if the value is zero, then it immediatelyaging the neighbor information immediately.

4.7.2 LLDP in place

4.7.2.1 LLDP Configuration Task Profile

move	Configuration tasks	clarification
1	Configuring the Global LLDP Function	Set the enable global LLDP function and configure the global parameters of LLDP The global LLDP function is disabled by default, mandatory.
2	Configuring Port LLDP Parameters	Configure the parameters related to the LLDP function of the port, including: the LLDP administrative state, Chassis Subtype, Port ID Subtype, Management Address Subtype, and the type of TLVs allowed to be issued, optional.
3	Viewing Port Information	View LLDP local information, neighbor information, statistics and status information for the specified port, optional
4	View Statistics	View global LLDP local information and statistics, optional
5	View Neighborhood Information	View global LLDP neighbor information, i.e., LLDP information received from a neighbor that groups the information neighbor sends these messages to the current device as TLVs, optional

4.7.2.2 Configuring the Global LLDP Function

Select [Switching] [LLDP Configuration] in the navigation bar to enter the LLDP configuration interface, as shown in Figure 4-100, and the detailed parameters are shown in Table 4-101.

Figure 4-100 LLDP Global Configuration

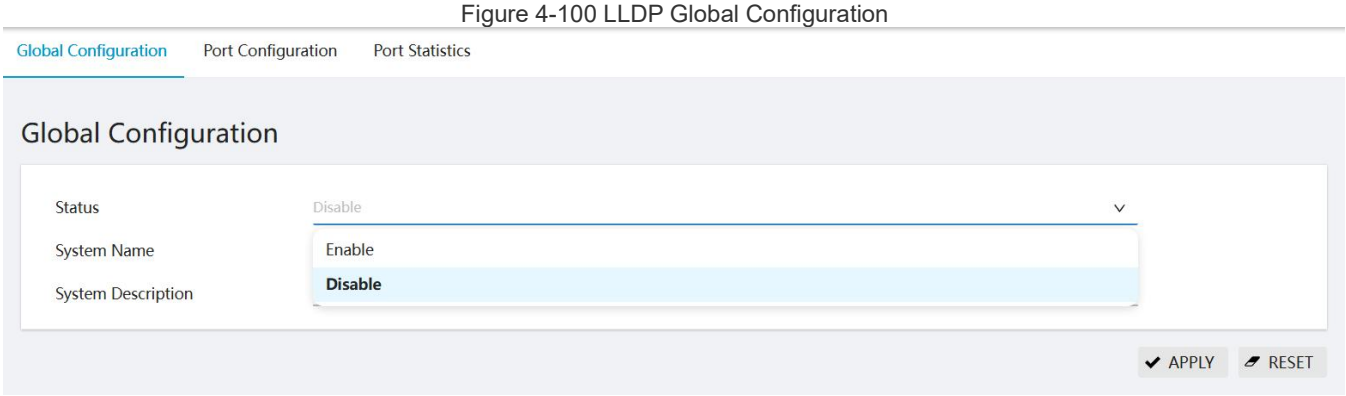


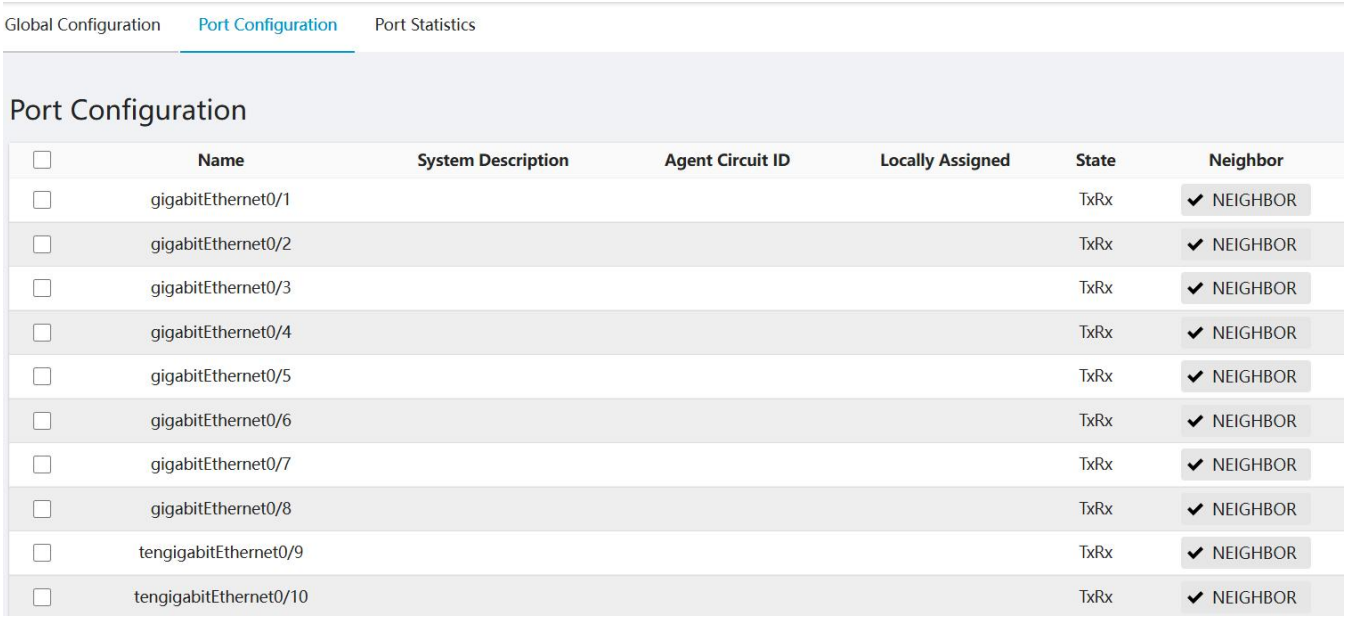
Table 4-101 LLDP Global Configuration Parameter Descriptions

configuration item	clarification
state of affairs	Disabled:Global enable disable Enabled:Global Enabled
system name	Name of the device, can be empty
system description	Description of the system, can be empty

4.7.2.3 Configuring Port LLDP Parameters

Step 1: In the current interface, click the "Port Configuration" tab in the upper-right corner to enter the LLDP port configuration overview interface, as shown in Figure 4-102.

Figure 4-102 LLDP Port Configuration Overview



Step 2: Check the ports that need to be configured, slide down and click the [Edit] button to enter the port detailed configuration interface, as shown in Figure 4-103, and the detailed parameters of the port configuration are shown in Table 4-104.

Figure 4-103 LLDP Port Detailed Configuration Screen

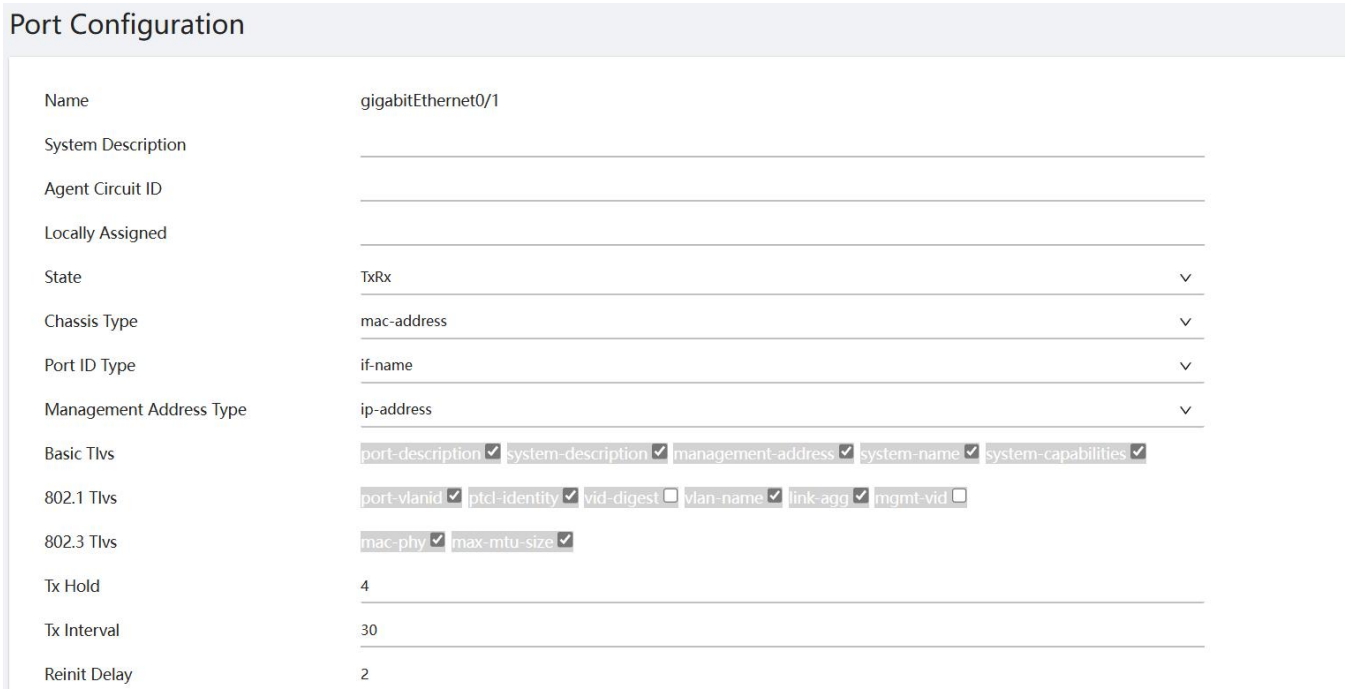


Table 4-104 Description of LLDP Port Configuration Parameters

configuration item	clarification
state of affairs	Disabled: neither send nor receive LLDPDUs TxOnly: only send and not receive LLDPDUs RxOnly: only receive and not send LLDPDUs TxRx: both send and receive LLDPDUs
Chassis Subtype	Mac-address: indicates the MAC address. If-alias: indicates the interface alias. If-name: interface name Ip-address: the IP address. Locally-assigned: Indicates the local configuration.
descriptive	Displays the name of the currently configured LLDP port
Agent Circuit ID	Proxy Circuit Logo
Locally Assigned	local configuration
Port ID Subtype	Mac-address: Indicates the MAC address If-alias: Indicates the interface alias If-name: Interface name Ip-address: Indicates the IP address Agt-circuit-id: Proxy circuit ID Locally-assigned: Indicates local configuration
Management Address Subtype	Mac-address:device MAC address Ip-address:device IP address
Basic Tlvs	port-description:port-descriptor system-description:system descriptor management-address:management-address system-name:system name system-capabilities:system capabilities

802.1 Tlvs	port-vlanid:port vlanid ptcl-identity:protocol-id vid-digest:vid digest vlan-name:vlan name port-ptcl-vlanid:port protocol vlanid link-agg mgmt-vid:link-aggregation mgmt-vid
802.3 Tlvs	mac-phy:mac-phy max-mtu-size:max-mtu value
Tx hold	Transmission hold, default value txFastInit is 4, used for message TTL calculation; TTL = msgTxInterval * msgTxHold + 1
Tx interval	Transmission interval, the default value is 30 s; the administrator can change this value to any value between 5 and 3600.
Reinit delay	Indicates the amount of delay between when adminStatus becomes "disabled" and when it tries to reinitialize. The default value of reinitDelay is 2 s.。
Fast tx	Defines the time interval between timer intervals during a fast transmission cycle (i.e., txFast is not zero). The default value for msgFastTx is 1; the administrator can change this value to any value between 1 and 3600.
Tx fast init	This variable is used as the initial value of the txFast variable. This value determines the number of LLDPDUs transmitted during the fast transfer cycle.
Tx credit max	Configure the maximum value of txCredit.The default value is 5. The administrator can change this value to any value in the range of 1 to 10.

4.7.2.4 View Statistics

In the current interface, click the [Port Statistics] button on the upper right to enter the LLDP status interface, as shown in Figure 4-105, and the specific parameters are described as described in Table 4-106.

Figure 4-105 LLDP Statistical Information

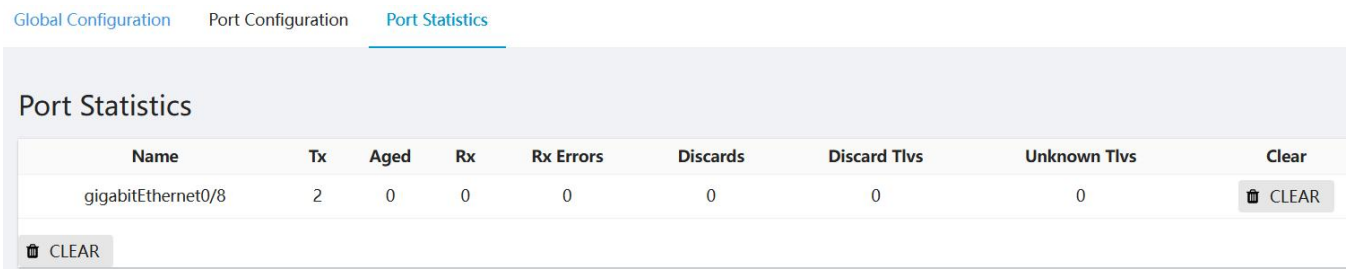


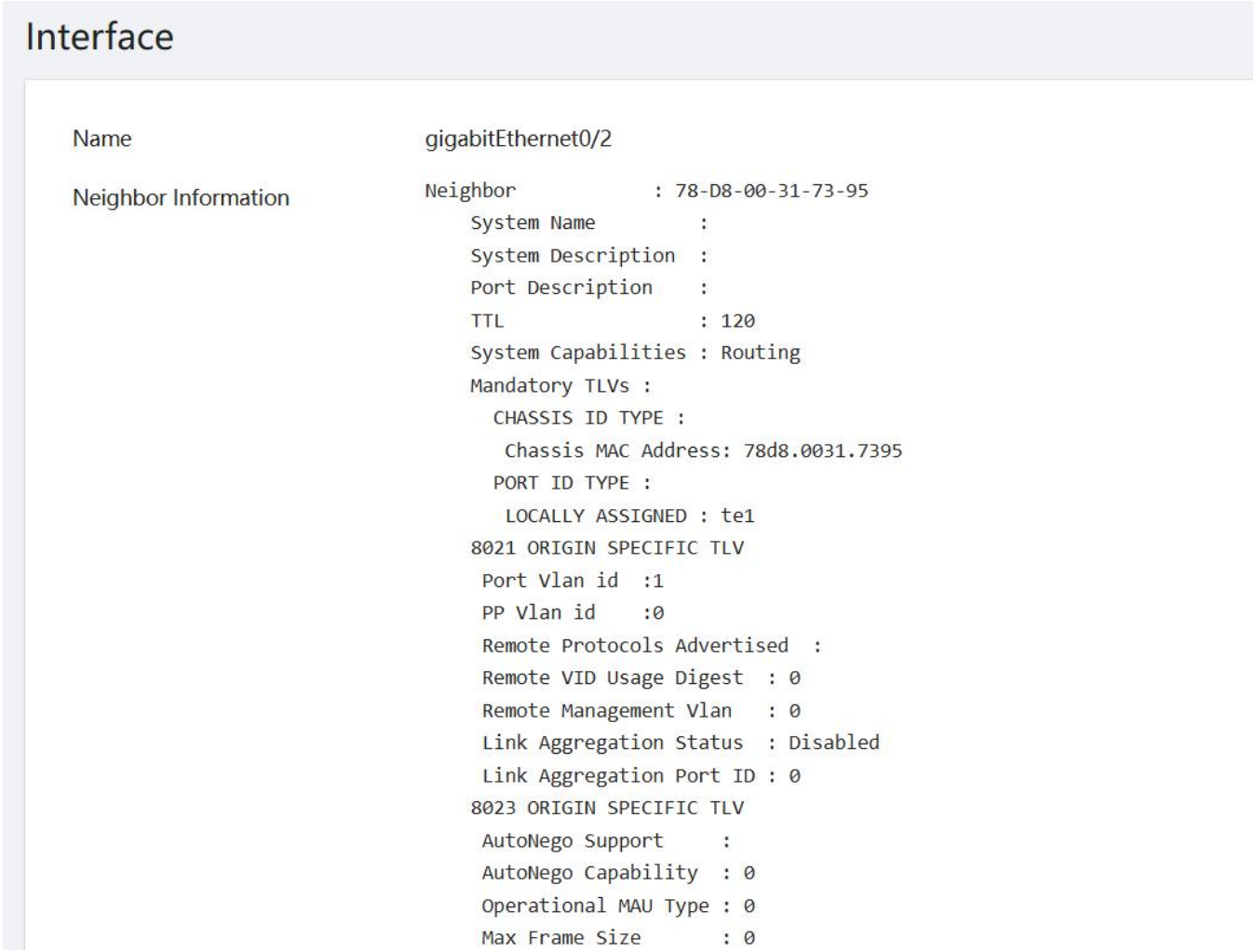
Table 4-106 Description of LLDP Port Configuration Parameters

configuration item	clarification
name	Display interface name
Tx	Number of messages sent
Aged	Number of aged messages
Rx	Number of messages received
Rx Errors	Number of reception errors
Discards	Number of messages discarded
Ddiscard Tlvs	Number of Tlv's discarded
Unknown Tlvs	Unknown Tlv number
removals	Clear current count

4.7.2.5 View Neighborhood Information

In the "Port" tab, click the "Neighbor" button of the corresponding port to enter the Neighbor Information Viewing Interface, as shown in Figure 4-107.

Figure 4-107 LLDP Neighbor Information



5 routing (in computer networks)

5.1 static route

A static route is a special type of route that is manually configured by the administrator.When the network structure is relatively simple, only static routes need to be configured to make the network work properly.

Static routes do not automatically adapt to changes in network topology.When the network fails or the topology changes, the configuration must be modified manually by the network administrator.

Viewing Static Route Configuration

Select [Routing] [Static Route] in the navigation bar to enter the static route configuration page, as shown in Figure 5-1.In the "Overview", you can display the configuration of static routes, and the description of each parameter is shown in Table 5-2.

Figure 5-1 Static Route Display Interface

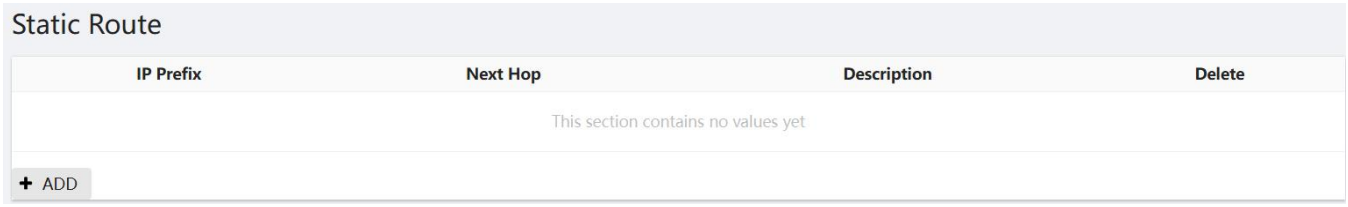


Table 5-2 Static Route Parameter Descriptions

configuration item	clarification
Route Type	Select the type of route, IPv4 and IPv6
prefix (linguistics)	Contains the route prefix address and segment length. Route prefix address, or route segment; for example, in the common route 0.0.0.0/0 192.168.1.1, the prefix IP is 0.0.0.0; route segment length; for example, in the above example, the length is 0
the next jump	Route the next hop address; for example, the next hop in the above example is 192.168.1.1
descriptive	Route description information, optional configuration

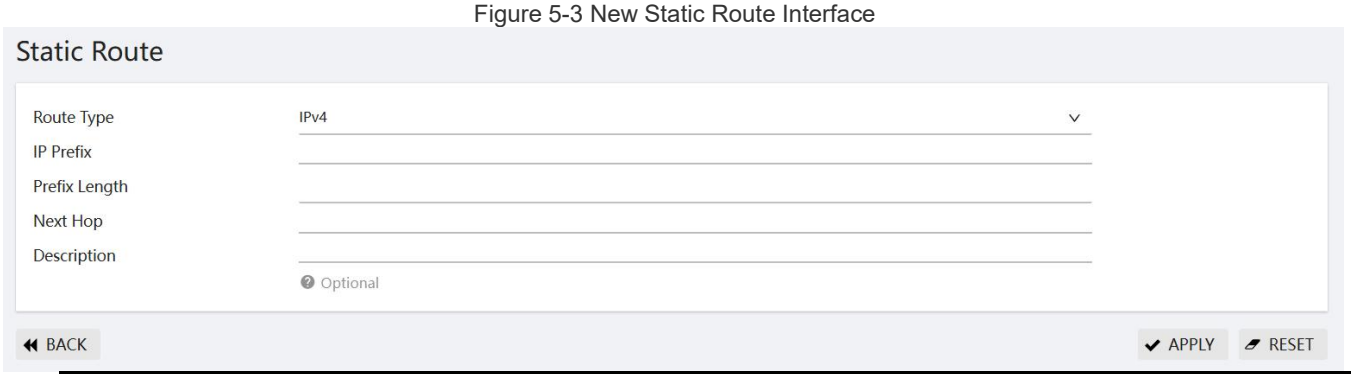
New Static Route Steps

(1) Select [Switching] [VLAN] in the navigation bar to create a VLAN and select Untagged member ports.

(2) Select [Routing] [Layer 3 Ports] [Port Configuration] in the navigation bar to add Layer 3 SVI ports.

(3) Select [Routing] [Static Route] in the navigation bar, as shown in Figure 5-3, to create a static route.

Figure 5-3 New Static Route Interface



attention

- When you add a new SVI port, the default management IP address is automatically removed. Make sure the new SVI port can continue to access the

5.2 ARP/Neighbor Configuration

5.2.1 summarize

ARP(Address Resolution Protocol, Address Resolution Protocol) is a protocol that resolves IP addresses into Ethernet MAC addresses (or physical addresses).

In a LAN, when a host or other network device has data to send to another host or device, it must know the other party's network layer address (i.e., IP address). But an IP address is not enough, because IP data messages must be encapsulated into frames before they can be sent over a physical network, so the sending station must also have the physical address of the receiving station, so

a mapping from IP addresses to physical addresses is needed.ARP is the protocol that accomplishes this.

ARP

After the device resolves to the destination MAC address through ARP, it will add an IP address to MAC address mapping table entry in its own ARP table for subsequent forwarding of messages to the same destination.

ARP table entries are categorized into dynamic ARP table entries and static ARP table entries.

1.Dynamic ARP table entries

Dynamic ARP table entries are automatically generated and maintained by the ARP protocol through ARP messages and can be aged, updated by new ARP messages, and overwritten by static ARP table entries.The corresponding dynamic ARP table entries are deleted when the aging time is reached and the interface is down.

2.Static ARP table entries

Static ARP table entries are configured and maintained manually and are not aged out and overwritten by dynamic ARP table entries.

Configuring static ARP table entries increases the security of communications.Static ARP table entries can restrict the communication with the device with the specified IP address to use only the specified MAC address, in which case the attack packets cannot modify the mapping relationship between the IP address and the MAC address of the table entry, thus protecting the normal communication between this device and the specified device.

5.2.2 Configuring ARP Management

Viewing ARP Table Entries

Select [Routing] [ARP/Neighbor Information] in the navigation bar to enter the ARP/Neighbor Information page, as shown in Figure 5-4.You can see the ARP/neighbor table entry information in "Overview", and the description of each parameter is shown in Table 5-5.

Figure 5-4 ARP/Neighbor Table Entry Information

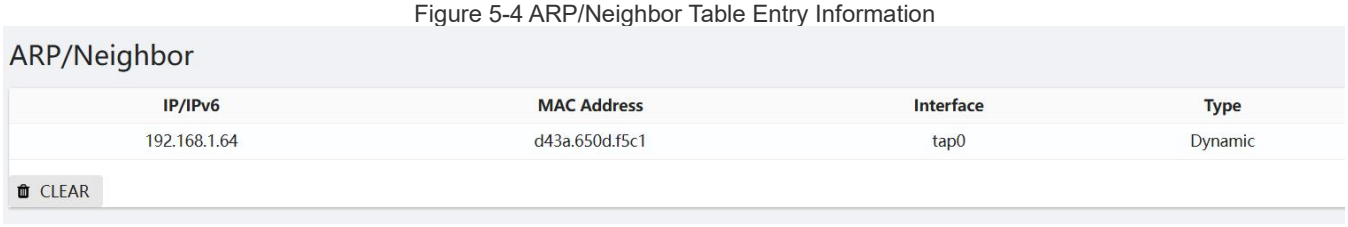


Table 5-5 ARP Table Entry Parameter Descriptions

configuration item	clarification
IPv4/IPv6	Terminal IPv4/IPv6 address
MAC address	terminal MAC address

interface	The name of the Layer 3 interface where the terminal is located
typology	ARP address type

Configure ARP table entries

(1) Select [Routing] [ARP/Neighbor Information] [Configuration] in the navigation bar to enter the ARP/Neighbor Configuration interface, as shown in Figure 5-6.

(2) Click the [Add] button to enter the ARP/neighbor creation interface, as shown in Figure 5-7;

(3) Click the [Apply] button to complete the operation.

Figure 5-6 ARP/Neighbor Configuration Interface

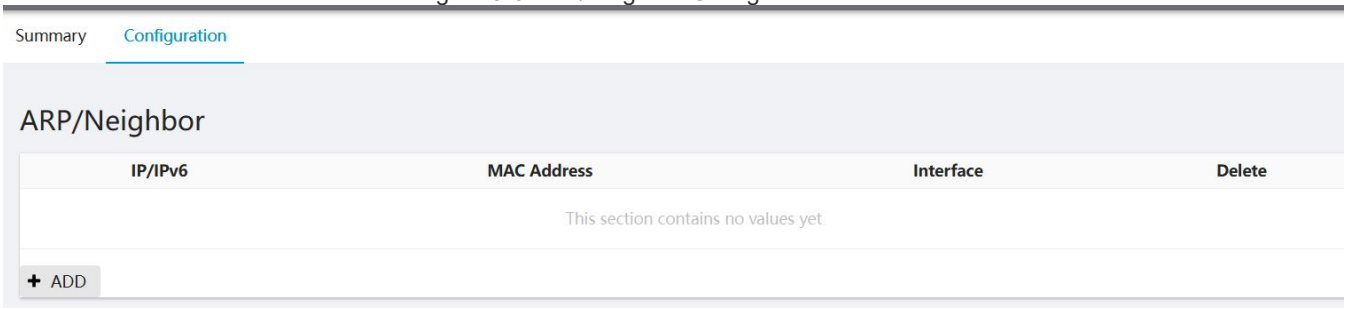
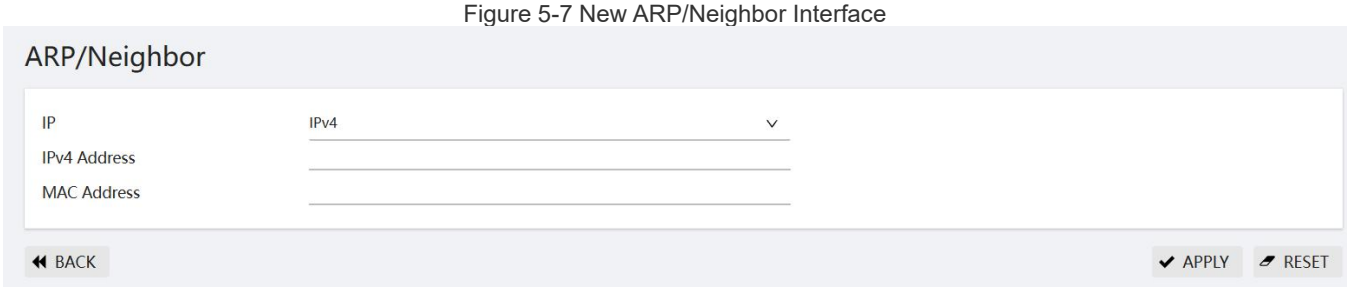


Figure 5-7 New ARP/Neighbor Interface



5.2.3 Example of Configuring ARP

1. Networking Requirements

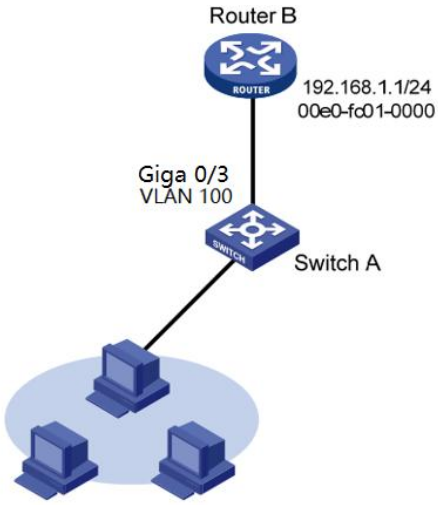
As shown in Figure 5-8:

-Switch A is connected to the host and Router B is connected via interface GigabitEthernet 0/3, which belongs to VLAN 100.

-Router B has an IP address of 192.168.1.1/24 and a MAC address of 00e0-fc01-0000.

To increase the security of communication between Switch A and Router B, you can configure a static ARP table entry on Switch A.

Figure 5-8 Static ARP Configuration Network Diagram



2. Configuration steps

(1) Create VLAN 100 and configure port GigabitEthernet 0/3 VLAN 100.

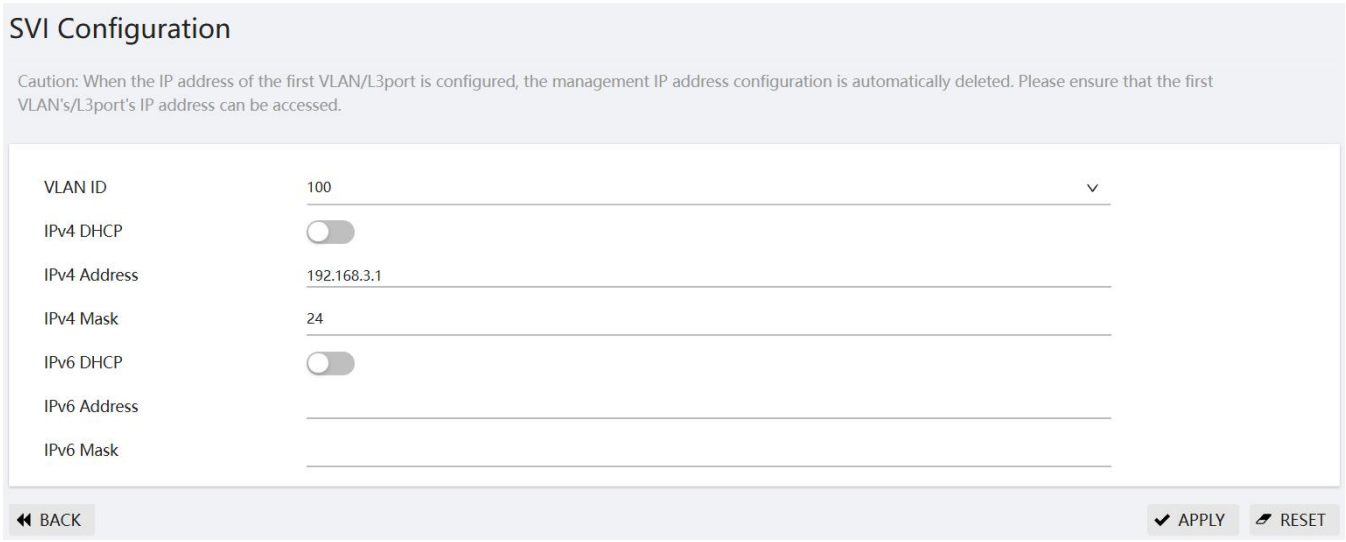
Select [Switching] [VLAN] to enter the VLAN configuration interface. In the VLAN configuration page, click the [Add] button to create VLAN 100 and select port GigabitEthernet 0/3 as the Untagged member port, as shown in Figure 5-9.

Figure 5-9 New VLAN100 Interface

(2) Creating Layer 3 SVI ports

Select [Routing] [Layer 3 Port] to enter the Layer 3 Port Configuration interface, click the [Add] button to configure the VLAN ID, Ipv4 address/mask, as shown in Figure 5-10, and click the [Apply] button to complete the configuration.

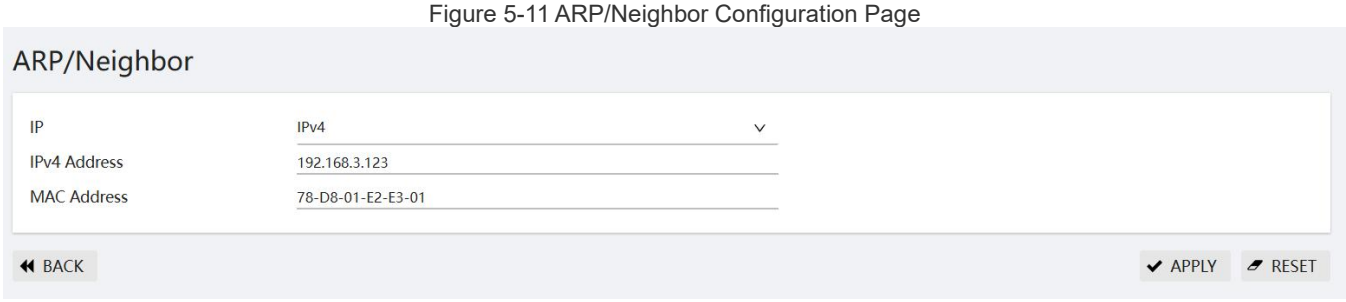
Figure 5-10 Creating a Layer 3 SVI Port



(4) Configure Router B for static ARP

Select [Advanced] [Layer 3] [ARP/Neighbor Configuration] in the navigation bar to enter the ARP/Neighbor Configuration interface, click the [Add] button to enter the configuration interface, configure the IP address and MAC address as shown in Figure 5-11, and click the [Confirm] button to complete the configuration.

Figure 5-11 ARP/Neighbor Configuration Page



6 surety

6.1 ACL

6.1.1 summarize

ACL（Access Control List，(Access Control List) realizes the function of packet filtering by configuring the matching rules and processing operations on the messages.It can effectively prevent illegal users from accessing the network, and at the same time control the traffic and save network resources.The packet matching rules defined by ACL can also be referenced by other functions that need to differentiate traffic, such as the definition of flow classification rules in QoS.

ACLs classify packets by a series of matching conditions, which can be the SMAC, DMAC, SIP, DIP, etc. of the packet.According to the matching conditions, ACLs can be categorized as follows:

IP-based standard ACL: Rules are formulated based on the source IP address of the packet only.

Extended IP-based ACLs: Rules are based on the source IP address, destination IP address, ETYPE, and protocol of the packet.

MAC-based ACLs: rules are formulated based on the source and destination MAC addresses of the packets.

IPV6-based ACLs: rules are formulated based on the source IPV6 address, destination IPV6 address, and protocol of the packet.

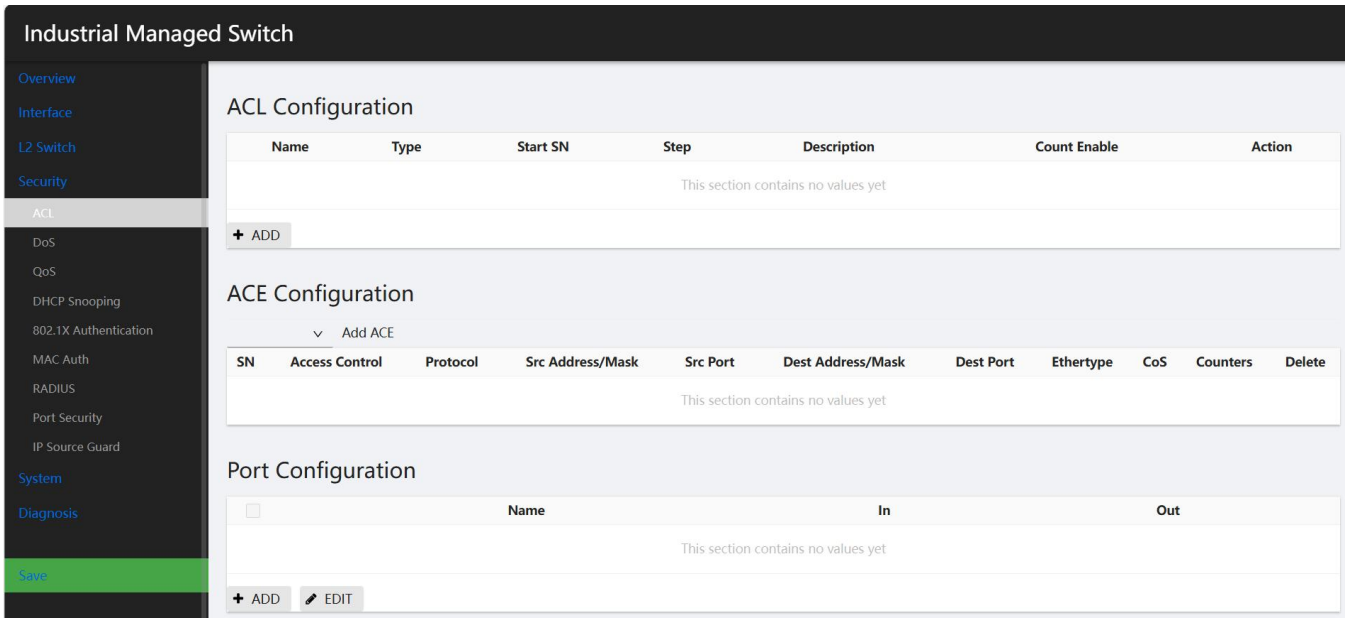
6.1.2 ACL deployment

clarification

- -Maximum 128 rules can be configured under a single ACL-ID; due to hardware resource limitation, the maximum number of application rules supported by a single device refers to the specific product specification document.
- When the ACL has been applied on the port, if you need to add or delete rules, you need to unapply them from the port first.。

Select [Security] [ACL] in the navigation bar to enter the ACL configuration interface, as shown in Figure 6-1, this page contains "ACL Configuration", "ACE Configuration", "Port Configuration", "Port Configuration", "Port Configuration", "Port Configuration", and "Port Configuration".This page contains "ACL Configuration", "ACE Configuration" and "Port Configuration".

Figure 6-1 ACL placement interface



Creating ACL Rules

The ACL module provides configuration based on ACL types, including IP, IP-Extend, IPV6, and MAC. The ACL configuration interface is shown in Figure 6-7~10, and the description of each parameter is shown in Table 6-2~6.

Table 6-2 ACL Type Parameter Descriptions

configuration item		clarification
ACL type	IP	ACL for standard IP that matches the source IP field in an IPv4 message
	IP-Extend	Extended ACL that matches protocol number, source IP address, destination IP

		address, Layer 4 port number, etc. of IPv4 packets
	IPV6	IPv6 ACL, Can match IPv6 message source IP address, destination IP address, protocol number, etc.
	MAC	MAC ACL, Can match fields such as destination MAC address, source MAC address, Etype, etc.
name		Standard IP Valid Numeric Range: <1-99> | <1300-1999> Extended IP valid numeric range: <100-199> | <2000-2699> MAC ACL valid numeric range: <200-699> | <200-299> IPv6 ACLs support string naming only, all ACLs support string naming, string length range <1-64>
counter enable		Enable the count function, when the message hits the ACL, the count value is added 1
Starting serial number		Rule table entry serial number start value, default:10, range <1-2147483647>
pacemaker		Serial number ground value added, default:10, range <1-2147483647>
descriptors		Define this ACL description information

Figure 6-7 ACL Type Configuration Interface

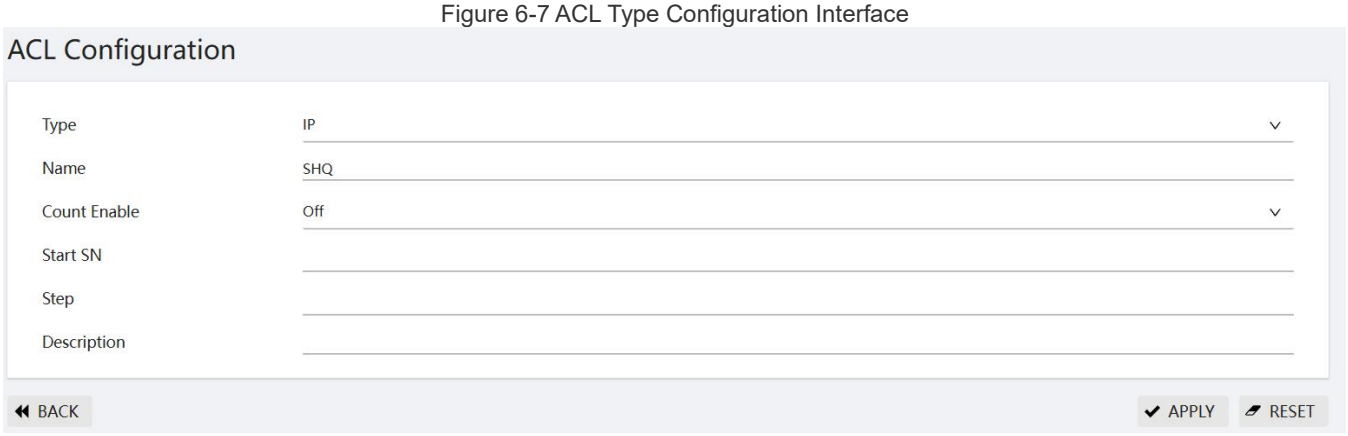


Table 6-3 ACL IP Type Parameter Descriptions

configuration item		clarification
access control	Permit	Release messages that hit this rule
	Deny	Discard messages that hit this rule
product key (software)		Rule table entry number
source address		Source IP address, e.g. 192.168.64.1
source mask		The mask of IP is inverted, such as matching the first 24 bits of the IP address, the mask is 255.255.255.0, here you need to configure to 00.00.00.255

Figure 6-8 IP Type ACE Configuration Interface

Table 6-4 IP-Extend Type ACE Parameter Descriptions

configuration item		instructions
access control	Permit	Release messages that hit this rule
	Deny	Discard messages that hit this rule
product key (software)		Rule table entry number
pact		Support common protocol options, including tcp, udp, vrrp, igmp, gre, ipcomp, ospf, pim, rsvp and so on. Supports all IPv4 messages Supports IPv4 messages with customized protocols.
source address		Source IP address, e.g. 192.168.64.1
source mask		The mask of IP is inverted, such as matching the first 24 bits of the IP address, the mask is 255.255.255.0, here you need to configure to 00.00.00.255
target address		Destination IP address, e.g. 192.168.64.100
target mask		homology mask

Figure 6-8 IP-Extend Type ACE Configuration Interface

Table 6-5 IPV6 Type ACE Parameter Descriptions

configuration item		clarification
access control	Permit	Release messages that hit this rule
	Deny	Discard messages that hit this rule
product key (software)		Rule table entry number

pact	Support common protocol options, including tcp, udp, icmp, etc. Supports all IPv6 messages Supports IPv6 messages with customized protocols.
source address	Source MAC address, such as 00.d0.f8.22.33.40
source mask	MAC address mask is reversed, such as matching the first 24 bits of the MAC address, the mask is ffff.ff00.0000, here you need to configure for 0000.00ff.ffff
target address	Destination MAC address, e.g. 00.d0.f8.22.33.41
target mask	homology mask

Figure 6-9 IPV6 Type ACE Configuration Interface

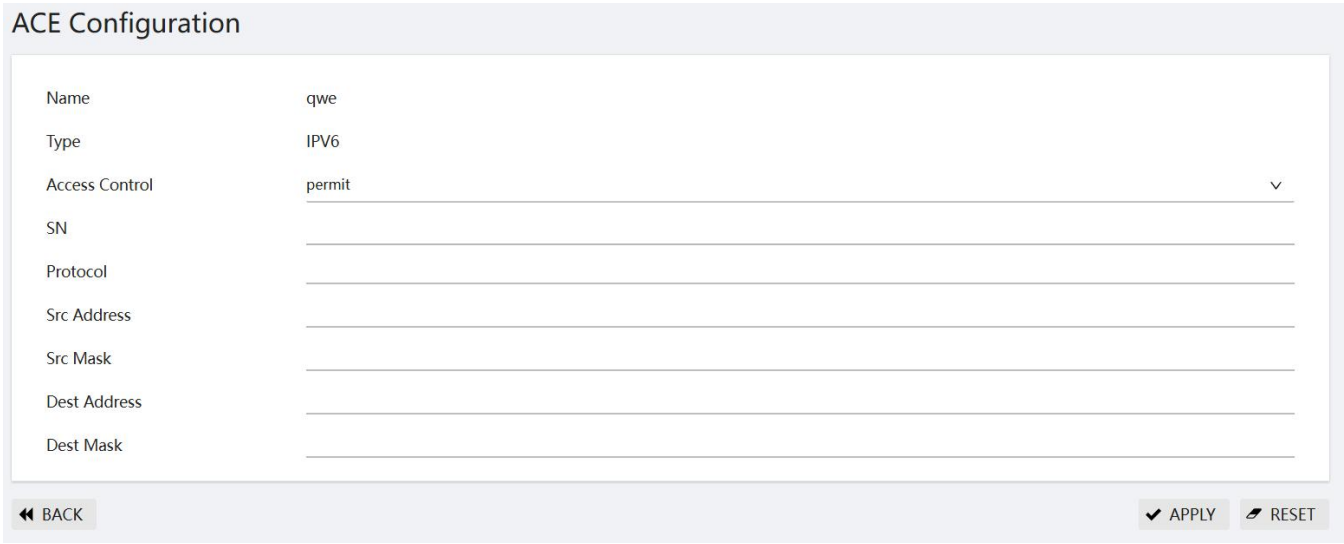


Table 6-6 Description of MAC Type ACE Parameters

configuration item		clarification
interviews	Deny	Release messages that hit this rule
	Permit	Discard messages that hit this rule
product key (software)		Rule table entry number
Ethernet protocol		Ethernet protocol type , range (0x05DD-0xFFFF)
prioritization		cos value of the message, range (0-7)
source address		Message source MAC address
source mask		The source MAC address mask is inverted, e.g., select the first 32 bits of the MAC address with a mask of 0000.0000.fffff
destination address		Message destination MAC address
destination mask		The destination MAC address mask is reversed, e.g., select the first 32 bits of the MAC address with a mask of 0000.0000.fffff

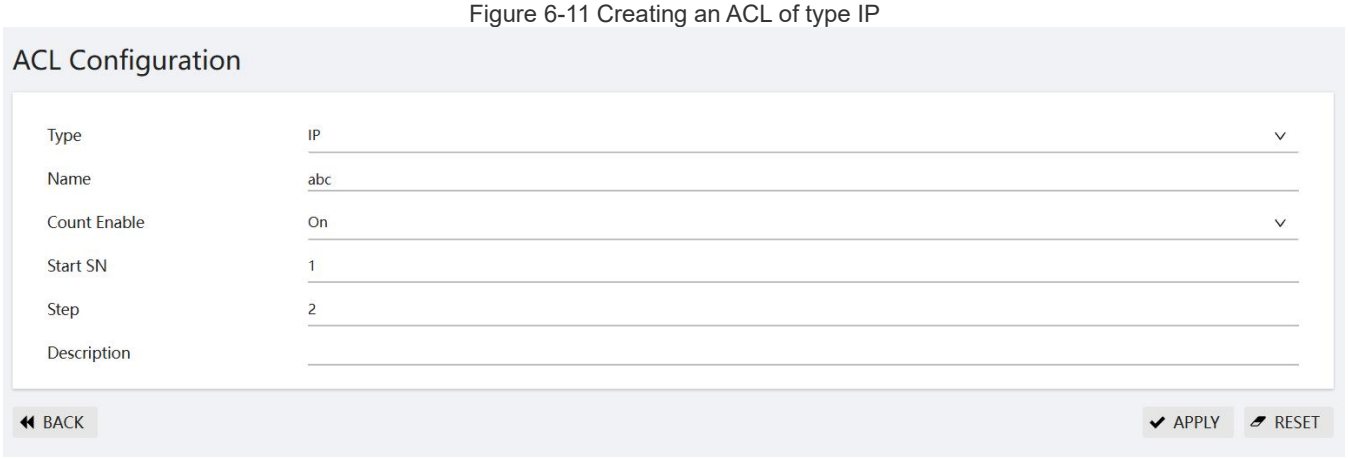
Figure 6-10 MAC Type ACE Configuration Interface

Procedure.

(1) Select [Security] [ACL Configuration] in the navigation bar to enter the ACL configuration interface.

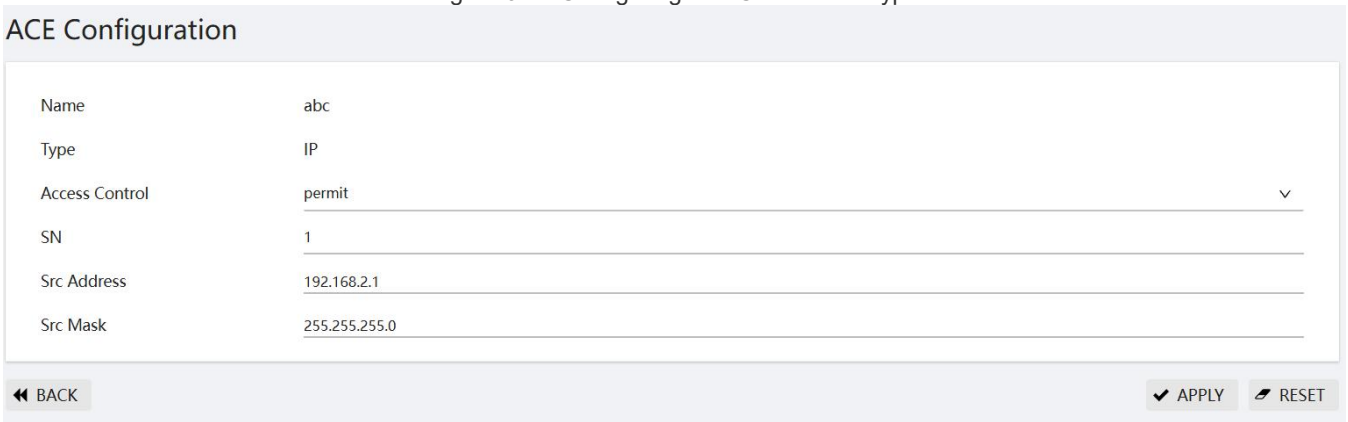
(2) Click "ACL Configuration" below the [Add ACL] button to enter the ACL rule creation interface, fill in the parameters according to the requirements, as shown in Figure 6-11, click [Confirm] button to complete the configuration.

Figure 6-11 Creating an ACL of type IP



(3) Click "ACE configuration" below the [Add ACE] button to enter the ACE configuration interface, fill in the parameters according to the requirements, as shown in Figure 6-12, click [Confirm] button to complete the configuration.

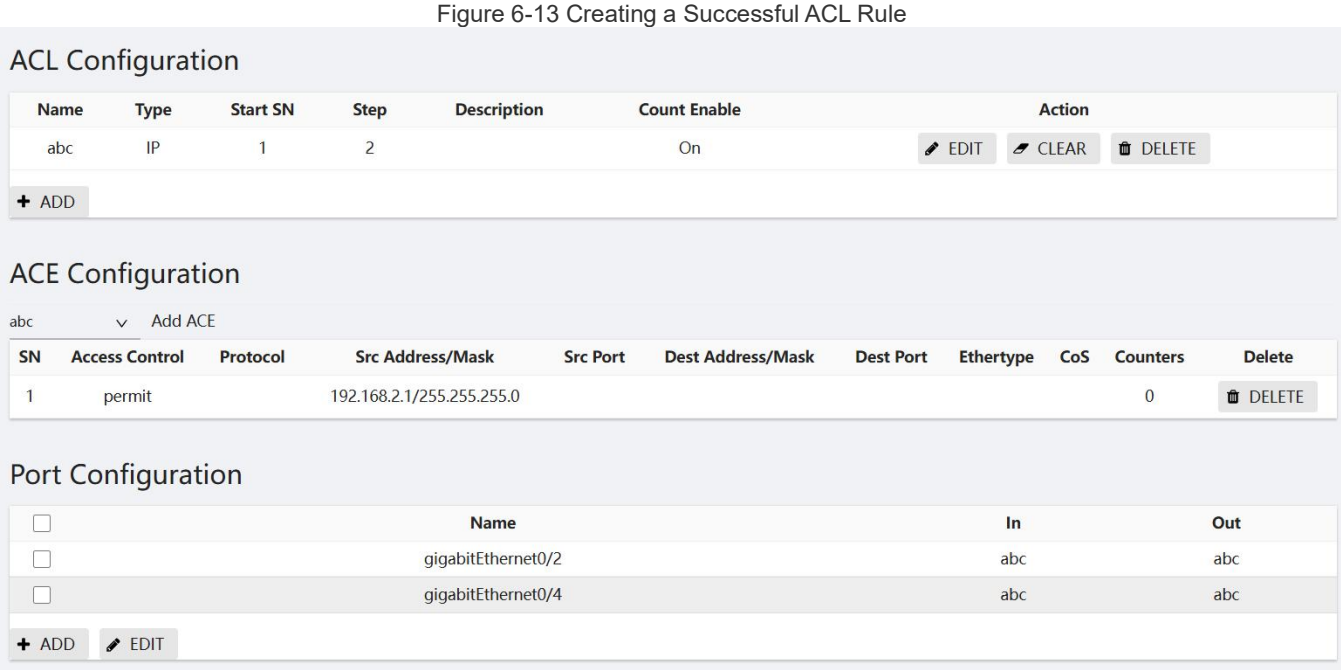
Figure 6-12 Configuring an ACE for an IP type



(4) Click the "Port Configuration" below the [Edit] button, select the ACL regulation "abc", the port panel select 2, 4, as shown in Figure 6-13, click [Apply] button to complete the configuration.

After the successful creation of the ACL complete interface as shown in Figure 6-13

Figure 6-13 Creating a Successful ACL Rule



（5）Click the [Save] button in the navigation bar to save the configuration

6.2 DoS

6.2.1 summarize

The purpose of a DoS (Denial of Service) attack is to prevent a computer or network from providing normal services. There are many different types of DoS attacks, and there are different ways to realize them.The common denominator is that the victim host or network is unable to receive and process external requests in a timely manner.Some typical types of DoS attacks are listed below.

SYN Flood message attack:

SYN Flood attack is the most common DDOS attack on the current network and the most classic DoS attack.By sending a large number of attack messages with forged source addresses to the port where the network service is located, it causes the connection queue of the target server to be full, thus preventing other legitimate users from accessing it.

ICMP Flood Message Attack:

ICMP Flood is a DDOS attack that sends a large number of ping packets to the destination host in a short period of time, consuming host resources.The host is unable to provide other services when its resources are exhausted.

ARP Flood Message Attack:

ARP Flood is a DDOS attack that sends a large number of ARP request packets to the destination host in a short period of time, consuming host resources.The host is unable to answer other ARP requests when it runs out of resources.

NULL SCAN attack:

The NULL SCAN attack mainly involves the attacker sending TCP messages to the target host IP without setting any flags, and some operating systems actively feed back RST messages, from which the attacker obtains ports for unclosed sessions.The essence of the anti-NULL SCAN attack is to discard TCP messages without any TCP flags, which can effectively prevent the attacker from obtaining the closure of ports through NULL SCAN and then launching subsequent attacks.

TCP messages with both SYN and FIN set at the same time:

Normally, the SYN flag (Connection Request Flag) and the FIN flag (Connection Dismantle Flag) cannot both appear in a TCP message, and the RFCs do not specify how the IP stack handles such malformed messages.An attacker can then take advantage of this feature to determine the type of operating system by sending a message with both SYN and FIN set at the same time.

TCP messages with FIN set but no ACK set:

Normally, the ACK flag is set on all but the first message (SYN message), including TCP connection dismantling messages (messages with the FIN flag set).However, some attackers may send TCP messages to the target host with the FIN flag set but without the ACK flag, which may cause the target host to crash.

TCP packets with SYN set and source port number 0-1023:

Port numbers 0-1023 are known port numbers assigned by the IANA and can only be used on most systems by system (or root) processes or programs executed by privileged users.These ports (0-1023) cannot be used as the source port number for the first TCP message (with the SYN flag set) sent by a client.To activate the Anti-Illegal TCP Message Attack function, the device checks the non-TCP message characteristics and discards it if it is illegal.

Our company provides the above kinds of anti-DoS attack functions.

6.2.2 denial-of-service (DoS) placement

Select [Security] [DoS Configuration] in the navigation bar to enter the DoS configuration interface.This page contains "Global Configuration", "SYN Configuration", "ICMP Configuration" and "ARP Configuration".ARP Configuration".

global configuration

The global configuration interface, shown in Figure 6-13, contains several global anti-DoS attack configurations, with specific parameters shown in Table 6-14.Global "SYN Flood
"ICMP Flood" and "ARP Flood" are configured in the same way, taking "ARP Flood" as an example.The configuration interface is shown in Figure 6-15.

Figure 6-13 DoS Global Configuration Interface

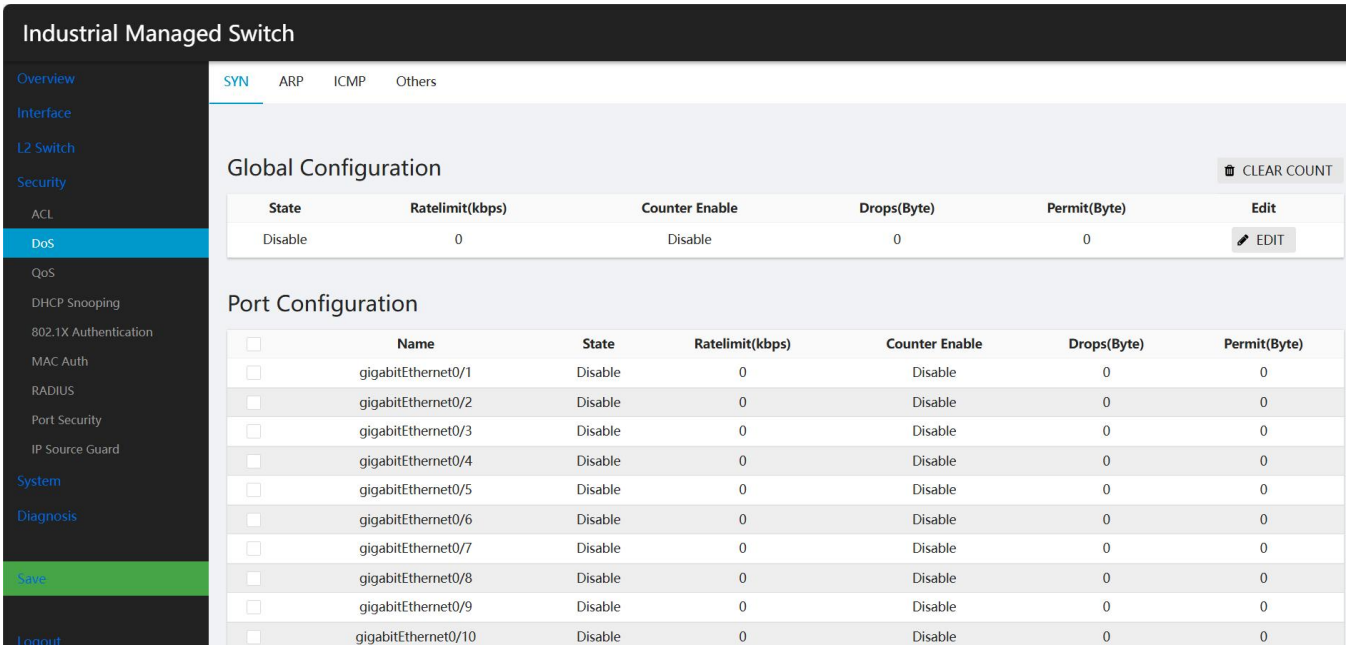


Table 6-14 DoS Global Configuration Parameter Descriptions

configuration item	clarification
Anti-NULL SCAN attack	Configure global resistance to NULL SCAN attacks, and discard TCP packets without any flags set when turned on
Anti-SYN FIN attack	Configure global anti-SYN FIN attack and discard TCP packets with both SYN and FIN set when turned on
Defense against SYN SPORT (0-1023) attacks	Configure global resistance to SYN SPORTL1024 attacks, and discard synchronization packets for TCP on source ports (0-1023) when turned on
Failure to protect against the FIN NOACK attack.	Configure the global anti-FIN NOACK attack to discard TCP packets with FIN set but no ACK set when enabled.
SYN/ICMP/ARP Flood	Configuring Global Anti-SYN/ICMP/ARP Flood Attacks
SYN/ICMP/ARP Flood 限速	Configure the anti-SYN/ICMP/ARP Flood attack speed limit range, 0 to deny all attack messages
counter enable	Configure the anti-SYN/ICMP/ARP Flood attack counter to be enabled, and when the counter is turned on, it will count the hit attack packets.

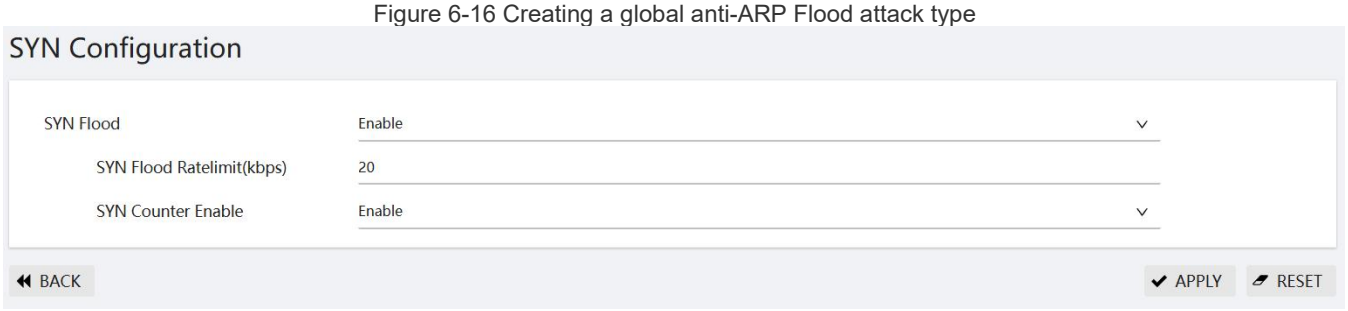
Figure 6-15 APR Configuration Interface

procedure:

(1) Select [Security] [DoS Configuration] in the navigation bar to enter the DoS configuration interface.

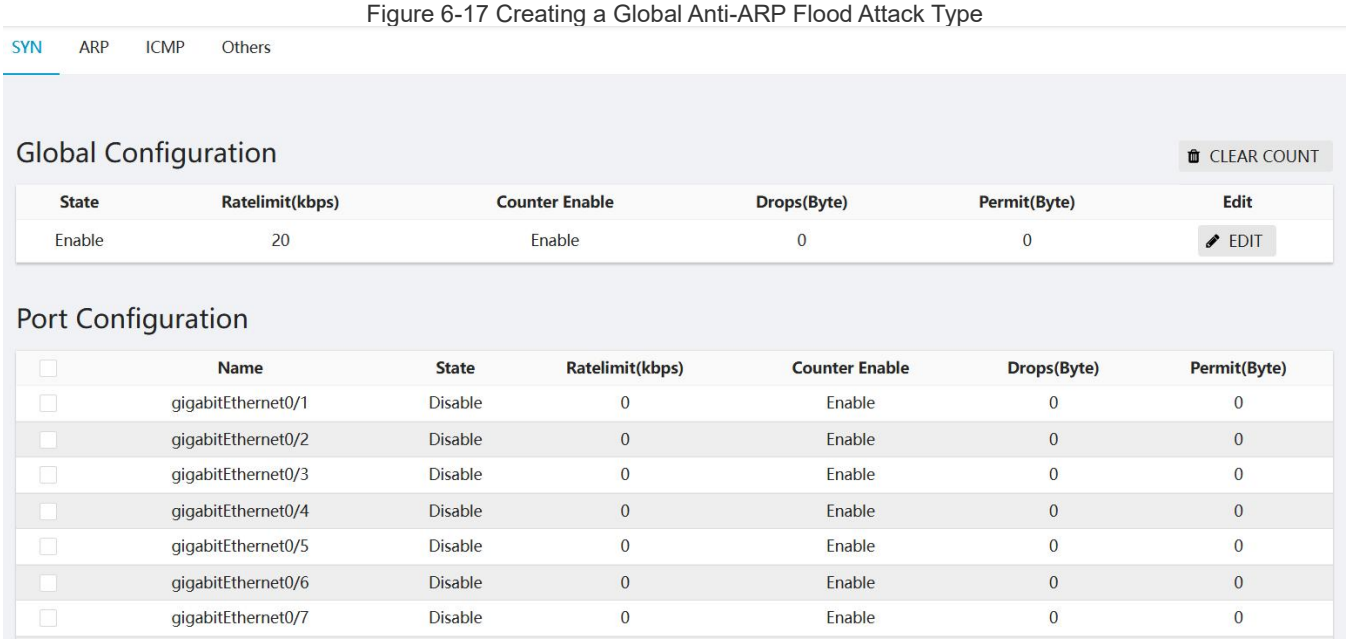
(2) Click the [Edit] button in the "Global Configuration" form to enter the anti-DoS attack creation interface, fill in the parameters according to the requirements of the global "ARP Flood" configuration, for example, as shown in Figure 6-16, click the [Confirm] button to complete.Configuration.

Figure 6-16 Creating a global anti-ARP Flood attack type



The DoS global configuration screen after successful creation is shown in Figure 6-17.

Figure 6-17 Creating a Global Anti-ARP Flood Attack Type



SYN/ICMP/ARP placement

The port configuration anti-DoS attack includes SYN Flood, ICMP Flood and ARP Flood, the configuration interface is shown in Figure 6-19~21, and the description of each parameter is shown in Table 6-18.

Table 6-18 Parameter Description of Anti-SYN/ICMP/ARP Flood Attack Type

configuration item	clarification
SYN Flood	Enable anti-SYN Flood attack
SYN Flood speed limit(kbps)	Limit SYN message attack flow rate
ICMP Flood	Enable protection against ICMP Flood attacks
ICMP Flood speed limit(kbps)	Limit ICMP message attack flow rate
ARP Flood	Enable protection against ARP Flood attacks
ARP Flood speed limit(kbps)	Limit the rate of ARP packet attack flow

Figure 6-19 SYN Configuration Interface

Figure 6-20 ICMP placement interface

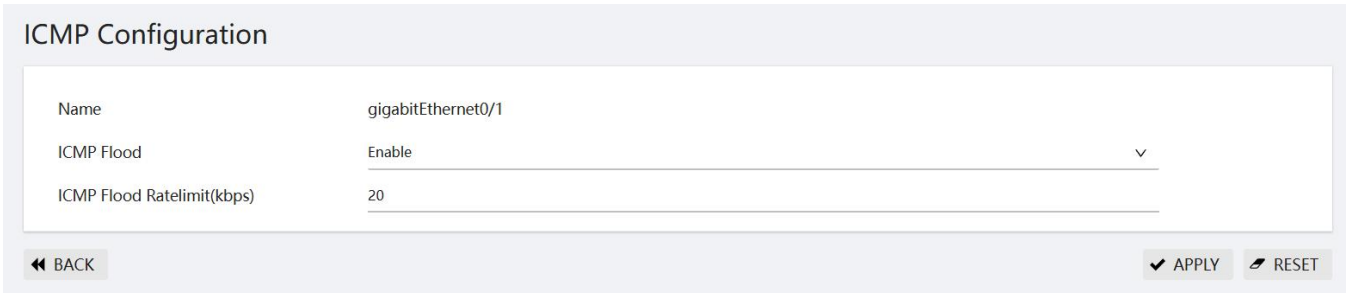


Figure 6-21 ARP Configuration Interface

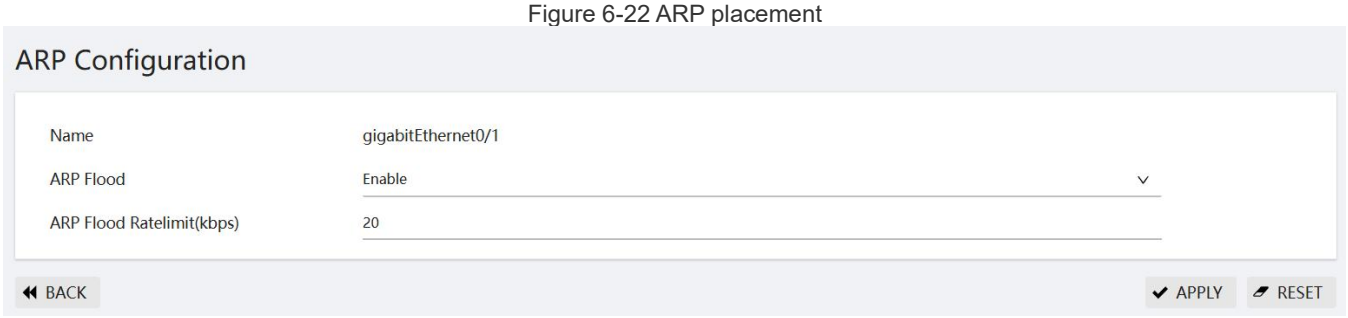
Configuration steps:

(1) Select [Security] [DoS Configuration] in the navigation bar to enter the DoS configuration interface.

(2) Click the [Batch Edit] button under "SYN/ICMP/ARP Configuration" to enter the SYN/ICMP/ARP creation interface to create a configuration example in case of ARP Flood attack, as shown in Figure 6-22.

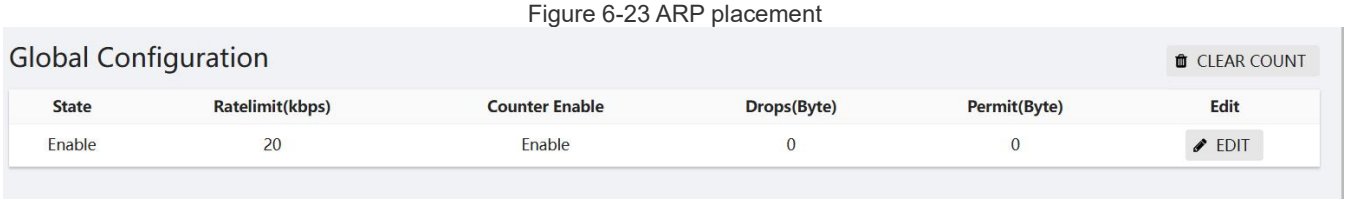
(3) Select the port members to be configured and click the [Confirm] button to complete the operation.

Figure 6-22 ARP placement



The ARP configuration interface after successful creation is shown in Figure 6-23。

Figure 6-23 ARP placement



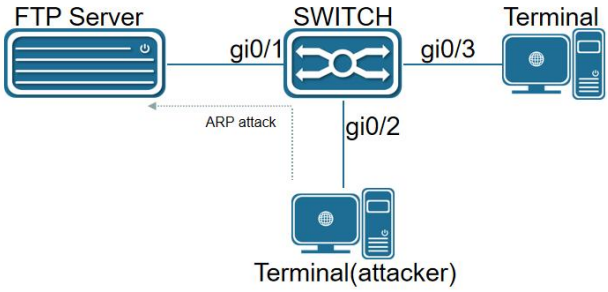
6.2.3 Configuration Example

As an example of anti-ARP Flood attack configuration, the following networking requirements, as shown in Figure 6-24:

- Port gi0/1 connects to the FTP server, and ports gi0/2 and gi0/3 connect to the terminal devices respectively.

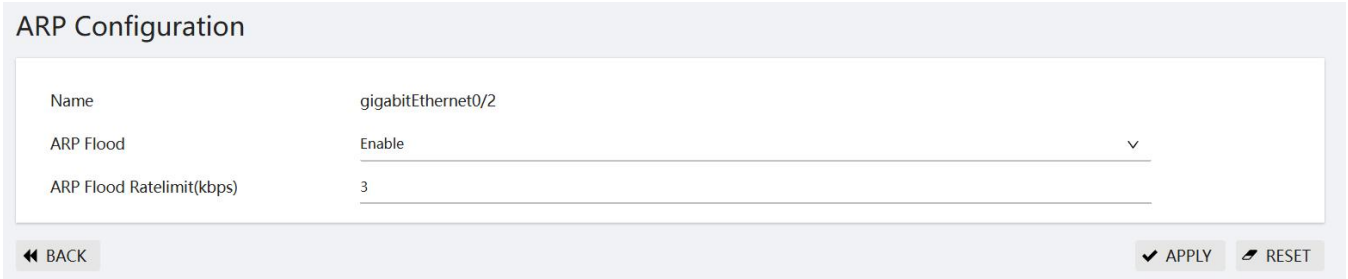
- Port gi0/2 is connected to a terminal device that forges a large number of IP and MAC addresses to launch an ARP attack, causing the FTP server to be unable to process normally requested ARP packets.

Figure 6-24 Network Topology



Step 1: Select [Security] [DoS Configuration] in the navigation bar to enter the DoS configuration interface.
Step 2: Click the [Port Configuration] button under "ARP Configuration" to enter the ARP configuration interface, select GigabitEthernet0/2 in the port panel, and then click Edit to configure, as shown in Figure 6-25.

Figure 6-25 Anti-ARP Flood Configuration Interface



Step 3: Click the [Save] button on the navigation bar to save the configuration.

6.3 QoS

6.3.1 summarize

QoS (Quality of Service) refers to the ability of a network to utilize various underlying technologies to provide better service for specified network traffic.
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 are likely to be discarded.In order to meet the requirements of different applications with different quality of service, it is necessary for the network to be able to allocate and schedule resources according to the user's requirements and provide different quality of service for different data streams.
Devices that support QoS functions can provide transmission quality services. For a certain category of data flow, it can be assigned a certain level of transmission priority to identify its relative importance, and use the various priority forwarding policies, congestion avoidance and other mechanisms provided by the device to provide special transmission services for these data flows.

A network environment configured with QoS increases the predictability of network performance and enables effective allocation of network bandwidth and more rational utilization of network resources.

6.3.2 QoS deployment

clarification

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 traffic spike is higher, the speed limit is more stable, but the average rate may be higher than the speed limit value; when the cbs value is small, the traffic spike is low, the speed limit fluctuates more, and the average rate may be smaller than the speed limit value.It is recommended that the cbs configuration take 4 times the value of cir and the small value of 31250.

Enable QoS

(1) Select [Security] [QoS Configuration] in the navigation bar to enter the QoS configuration interface, as shown in Figure 6-26.

Figure 6-26 QoS Global Configuration Interface

（2) Click the right button, select Algorithm, and click the [Enable] button to enable QoS.

Table 6-27 QoS Global Configuration Parameter Descriptions

configuration item	clarification		
global configuration	state of affairs		QOS enabled, all QOS features are not supported for configuration until enabled
	arithmetic	Sp	Absolute priority scheduling, queue ID large high priority, high priority queue processing is completed after processing low priority queue
		Wrr	Rotation scheduling algorithm that schedules each queue sequentially from the largest to the smallest queue ID based on the queue weights.

Configuring Qos Mapping

(1) In the current interface, click the [Queue] button under "QoS Mapping" to enter the queue configuration interface, as shown in Figure 6-28, and the parameter description is shown in Table 6-29.

Figure 6-28 Queue Configuration Interface

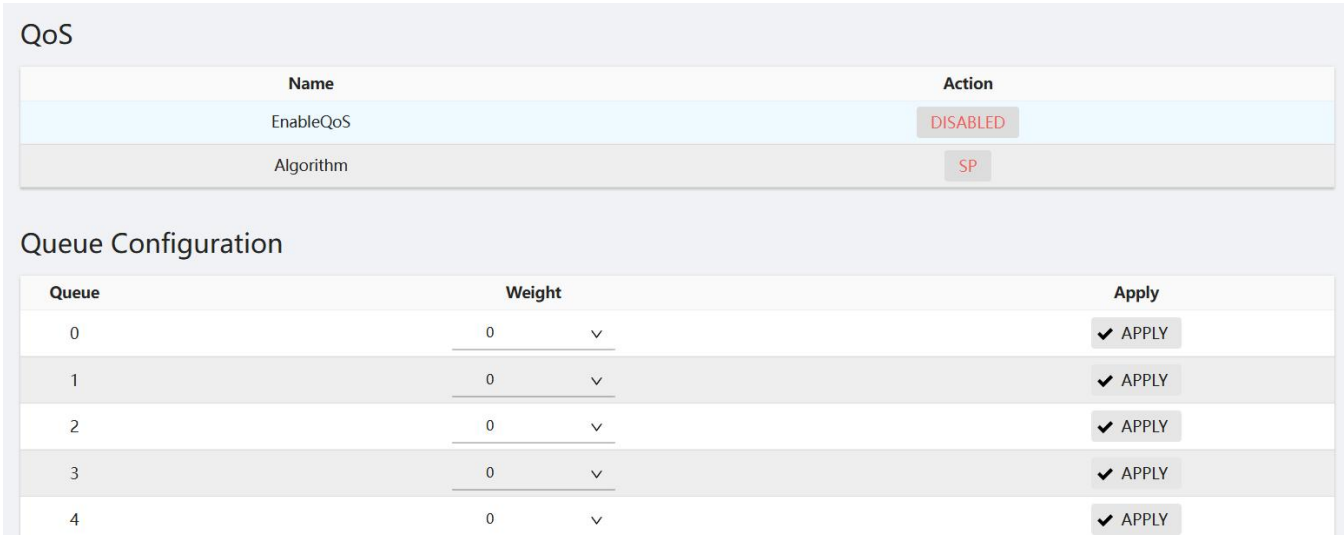


Table 6-29 Queue Parameter Descriptions

configuration item	clarification	
queue weight	formation	<0， 7>
	weights	<0, 32>, the larger the value, the higher the weight, the higher the probability of prioritizing this queue message in case of channel congestion, 0 means infinity.

（2）Click the [CoS] button under "QoS Mapping" to enter the CoS configuration interface, as shown in Figure 6-30, and the parameter description is shown in Table 6-31.

Figure 6-30 CoS configuration interface

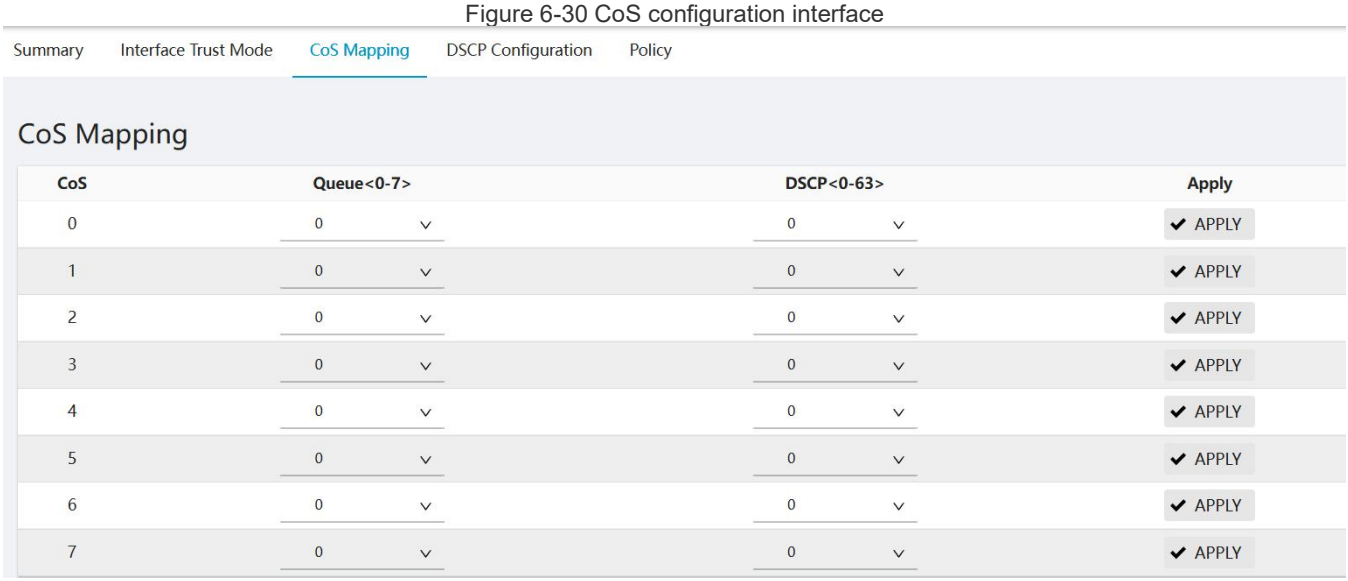


Table 6-31 Description of CoS Parameters

configuration item		clarification
CoS placement	CoS	<0， 7>
	formation	<0， 7>， The cos-queue mapping relationship, which modifies the message egress queue based on the port's tagged cos, takes effect when the port is configured for no trust, trust cos, or trust dscp and is not an ip message.
	DSCP	cos-dscpmapping relationship, which takes effect when the port is configured for no trust, trust cos, or trust dscp and is not an ip packet, modifies the packet dscp value

（3）Click the [DSCP] button under "QoS Mapping" to enter the DSCP configuration interface, as shown in Figure 6-32, and the parameter description is shown in Table 6-33.

Figure 6-32 DSCP placement interface

Table 6-33 Description of DSCP Parameters

configuration item		clarification
DSCP mapping	DSCP	<0， 63>
	formation	<0， 7>， The dsp-queue mapping relationship, which takes effect when the port is configured for trust dscp and ip packets, modifies the packet egress queues
	CoS	<0， 7>， The dscp-cos mapping relationship, which takes effect when the port is configured for trust dscp and ip messages, modifies the message cos field
	new DSCP price	<0， 63>， The dscp-dscp mapping relationship, which takes effect when the port is configured for trust dscp and ip messages, performs the dscp-dscp mapping first, followed by the dscp-cos mapping

6.3.2.1 Qos Categorized Configurations

In the current QoS interface, click the [Add] button under "Classification Configuration" to enter the Classification Configuration interface, as shown in Figure 6-34, and the parameter description is shown in Table 6-35.

Figure 6-34 Classification Configuration Interface

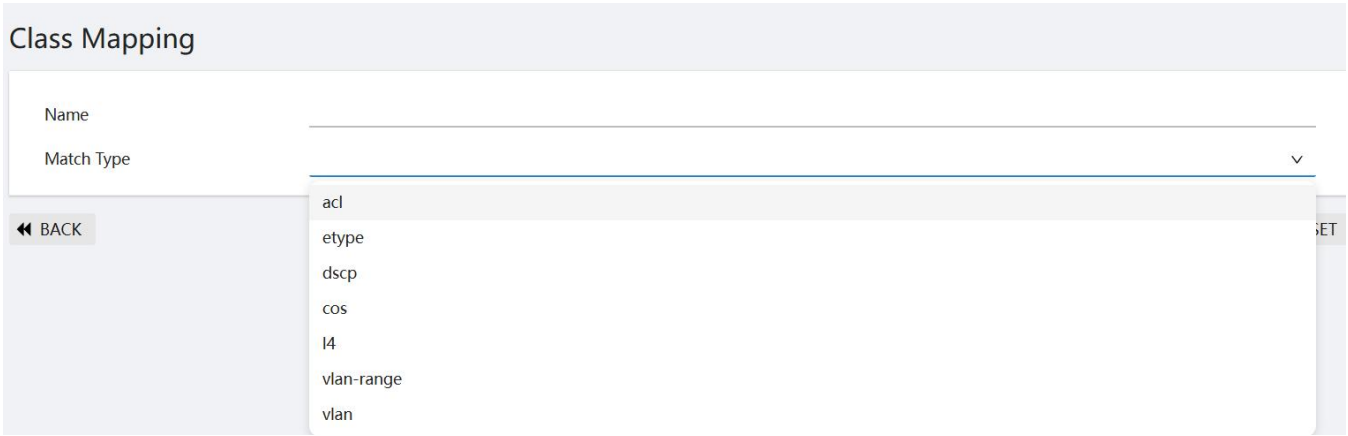


Table 6-35 Classification Configuration Parameter Descriptions

configuration item		instructions
Categorized Configurations	name	Create categories, define category names
	Match Type	Define match types to support associations acl，etype，dscp，cos，l4，vlan-rangge，vlan

6.3.2.2Qos Strategy Configuration

In the current QoS interface, click the [Add Policy Rule] button under "Policy Configuration" to enter the rule configuration interface, as shown in Figure 6-36, and the parameter description is shown in Table 6-37.

Figure 6-36 Rule Configuration Interface

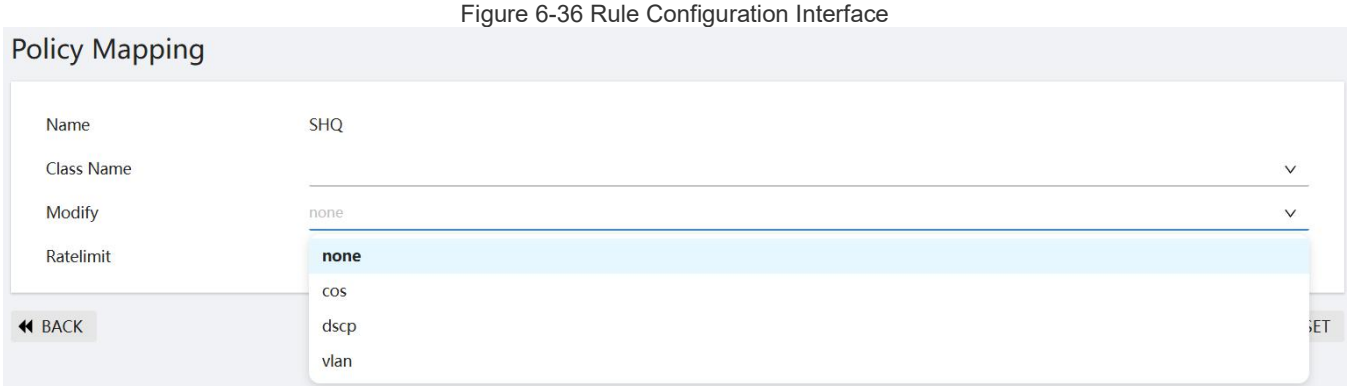


Table 6-37 Description of Rule Configuration Parameters

configuration item		instructions
Rule Configuration	name	Name of the rule
	classification name	Select Category Name
	modifications	The policy corresponds to action one, which supports modifying cos, dscp, vlan, etc.
	speed limit	The strategy corresponds to action two, speed limit
	CIR	Speed Limit Waterline in kbps
	CBS	Burst capacity in Kbyte

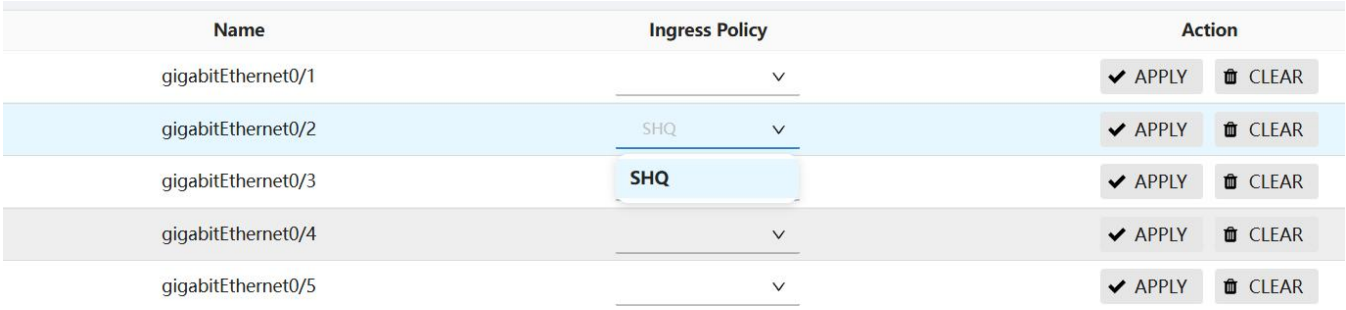
6.3.2.3Qos Port Configuration

In the QoS interface, click the [Batch Edit] button under "Port Configuration" to enter the port configuration interface, as shown in Figure 6-38, and the description of port configuration parameters is shown in Table 6-39.

Table 6-38 Description of Rule Configuration Parameters

configuration item		clarification
Port Configuration	Default CoS	<0, 7>, when a port is configured to be untrusted, or when trust is configured but the message does not satisfy the trust conditions, the port default cos mark ingress message is used
	trust	Supports no trust, trust cos, and trust dscp configuration.When in no trust mode, the ingress phase modifies the cos field of the message and the dscp field according to the default cos of the port; when trust cos is configured, the same no trust mode is used for untagged messages, and for tagged messages, the cos of the message is selected; when trust dscp is configured, the cos of the message is selected for ip messages; when trust dscp is configured, the cos of the message is selected for ip messages.dscp, and for non-ip packets, the same as trust cos mode.
	entrance strategy	Select the policy to create

Figure 6-39 QoS Port Configuration Interface



6.4 DHCP Snooping

6.4.1 summarize

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

DHCP Snooping is a DHCP security technology that realizes the isolation of illegal DHCP Server by detecting and managing the DHCP interaction messages, and the DHCP isolation function can be effective based on VLAN.

DHCP TRUST Port

For the port connecting to the legitimate DHCP Server, it is recognized as a TRUST port, and other ports are UNTRUST ports.When the DHCP Snooping function is enabled, the device prevents client DHCP broadcast messages from being sent to UNTRUST ports.

DHCP Message Port Speed Limit

In response to DHCP message traffic attacks by some users on the port, the device supports DHCP message port speed limiting to reduce or eliminate the impact of user attacks on the network environment under the port.

MAC Address Inspection

For DHCP messages sent from UNTRUST ports, detect the source MAC address in the Layer 2 header and the CLIENT HARDWARE ADDRESS field in the data segment of the message, if they are not the same, then it is an illegal message.

Option-82 Option

The DHCP Option82 option, also known as the DHCP Relay Agent Information Option, is an option in DHCP messages.The Option82 option is a DHCP option proposed to enhance the security of the DHCP server and improve the IP address allocation policy, and is implemented by the relay component.Option82 is a DHCP option proposed to enhance the security of the DHCP server and improve the IP address allocation policy, and is realized by the relay component to add and strip the option.

DHCP Legitimate Users

DHCP Snooping counts the information of users assigned by legitimate servers by monitoring DHCP messages.as legitimate users on the port when the ip verify source function is enabled on the port.

6.4.2 DHCP Snooping deployment

Configuration steps:

(1) Select [Security] [DHCP Snooping Configuration] in the navigation to jump to the DHCP Snooping configuration interface, as shown in Figure 6-40, and the global configuration parameters are shown in Table 6-41.

Figure 6-40 DHCP Snooping Global Configuration

Table 6-41 DHCP Snooping Global Configuration

configuration item	instructions
state of affairs	Enable or disable DHCP Snooping globally.
VLAN List	Configure the VLAN effective range of DHCP Snooping, the default is all VLANs are effective
MAC address verification	Enable/disable MAC address verification for DHCP messages
Option 82	Configure to add option-82 information to DHCP request messages and exclude option-82 information from answer messages
Database delays	Configure the interval at which DHCP Snooping database data is timed to be written to flash
appliance	Click on this application to complete the configuration

(2) Select the corresponding port that needs to open this function, click the [Edit] button or click the [Batch Configuration] button under "Port Configuration" to enter the port configuration interface, as shown in Figure 6-42, and the description of the port configuration parameters is shown in Table 6-43.

Table 6-42 DHCP Snooping Trust Port Configuration Parameters

configuration item	clarification
trust	Enable DHCP Snooping trust port
speed limit	Set the port DHCP speed limit, PPS is the number of messages per second, range 0-128

Figure 6-43 DHCP Snooping credential mouth placement

6.5 802.1X accreditation

6.5.1 Overview

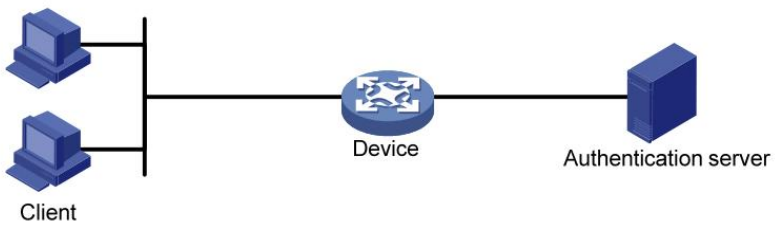
Initially, the IEEE 802 LAN/WAN committee proposed the 802.1X protocol to address wireless LAN network security issues.Later, the 802.1X protocol was widely used in Ethernet as a common access control mechanism for LANs, mainly addressing authentication and security concerns within Ethernet.

The 802.1X protocol is a port-based network access control protocol, that is, it authenticates the accessed user devices on the ports of LAN access devices so that the user devices can control the access to network resources.

Architecture of 802.1X

The 802.1X system includes three entities: the client (Client), the device side (Device), and the authentication server, as shown in Figure 6-44.

Figure 6-44 802.1X Architecture



-A client is a user terminal device that requests access to the LAN and is authenticated by the device side of the LAN.Client software that supports 802.1X authentication must be installed on the client.

-Device side is a network device in the LAN that controls client access and is located between the client and the authentication server. It provides the client with a port (physical or logical) to access the LAN and authenticates the connected client through interaction with the server.

-Authentication server is used for authentication, authorization and billing of clients, usually a RADIUS (Remote Authentication Dial-In User Service) server.The authentication server verifies the legitimacy of the client based on the client authentication information sent from the device side, and notifies the device side of the verification result, and the device side decides whether to allow the client to access.In some smaller network environments, the role of the authentication server can also be replaced by the device side, that is, the device side of the local authentication, authorization and billing of clients.

802.1X Control of Ports

1、Controlled/uncontrolled ports

The port on the device side that provides access to the LAN for clients is divided into two logical ports: the controlled port and the uncontrolled port.Any frame arriving on this port is visible on both the controlled and uncontrolled ports.

The uncontrolled port is always in a bi-directional state and is mainly used to pass EAPOL (Extensible Authentication Protocol over LAN) protocol frames to ensure that clients can always send or receive authentication messages.

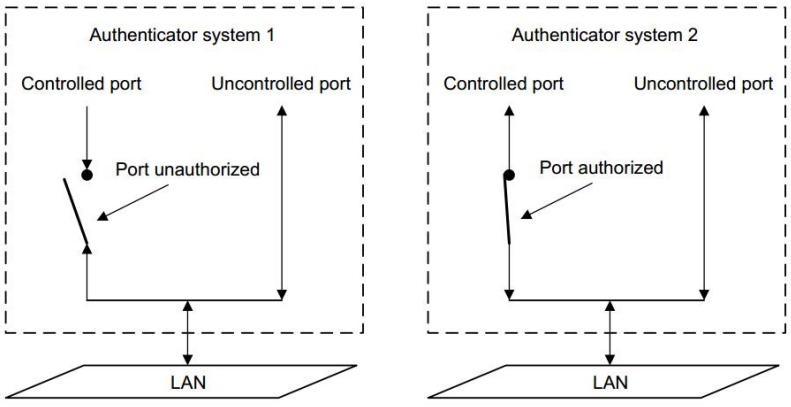
-Controlled ports are bi-directionally connected in the authorized state and are used to deliver service messages; in the unauthorized state, they are prohibited from receiving any messages from the client.

2、Authorized/non-authorized status

The device side uses the authentication server to perform authentication on clients that need to access the LAN, and controls the authorization status of the controlled port accordingly based on the authentication result (Accept or Reject).

Figure 6-45 shows the effect of different authorization states on a controlled port on the packets passing through that port.The figure compares the port states of two 802.1X authentication systems.System 1's controlled port is in the unauthorized state and does not allow messages to pass; System 2's controlled port is in the authorized state and allows messages to pass.

Figure 6-45 Effect of Authorization Status on Controlled Ports



3、controlled direction

In the unauthorized state, the controlled port can be set to unidirectional controlled and bidirectional controlled.

In the bi-directional controlled state, sending and receiving of frames is prohibited;

-When in unidirectional controlled state, receiving frames from the client is prohibited, but sending frames to the client is allowed.

instructions

Controlled ports on our devices can only be in a unidirectional

-

4.4.1.3 Authentication Trigger Methods for 802.1X

The 802.1X authentication process can be initiated either by the client on its own initiative or by the device side.

1、Client-initiated triggering method

- -Multicast trigger: The client actively sends an EAPOL-Start message to the device side to trigger authentication, and the destination address of the message is the multicast MAC address 01-80-C2-00-00-03.
- -Broadcast trigger: The client actively sends an EAPOL-Start message to the device side to trigger authentication, and the destination address of the message is the broadcast MAC address.This method can solve the problem that the authentication device cannot receive the client's authentication request due to the fact that some devices in the network do not support the above multicast message.

instructions

目前我司设备仅支持组播触发方式。

2、Device-side active trigger method

The device-side active trigger method is used to support clients that cannot actively send EAPOL-Start messages, such as 802.1X clients that come with Windows XP.

802.1X client that comes with Windows XP.There are two ways for the device to actively trigger authentication:

-Multicast trigger: The device actively sends Identity type EAP-Request frames to the client multicast every N seconds (default is 30 seconds) to trigger authentication.

Unicast trigger: When the device receives a message with an unknown source MAC address, it actively sends an Identity-type EAP-Request frame to the MAC address to trigger authentication.If the device does not receive a response from the client within the set time limit, the message is retransmitted.

802.1X Authentication Process

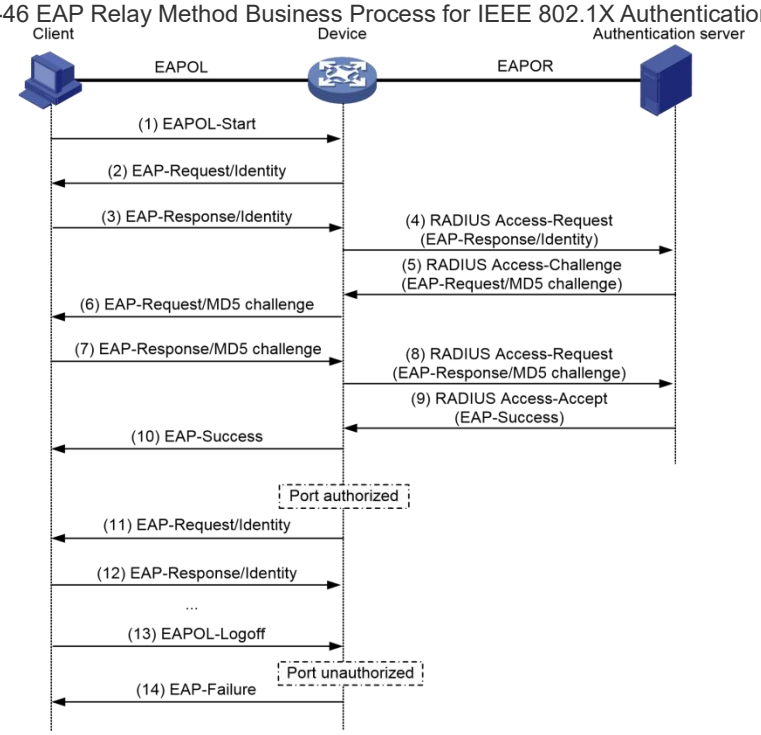
The 802.1X system supports EAP relay and EAP termination methods to interact with the remote RADIUS server.

EAP trunking method

This approach, specified in the IEEE 802.1X standard, carries EAP within other high-level protocols, such as EAP over RADIUS, in order to extend the authentication protocol messages across complex networks to the authentication server.In general, the RADIUS server is required to support the EAP attributes: EAP-Message and Message-Authenticator, which are used to encapsulate the EAP message and protect the RADIUS message carrying the EAP-Message, respectively.

The following MD5-Challenge authentication method as an example to introduce the basic business process, the authentication process shown in Figure 6-46.

Figure 6-46 EAP Relay Method Business Process for IEEE 802.1X Authentication System



(2) When the user needs to access the external network open the 802.1X client program, enter the user name and password that have been applied and registered, and initiate a connection request.At this time, the client program will send an authentication request frame (EAPOL-Start) to the device side to start an authentication process.

(3) When the device side receives the authentication request frame, it sends out an Identity type request frame (EAP-Request/Identity) requesting the user's client program to send the entered user name.

(4) The client program responds to the request from the device side and sends the user name information to the device side via an Identity type response frame (EAP-Response/Identity).

(5) The device side will send the EAP message in the response frame sent by the client side encapsulated in a RADIUS message (RADIUS Access-Request) to the authentication server for processing.

(6) After the RADIUS server receives the user name information forwarded by the device side, it compares the information with the user name list in the database, finds the password information corresponding to the user name, encrypts the password with a randomly generated MD5 Challenge, and sends the MD5 Challenge to the device side via the RADIUS Access-Challenge message.The MD5 Challenge is sent to the device via a RADIUS Access-Challenge message.

(7) The device forwards the MD5 Challenge sent by the RADIUS server to the client.

(8) When the client receives the MD5 Challenge from the device side, it encrypts the password part with the Challenge, generates the EAP-Response/MD5 Challenge message, and sends it to the device side.

(9) The device side encapsulates the EAP-Response/MD5 Challenge message in a RADIUS message (RADIUS Access-Request) and sends it to the RADIUS authentication server.

(10) The RADIUS server compares the received encrypted password information with the local encrypted password information, and if they are the same, it considers the user to be a legitimate user and sends an authentication pass message (RADIUS Access-Accept) to the device.

(11) The device receives the authentication pass message and sends an authentication success frame (EAP-Success) to the client, and changes the port to the authorized state, allowing the user to access the network through the port.

(12) During the period when the user is online, the device side will monitor the online status of the user by sending handshake messages to the client periodically.

(13) After the client receives the handshake message, it sends an answer message to the device to indicate that the user is still online.By default, if the two handshake request messages sent by the device side are not answered by the client, the device side lets the user go offline to prevent the user from going offline for abnormal reasons that the device cannot sense.

(14) The client can send an EAPOL-Logoff frame to the device side to actively request to go offline.

(15) The device side changes the port state from authorized to unauthorized and sends an EAP-Failure message to the client.

 instructions

In the EAP relay method, you need to ensure that a consistent EAP authentication method is selected on both the client and the RADIUS server, whereas on the device, you only need to configure the

802.1X user authentication method as EAP.

- 802.1X Access Control Methods
- The device not only supports the port-based access authentication (Port Based) specified in the protocol, but also extends and optimizes it to support the MAC-based access control (MAC Based).
- When port-based access control is used, as long as the first user under the port is successfully authenticated, other users can use the network resources without authentication, but when the first user goes offline, other users will be denied access to the network.
- -When using MAC-based access control, all access users under the port need to be authenticated individually, and when a user goes offline, only that user cannot use the network.

6.5.2 Configuring 802.1X

View 802.1X Overview

Select [Security] [Dot1x] in the navigation bar to enter the Dot1x overview screen, as shown in Figure 6-47.The 802.1X configuration can be displayed in the profile interface, and the description of each parameter is shown in Table 6-48.

Figure 6-47 802.1X Overview Interface

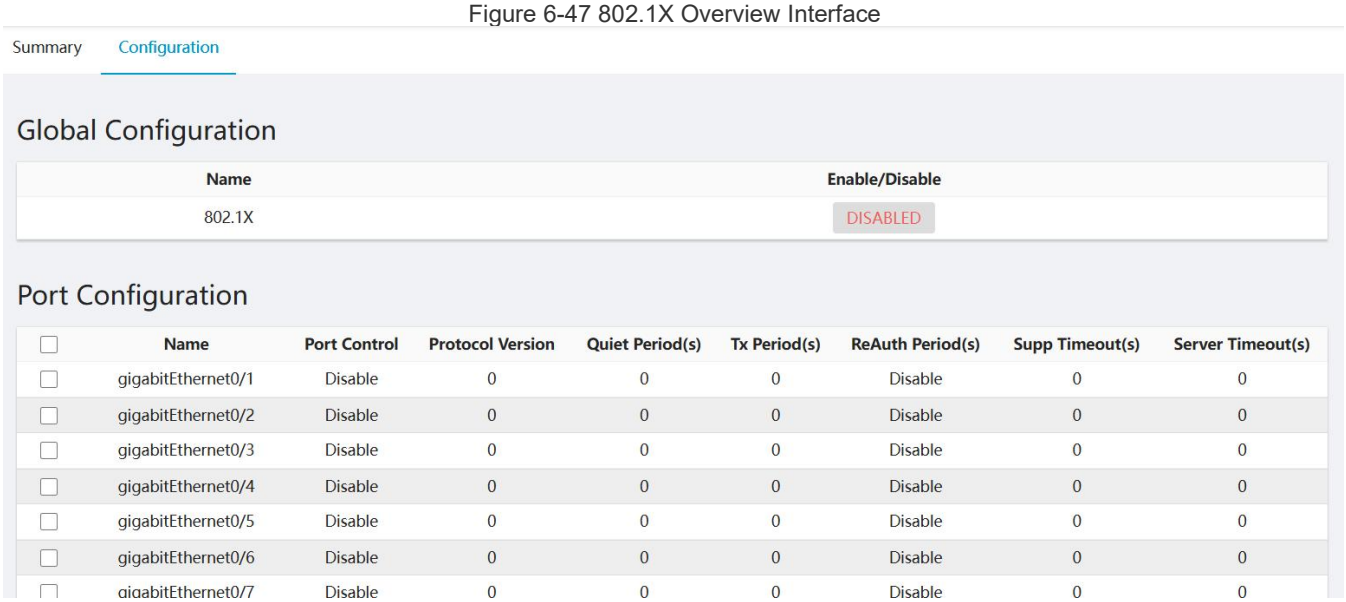


Table 6-48 802.1X Profile Parameter Descriptions

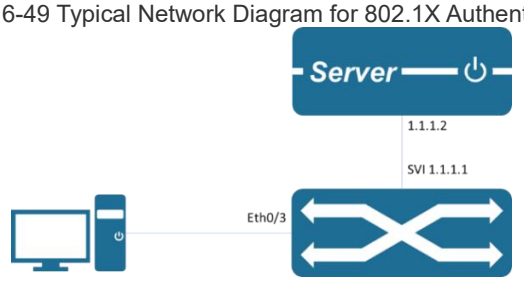
configuration item		clarification
global configuration	state of affairs	function switch
	RADIUS Deployment	Click to jump to the RADIUS configuration interface
Port Configuration	name	physical port
	port controlled	Port Controlled Mode
	protocol version	802.1X protocol version used
	silent time	Set the value of the silence timer so that when an 802.1X user fails to authenticate, the device needs to be silent for a certain period of time (set by the "Silence Duration") before re-initiating authentication.During the silence period, the device does not process 802.1X authentication.
	duty cycle	Message Retransmission Period
	Recertification cycle	Setting the value of the periodic reauthentication timer When the periodic re-authentication function is enabled on a port, the device will start the periodic re-authentication timer after the user is successfully authenticated, which is used to periodically initiate re-authentication for online users, so as to update the authorization information of the server for the user at regular intervals.
	Client Timeout	Setting the value of the client timeout timer When the device side sends an EAP-Request/MD5 Challenge request message to the client, the device side starts this timer, and if the device side does not receive a response from the client within the time limit set by this timer, the device side will retransmit the message.
	Server Timeout	Setting the server timeout timer value

		When the device sends a RADIUS Access-Request request message to the authentication server, the device starts the server timeout timer, and if the device does not receive a response from the authentication server within the time set by the timer, the device will resend the authentication request message.

6.5.3 802.1XConfiguration Example

- Scenario Requirements
- requires authentication of access users on port GigabitEthernet 0/3 to control their access to the Internet.
- RADIUS server group IP address 1.1.1.2.
- sets the shared key to name when the system interacts with the RADIUS server for messages.
- network diagram

Figure 6-49 Typical Network Diagram for 802.1X Authentication



Typical Configuration Example

Step 1: Configure the server side

Server-side:

Configure NAS authentication device 1.1.1.1 and communication key name.

In this example, freeradius is used as the server, and the main configuration is as follows:

vim /etc/freeRADIUS/3.0/clients.conf

Add client 1.1.1.1 {

ipaddr = 1.1.1.1

secret = name

}

Add user account test password test.

cat /etc/freeRADIUS/3.0/mods-config/files/authorize | grep "password"

testing Cleartext-Password := "password"

The corresponding authentication method needs to be supported, such as EAP-MSCHAPv2

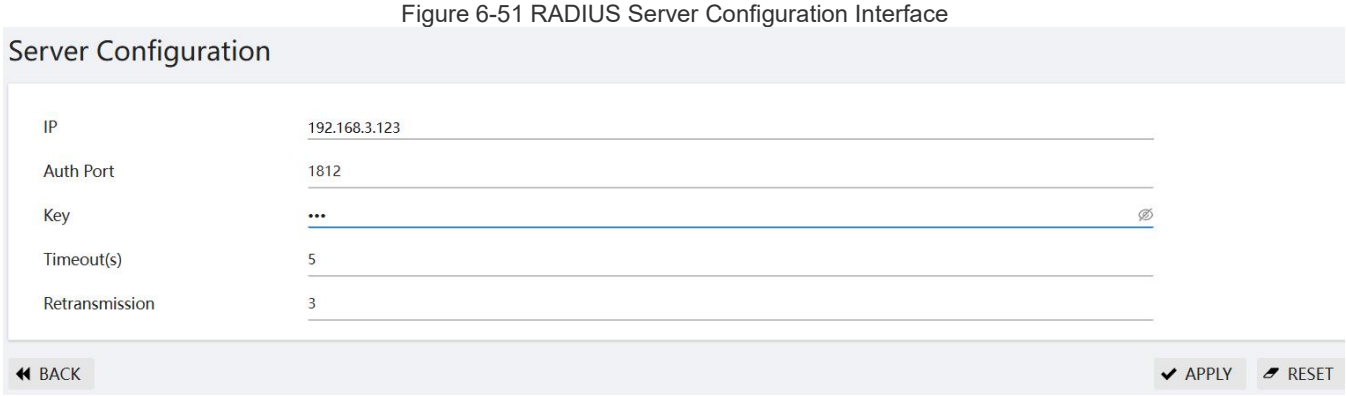
Step 2: Configure the RADIUS server.

Select [Security] [RADIUS] [Global Mode] in the navigation bar to enter the page shown in Figure 6-50.

Figure 6-50 RADIUS server overview screen

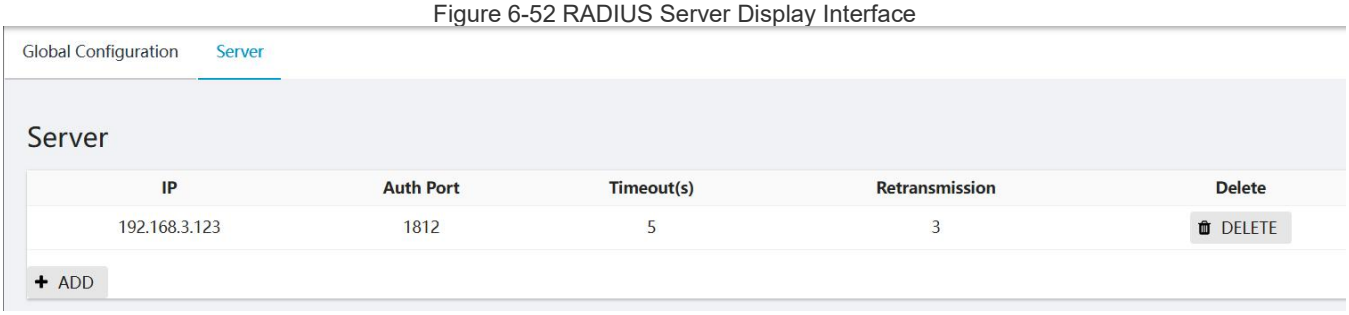
Click the [Add] button under "Server" to enter the RADIUS server configuration interface, as shown in Figure 6-51, configure the RADIUS server IP for 1.1.1.2, the default authentication port is 1812, enter the password, the timeout time is 5S by default, the number of retransmissions is 3, click the [Confirm] button!Finish the configuration.

Figure 6-51 RADIUS Server Configuration Interface



After the configuration is complete, it automatically returns to the following interface, as shown in Figure 6-52, where you can see the successfully created RADIUS server.

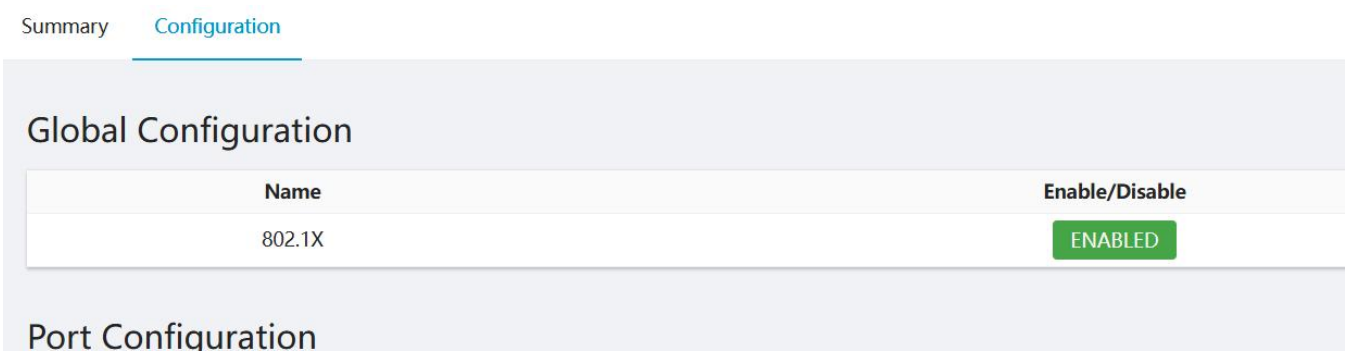
Figure 6-52 RADIUS Server Display Interface



Step 3: Enable 802.1X authentication global enable.

Select [Configuration] [Security] [Dot1x] in the navigation bar, enter the page shown in Figure 6-53, click the "Status" [Enable/Disable] button, and click the [Apply] button to enable 802.1X authentication.

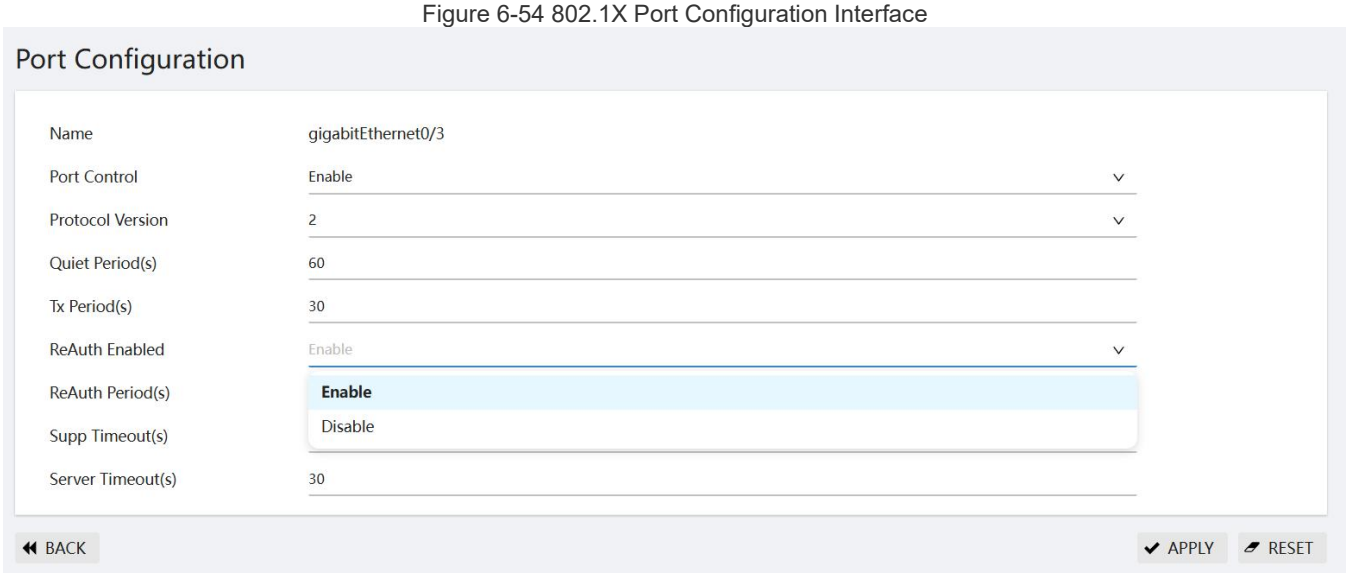
Figure 6-53 802.1X Global Configuration Interface



Step 4: Configure switch port 3 to enable 802.1X authentication globally.

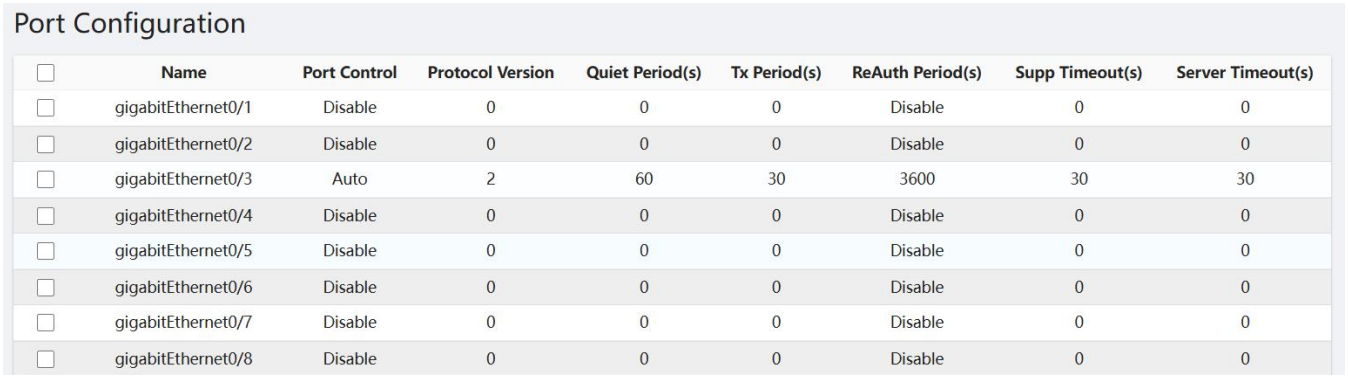
In the current interface, click the [Bulk Configuration] button under "Port Configuration" to enter the 802.1X port configuration page, enable the port to be controlled, the protocol version is "2", and select GigabitEthernet 0/3 for the port panel. As shown in Figure 6-54。

Figure 6-54 802.1X Port Configuration Interface



Click the [Confirm] button to complete the configuration, automatically return to the following interface, as shown in Figure 6-55, you can see the creation of a successful ordinance.

Figure 6-55 802.1X Port Configuration Display Boundary



Step 5: Configure the Authentication Client

Enable the 802.1X authentication client and log in using the account test.

The corresponding authentication method needs to be supported, such as the EAP-MSCHAPv2 method.

6.6 MAC accreditation

6.6.1 summarize

Introduction to MAC Address Authentication

MAC address authentication is an authentication method to control the user's network access rights based on the port and MAC address, which does not require the user to install any client software.After the device detects the user's MAC address for the first time on the port where MAC address authentication is activated, it starts the authentication operation for the user.During the authentication process, the user is not required to manually enter a user name or password.If the user is successfully authenticated, the user is allowed to access network resources through the port; otherwise, the user's MAC address is added as a silent MAC, and during the silent time (which can be configured by the silent timer), the device directly discards user messages from this MAC address when they arrive to prevent repeated authentication of illegal MACs within a short period of time.

attention (heed)

If the configured static MAC is the same as the silent MAC, the MAC silencing function will be disabled after a MAC address authentication failure。

The device currently supports MAC address authentication:
-Remote authentication through a RADIUS (Remote Authentication Dial-In User Service) server.
Currently, MAC address authentication supports two types of username formats:
-MAC Address Username: Uses the user's MAC address as the username and password for authentication.

6.6.2 Configuring MAC Authentication

View MAC Certification Overview

Select [Security] [MAC Authentication] in the navigation bar to enter the MAC Authentication Overview screen, such as the page shown in Figure 6-56.In the "Profile", you can display the MAC authentication configuration, and the description of each parameter is shown in Table 6-57.

Figure 6-56 MAC Authentication Overview Screen

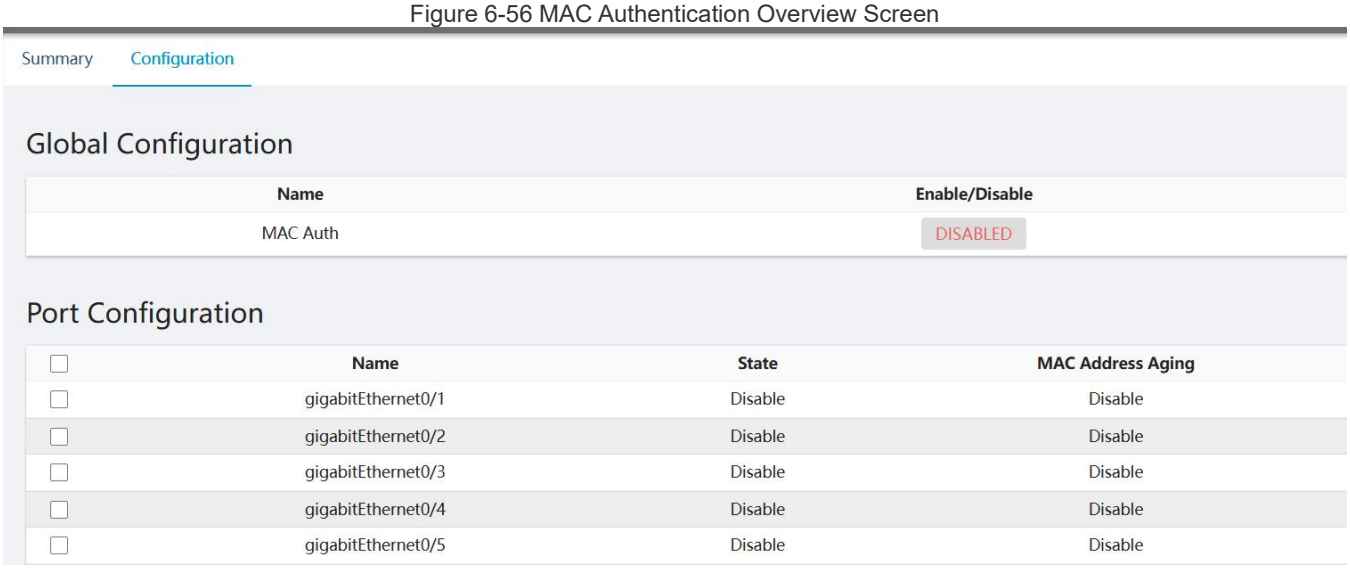


Table 6-57 MAC Profile Parameter Descriptions

configuration item	clarification

global configuration	state of affairs	function switch
	RADIUS deployments	Click to jump to the RADIUS configuration interface
Port Configuration	name	port name
	state of affairs	Function status, on or off
	MAC address aging	Whether to enable MAC aging
	manipulate	Click to edit the regulation

Configuring MAC Authentication

Select "Security > MAC Authentication > Configuration" in the navigation bar to enter the page shown in Figure 6-58.On this page, you can configure 802.1X globally as well as on an individual port basis.The configuration parameters are described in Table 6-59.

Figure 6-58 MAC Authentication Configuration Interface

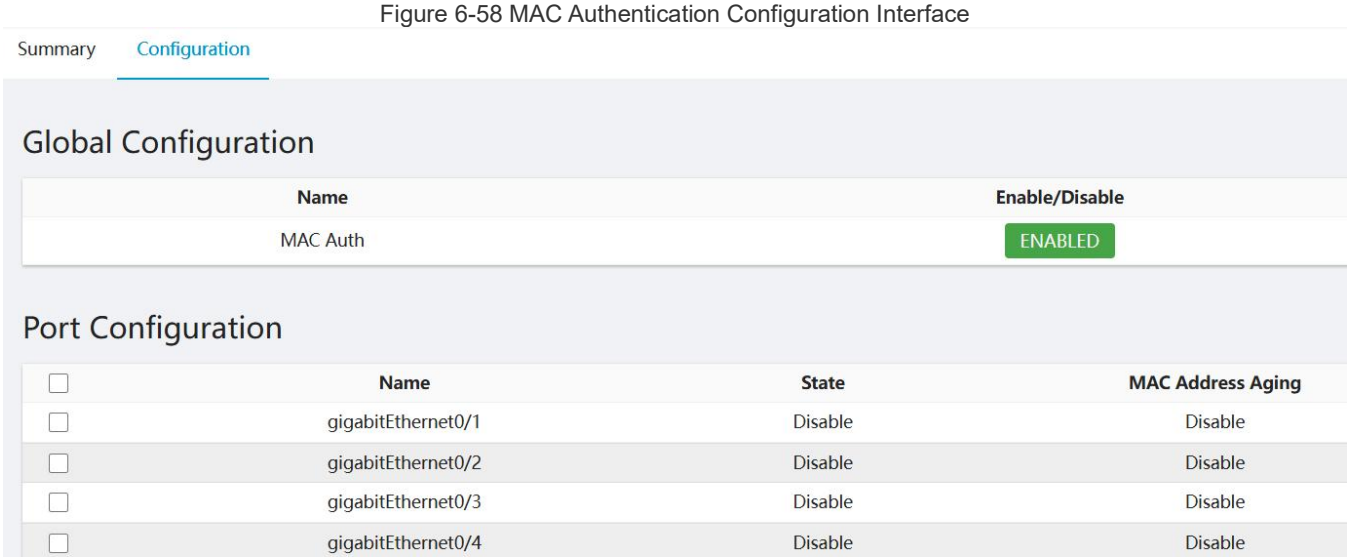


Table 6-59 Description of MAC Profile Parameters

configuration item		instructions
Port Configuration	state of affairs	Enable/disable this function
	state of affairs state of affairs	Whether to enable MAC aging

6.6.3 summarize

RADIUS (Remote Authentication Dial-In User Service, Remote Authentication Dial-In User Service) is a commonly used protocol to implement AAA (Authentication, Authorization and Accounting).

Introduction to RADIUS

RADIUS is a distributed, client/server structure of the information interaction protocol, can protect the network from unauthorized access to the interference, often used in both the requirements of high security, but also allows remote user access to a variety of network environments.The protocol defines the RADIUS message format and its message transmission mechanism, and provides for the use of UDP as the transport layer

protocol for encapsulating RADIUS messages (UDP ports 1812 and 1813 are used as authentication and billing ports respectively).

RADIUS was initially only a AAA protocol for dial-up users, but later, with the diversified development of user access methods, RADIUS also adapts to a variety of user access methods, such as Ethernet access, ADSL access.It provides access services through authentication and authorization, and collects and records users' use of network resources through billing.

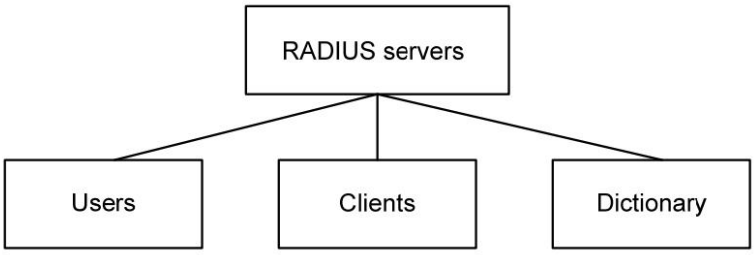
Client/Server Mode

-Client: The RADIUS client, generally located on the NAS device, can be distributed throughout the network, and is responsible for transmitting user information to the designated RADIUS server, and then conducts corresponding processing (e.g., accepting/declining user access) according to the information returned from the server.

-Server: A RADIUS server, typically running on a central computer or workstation, maintains relevant user authentication and network service access information, is responsible for receiving user connection requests and authenticating users, and then returns all required information to the client (e.g., accepting/rejecting authentication requests).

A RADIUS server typically maintains three databases, as shown in Figure 6-60.

Figure 6-60 RADIUS server composition creating a successful MAC authentication port



-Users": Used to store user information (e.g. user name, password and configuration information such as protocol used, IP address, etc.).

-Clients": Used to store information about RADIUS clients (e.g., shared key of the access device, IP address, etc.).

-Dictionary": Used to store information about attributes in the RADIUS protocol and the meaning of attribute values.

Security and Authentication Mechanisms

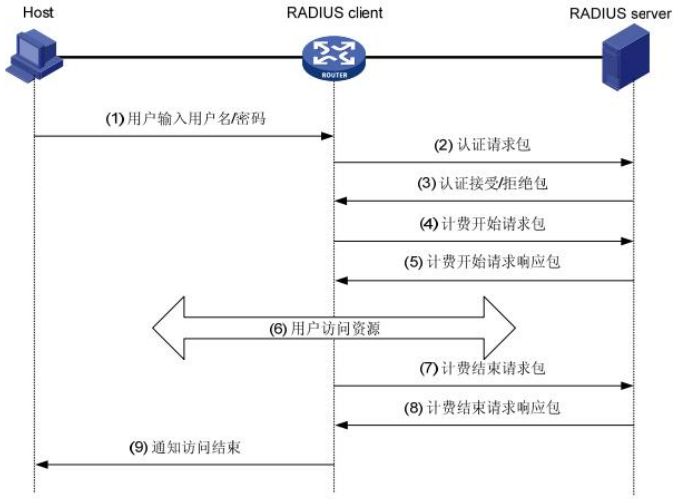
The interaction of authentication messages between the RADIUS client and the RADIUS server is accomplished through the participation of the shared key, and the shared key cannot be transmitted over the network, which enhances the security of information interaction.In addition, passwords are encrypted during transmission to prevent theft of user passwords when they are transmitted over an insecure network.

The RADIUS server supports multiple methods to authenticate users, such as PPP-based PAP and CHAP authentication.In addition, the RADIUS server can act as a proxy to communicate with other RADIUS authentication servers as a RADIUS client, responsible for forwarding RADIUS authentication and billing messages.

Basic RADIUS Message Interaction Flow

The interaction flow between a user, a RADIUS client, and a RADIUS server is shown in Figure 6-61.

Figure 6-61 Basic Message Interaction Flow of RADIUS



The message interaction flow is as follows:

(1) The user initiates a connection request and sends a username and password to the RADIUS client.

(2) The RADIUS client sends an authentication request packet (Access-Request) to the RADIUS server on the basis of the user name and password obtained, in which the password is encrypted by the MD5 algorithm with the participation of the shared key.

(3) The RADIUS server authenticates the user name and password.If the authentication is successful, the RADIUS server sends an authentication acceptance packet (Access-Accept) to the RADIUS client; if the authentication fails, it returns an authentication rejection packet (Access-Reject).Since the RADIUS protocol merges the processes of authentication and authorization, the authentication acceptance packet also contains the user's authorization information.

(4) The RADIUS client accesses/denies the user based on the received authentication result.If the user is allowed to access, the RADIUS client sends a Billing Start Request packet (Accounting-Request) to the RADIUS server.

(5) The RADIUS server returns the billing start response packet (Accounting-Response) and starts billing.

(6) The user starts accessing network resources;

(7) The user requests to be disconnected and the RADIUS client sends a billing stop request packet (Accounting-Request) to the RADIUS server.

(8) The RADIUS server returns a billing end response packet (Accounting-Response) and stops billing.

The user ends access to the network resource.

---

clarification

Our device does not support RADIUS billing function

6.7 RADIUS

6.7.1 deployment RADIUS

RADIUS Global Configuration

在 Select [Configuration] [Security] [RADIUS] in the navigation bar to enter the RADIUS global configuration interface, as shown in Figure 6-62.The description of each parameter of the global configuration is shown in Table 6-63.

Figure 6-62 RADIUS Global Configuration Interface

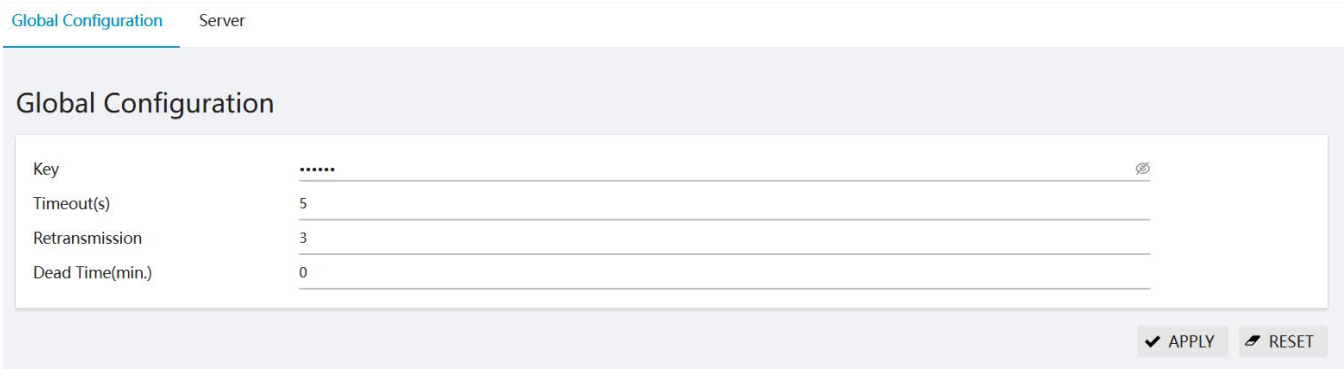


Table 6-63 Description of RADIUS Global Configuration Parameters

configuration item		clarification
global configuration	cryptographic	Global default password configuration; configurable, not readable; optional configuration
	overtime pay	Global server timeout; optional configuration
	retransmission	Global server retransmission count; optional configuration
	Time of death	Server death duration; optional configuration; default 0, indicating that the server is resurrected immediately after death

RADIUS Server Configuration

In the current interface, click the [Add] button under "Server Configuration" to enter the server configuration interface, as shown in Figure 6-64.The description of each server parameter is shown in Table 6-65.

Figure 6-64 RADIUS Server Configuration Interface

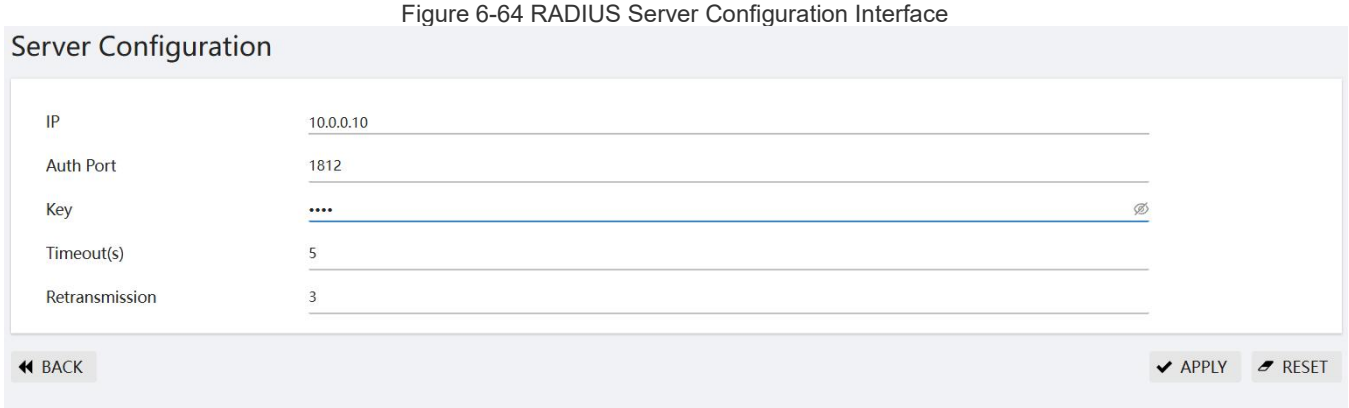


Table 6-65 Description of MAC Profile Parameters

configuration item	instructions
IP	server IP address

authentication port	Server authentication port number; default 1812
cryptographic	Server key; global configuration is used when no configuration is available
overtime pay	Server timeout; default 5s
retransmission	Number of server retransmissions, default 3

6.8 port security

6.8.1 summarize

The Port Security function achieves the purpose of restricting illegal users' access to the port by limiting the number of legal MAC addresses of the port, and the messages with illegal MACs will be directly discarded. The legal MAC can be generated either statically or dynamically.Static legal MACs are generated through user command line configuration; dynamic legal MACs are generated dynamically through the MAC address learning function.

When the number of secure addresses on the port has reached the maximum number of secure addresses configured value, new MAC access to the port will be recognized as an illegal MAC, resulting in a violation event, the user can configure the response to the generation of the violation event, respectively, restrict or shutdown port.

Restrict: Prohibit illegal MAC data from passing through, and generate alert log message.The illegal MAC will be prohibited from accessing the port during the MAC address aging time.It can be restored by shutdown, no shutdown port.

Shutdown: force the port to be down, and configurable port recovery time, the port will be recovered automatically when the time is up; it can also be recovered by shutdown, no shutdown command.

If you want to convert a dynamic security user to a static security user, you can enable the sticky function on the port.If you enable the sticky function on the port, the dynamic user learned on the port will exist as a static user, and if you save the configuration, the dynamic user will still exist after the device reboots.

---

clarification

only supports L2 ports to configure port security, such as normal physical ports, aggregated ports.

only supports configuring port security function in access mode.

does not support configuring port security function for member ports of aggregation ports.

does not support the destination port of SPAN to configure the port security function.

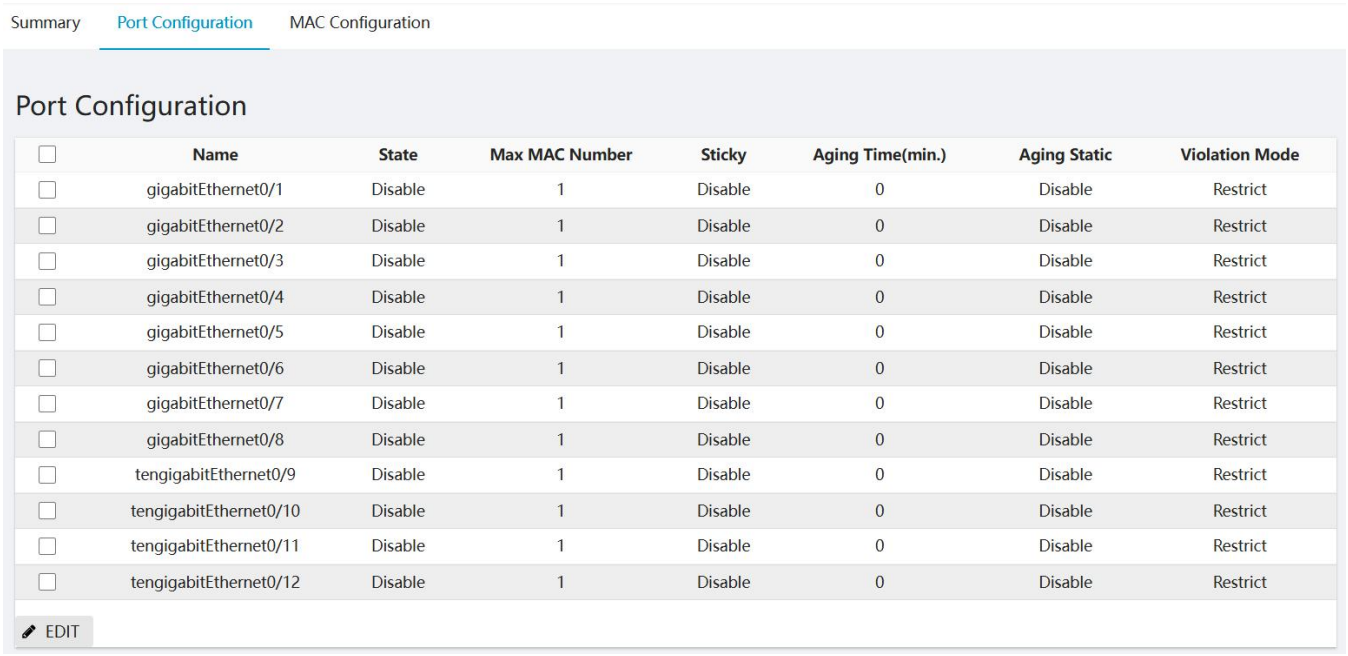
does not support configuring the port security function on configured static MAC address ports.

6.8.2 Configuring Port Security

Port Configuration

Select [Security] [Port Security] [Port Configuration] in the navigation bar to enter the Port Configuration Overview screen, as shown in Figure 6-66.

Figure 6-66 Port Configuration Overview



Click the [Edit] button under "Port Configuration" to enter the Port Configuration page, as shown in Figure 6-67.The description of each parameter of Port Configuration is shown in Table 6-68.

Figure 6-67 Port Configuration Page

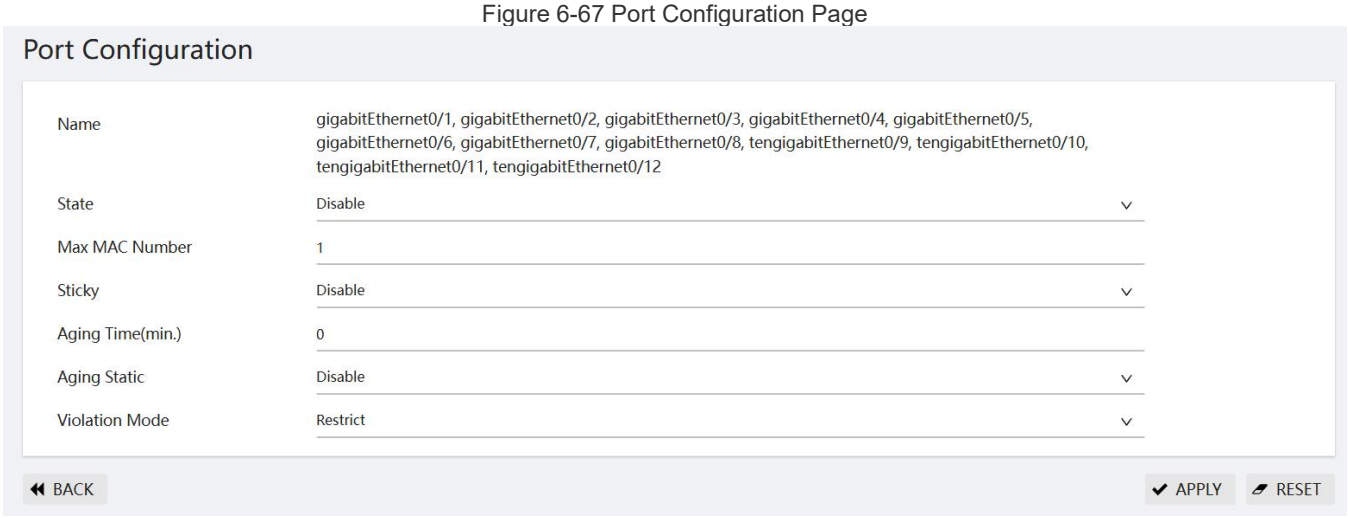


Table 6-68 Description of Port Configuration Parameters

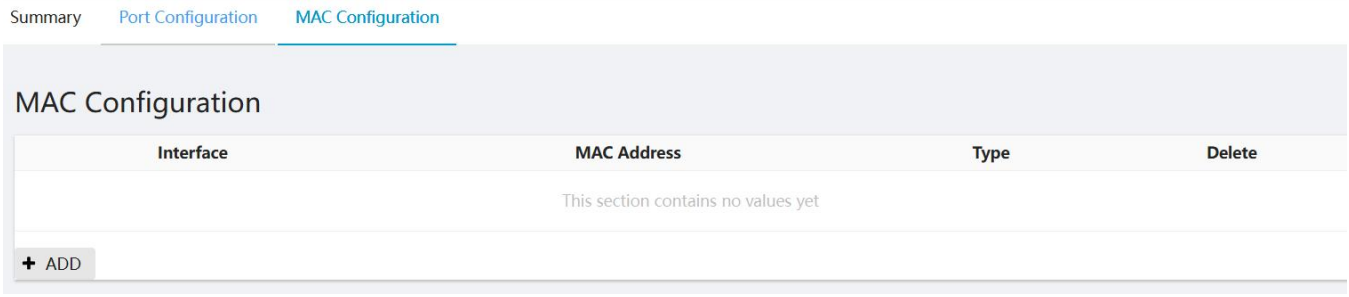
configuration item		clarification
Port Configuration	state of affairs	Enable/disable port security on the interface
	Maximum number of MACs	Configure the maximum number of secure MAC addresses for the port, the default maximum number of secure addresses is 1, range <1-1024>.
	Sticky	Enable/disable Sticky function
	aging time	Configure the security address aging time in minutes.The default aging time is 0, indicating that the aging function is turned off The aging time range is <0-1440>. The default aging function takes effect only for dynamic, sticky secure addresses
	Aging static addresses	Configuring Enabling Static Secure Address Aging

	default mode	Configure the port security violation processing, the default violation processing mode restricted Restrict: prohibit the passage of illegal user data, and log alerts Shutdown: Shut down the port and restore it after errdisable recovery time. shutdown/no shutdown commands, the same can be restored.

MAC deployment

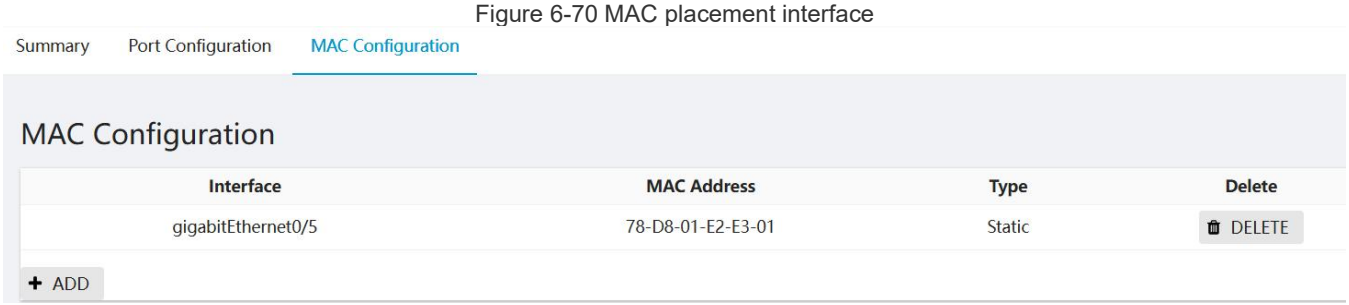
Select [Security] [Port Security] [MAC Configuration] in the navigation bar to enter the MAC Configuration Overview screen, as shown in Figure 6-69.

Figure 6-69 MAC Overview Screen



Click the [Add] button under "MAC Configuration" to enter the MAC configuration page, as shown in Figure 6-70.

Figure 6-70 MAC placement interface



The description of each parameter of the MAC configuration is shown in Table 6-71.

Table 6-71 Description of MAC Configuration Parameters

configuration item		clarification
Port Configuration	connector	Select the interface to be configured
	MAC address	Configure a static secure address, secure address format: XXXX.XXXX.XXXX The secure address cannot be a broadcast or multicast address
	typology	Configure the MAC address as Static or Sticky

6.8.3 Configuration Example

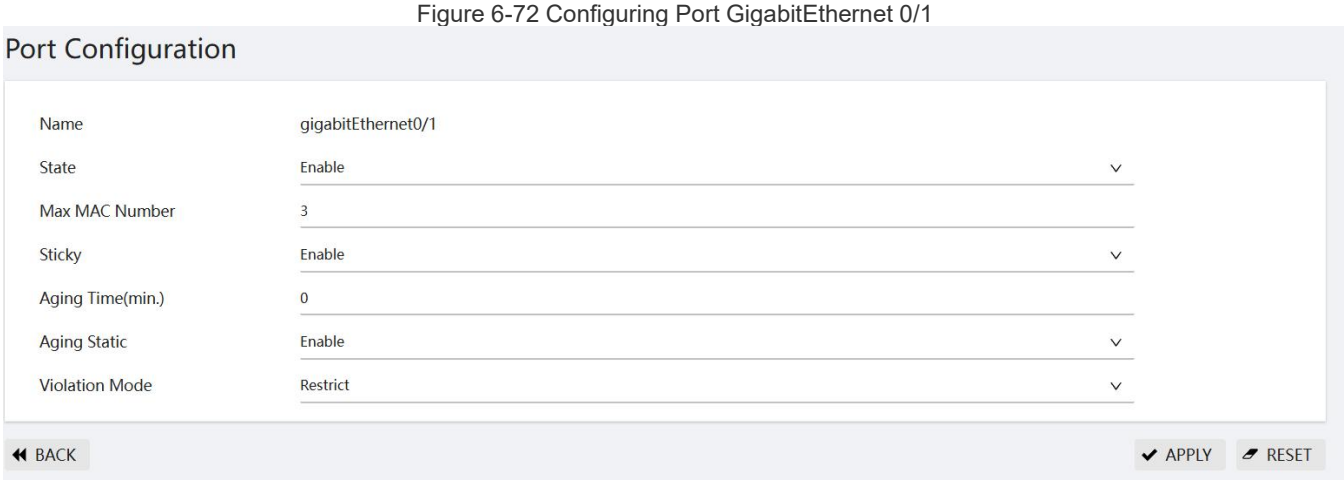
1) demand (economics)

- limits the number of legitimate users on interface GigabitEthernet 0/1 to 3. Illegal users with MACs 0001.0001.0001, 0001.0001.0002, and 0001.0001.0003, respectively, cannot access the device.

2) Typical Configuration Example

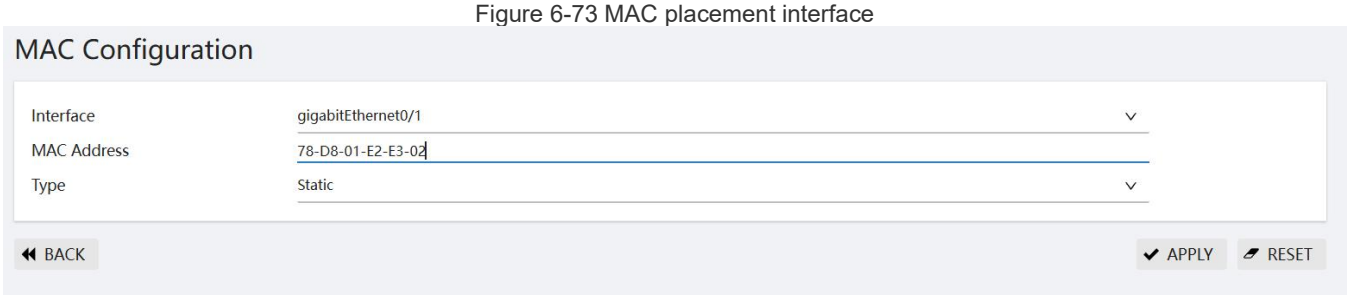
Step 1: Select [Security] [Port Security] in the navigation bar, click the [Batch Configuration] button under "Port Security" to enter the port configuration interface, select GigabitEthernet 0/1 in the port panel, and configure other settings as shown in Figure 6-72 below.

Figure 6-72 Configuring Port GigabitEthernet 0/1



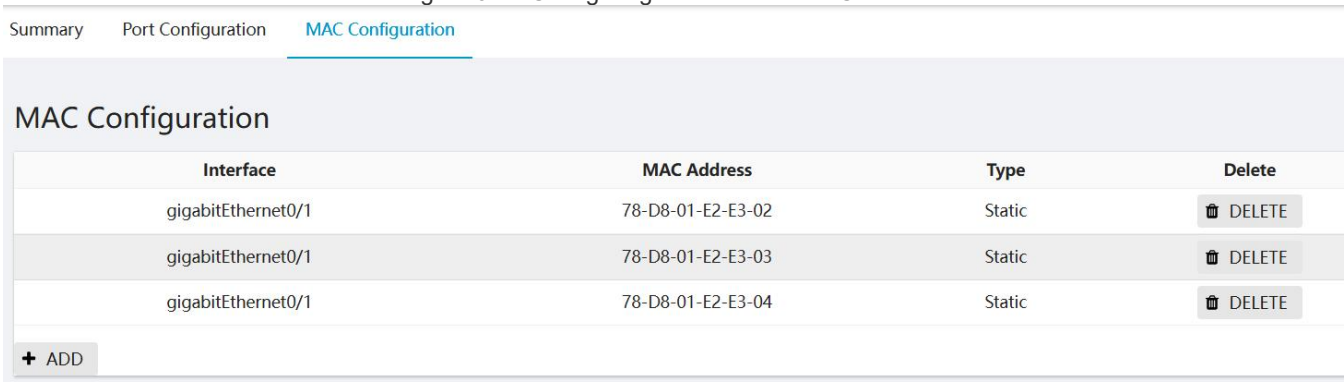
Step 2: In the current page, click "MAC Configuration" below the [Add button], enter the MAC configuration interface, interface selection GigabitEthernet 0/1, in the MAC address dialog box, enter "0001.0001.0003".In the MAC address dialog box, enter "0001.0001.0003", select "Static", the specific configuration is shown in Figure 6-73 below.

Figure 6-73 MAC placement interface



In the MAC address field, enter the three static addresses in turn, and the interface after successful configuration is shown in Figure 6-74.

Figure 6-74 Configuring a Successful MAC Address



6.9 IP Source Guard

6.9.1 summarize

IP Source Guard：

The Ip Source Guard binding function allows IP messages that match the IP+MAC binding to pass through the port, while messages that do not match are directly discarded, thus preventing IP/MAC spoofing attacks. There are two main sources of Ip Source Guard binding entries: user static configuration and dynamic acquisition in the ip dhcp snooping environment.

User Static Configuration: Mainly for host users with static IP addresses in the local area network.

Ip dhcp snooping dynamic acquisition: mainly to deal with host users in the local network who dynamically acquire IP addresses through dhcp.

IP/MAC Spoofing Attack: Illegal MAC users, send IP messages with legitimate source IPs to legitimize their access identity.

ARP Check:

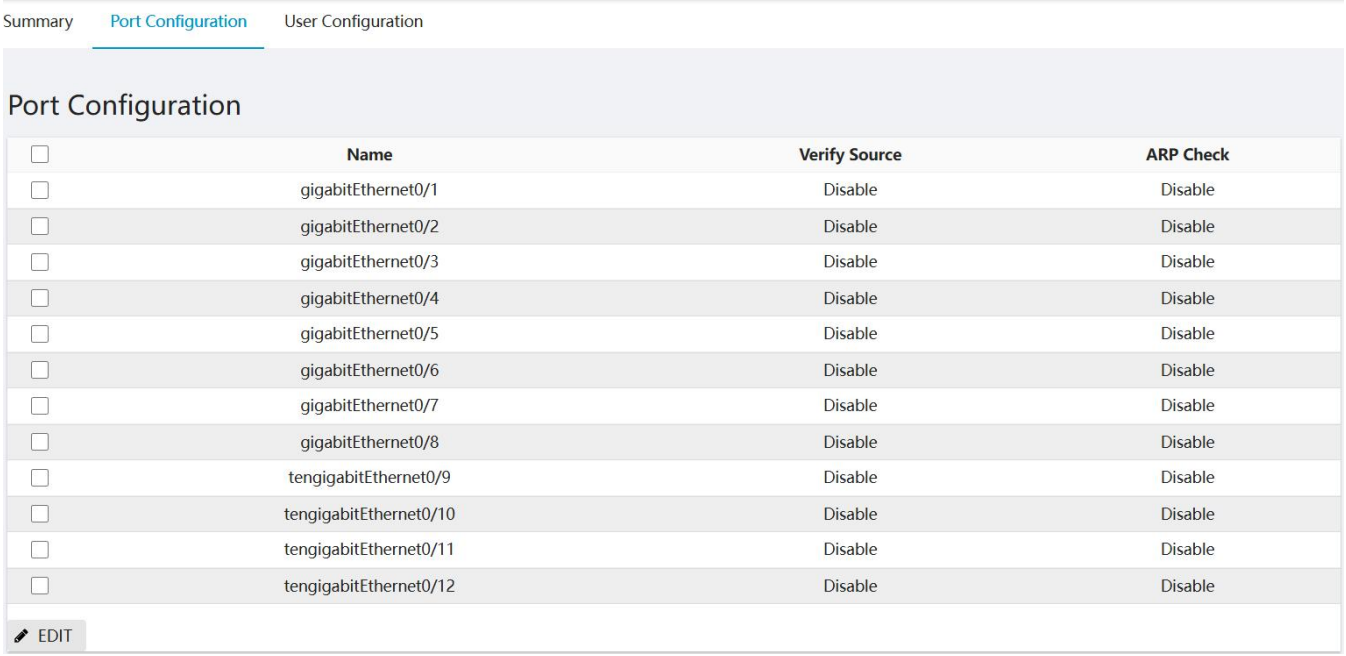
Arp-check (ARP message checking) function filters all ARP messages under the port and discards all illegal ARP messages, which can effectively prevent ARP spoofing in the network and improve the stability of the network.

In devices that support the Arp-check function, the Arp-check function can generate corresponding ARP filtering information according to the legitimate user information (IP+MAC) generated by security application modules such as IP Source Guard, thus realizing the filtering of illegal ARP messages in the network.

6.9.2 IP Source Guard

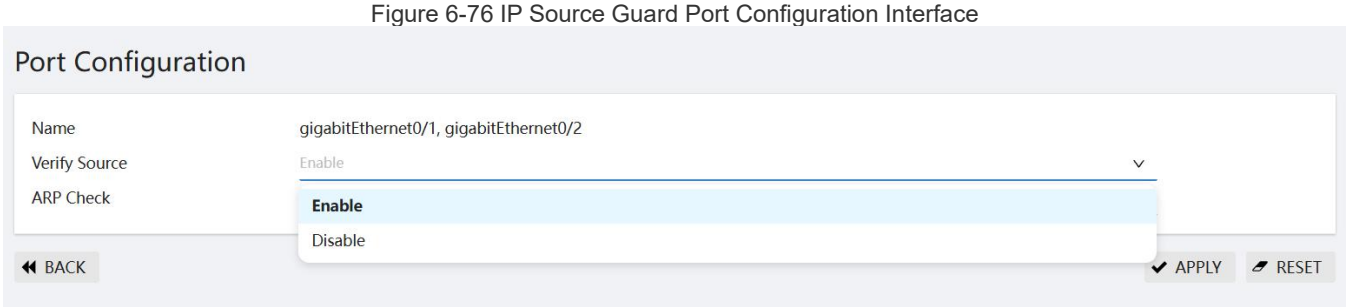
Step 1: Select [Configuration] [Security] [IP Source Guard] in the navigation bar to enter the IP Source Guard port configuration overview page, as shown in Figure 6-75.

Figure 6-75 IP Source Guard Overview Screen



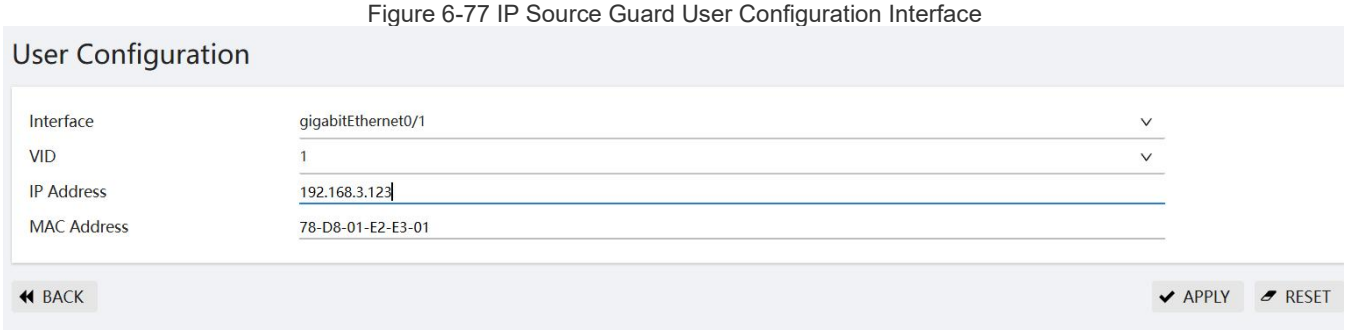
Step 2: On the current page, click the [Batch Configuration] button under "Port Configuration" to enter the IP Source Guard port configuration interface.Select the port to be configured, click "Verify Source" button, as shown in Figure 6-76, click [Confirm] button to complete the configuration.

Figure 6-76 IP Source Guard Port Configuration Interface



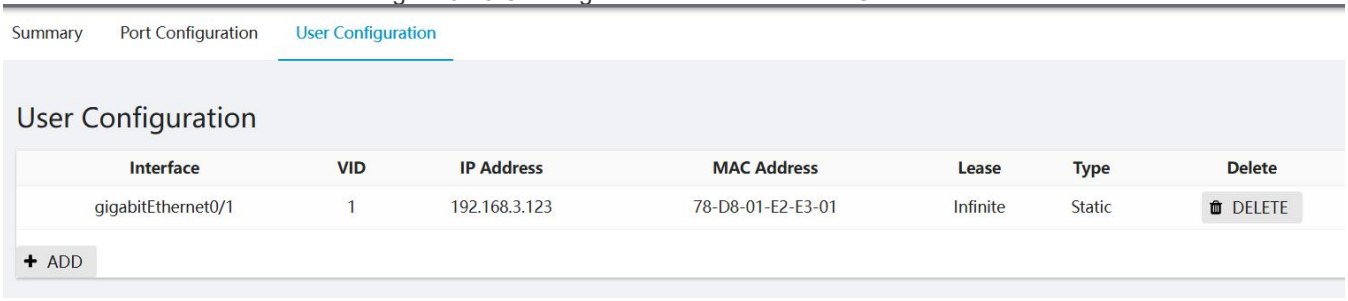
Step 3: On the current page, click the [Add] button under "User Configuration" to enter the IP Source Guard user configuration interface.Select the interface to be configured, VID, enter the MAC address and IP address, as shown in Figure 6-77.

Figure 6-77 IP Source Guard User Configuration Interface



Click the [Confirm] button to complete the configuration, and you can see the successfully created IP Source Guard rule in the user configuration interface, as shown in Figure 6-78.

Figure 6-78 Creating a Successful IP Source Guard Rule

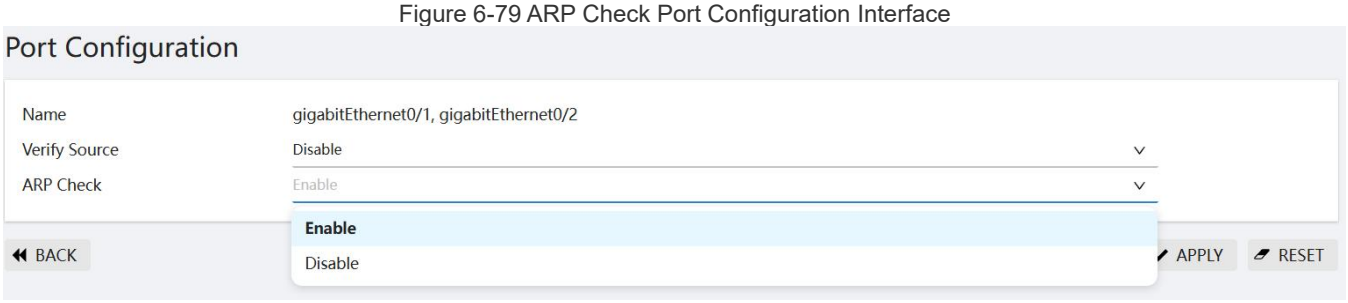


6.9.3 Configuring ARP Check

Step 1: Select [Configuration] [Security] [IP Source Guard] in the navigation bar to enter the IP Source Guard port configuration overview page.

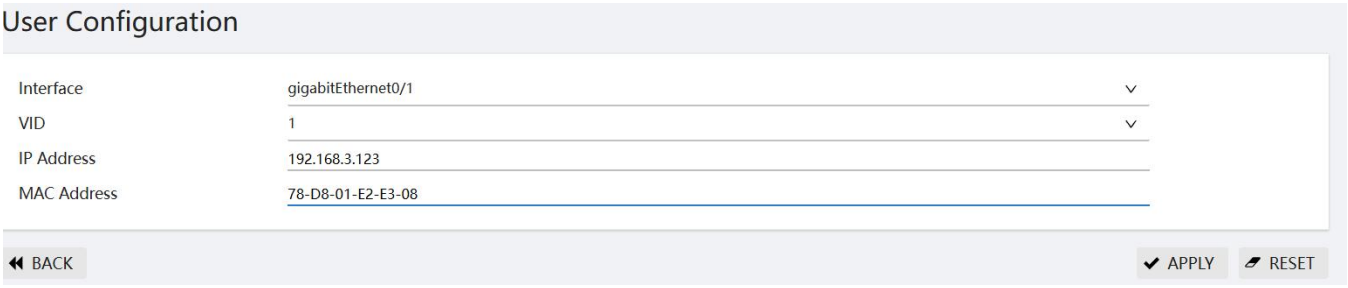
Step 2: On the current page, click the [Batch Configuration] button under "Port Configuration" to enter the IP Source Guard port configuration interface.Select the port to be configured, click the "ARP Check" button, as shown in Figure 6-79, click the [Confirm] button to complete the configuration.

Figure 6-79 ARP Check Port Configuration Interface



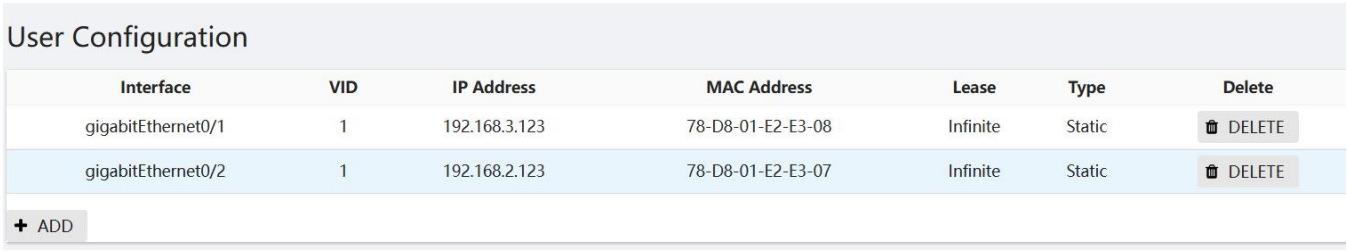
Step 3: On the current page, click the [Add] button under "User Configuration" to enter the IP Source Guard user configuration interface.Select the interface to be configured, VID, enter the MAC address and IP address, as shown in Figure 6-80.

Figure 6-80 ARP Check Port Configuration Interface



Click the [Apply] button to complete the configuration and see the successfully created ARP Check rule in the User Configuration interface, as shown in Figure 6-81.

Figure 6-81 Creating a Successful ARP Check Rule



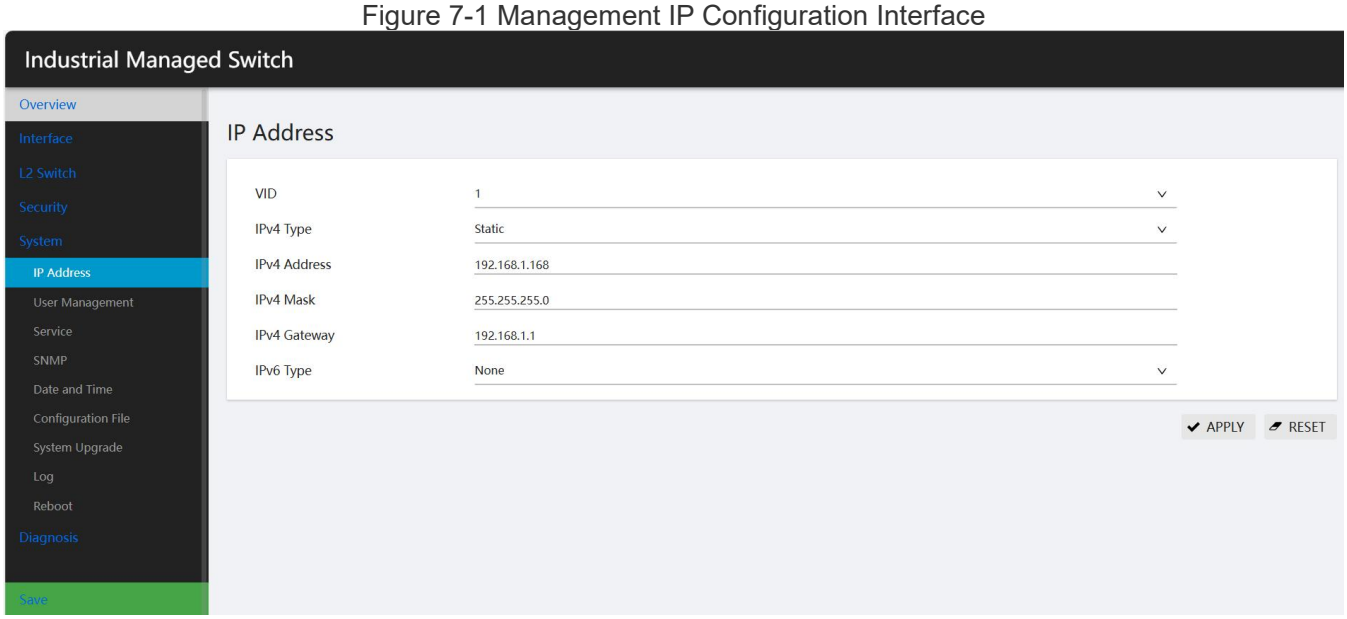
7 systems

7.1 Management Information

attention (heed)

- After changing the IP address, you need to manually re-access the switch by pointing the web page to the new address.

Figure 7-1 Management IP Configuration Interface



As in Figure 5-3, select [System] [Management Information] in the navigation bar to enter the IP address management interface, and the description of each parameter is shown in Table 7-2.

Table 7-2 Parameter Description

configuration item	clarification

VID	Management VLAN configuration to specify which VLAN to use as the management VLAN, which must already exist.
IPV4 type	None: No IPV4 management address is used. Static: Indicates that the IPv4 address is specified by manual configuration, you need to set the IPv4 address and mask length when selecting this item. DHCP: Indicates that the IPv4 address is obtained through DHCP allocation.
IPV4 address	Set the IPV4 management IP address, which is available when "static" is selected for the IPv4 address acquisition method.
IPV4 mask	Set the subnet mask, the default is 255.255.255.0, which is available when "static" is selected as the IPv4 address acquisition method.
IPV4 gateway	Specify the IP address of the gateway, available when "static" is selected for IPv4 address acquisition.
IPV6 type	None: No IPV6 management address is used. Static: Indicates that the IPv6 address is specified by manual configuration, you need to set the IPv6 address when you select this item. DHCP: Indicates that the IPv6 address is obtained through DHCP assignment.
IPV6 address	Set the IPV6 management IP address, which is available when "static" is selected for the IPv6 address acquisition method.
IPV6 prefix length	Set the IPV6 prefix length, available when "static" is selected as the acquisition method for IPv6 addresses.
IPV6 Gateway	Set up an IPV6 gateway, available when "static" is selected for IPv6 address acquisition.

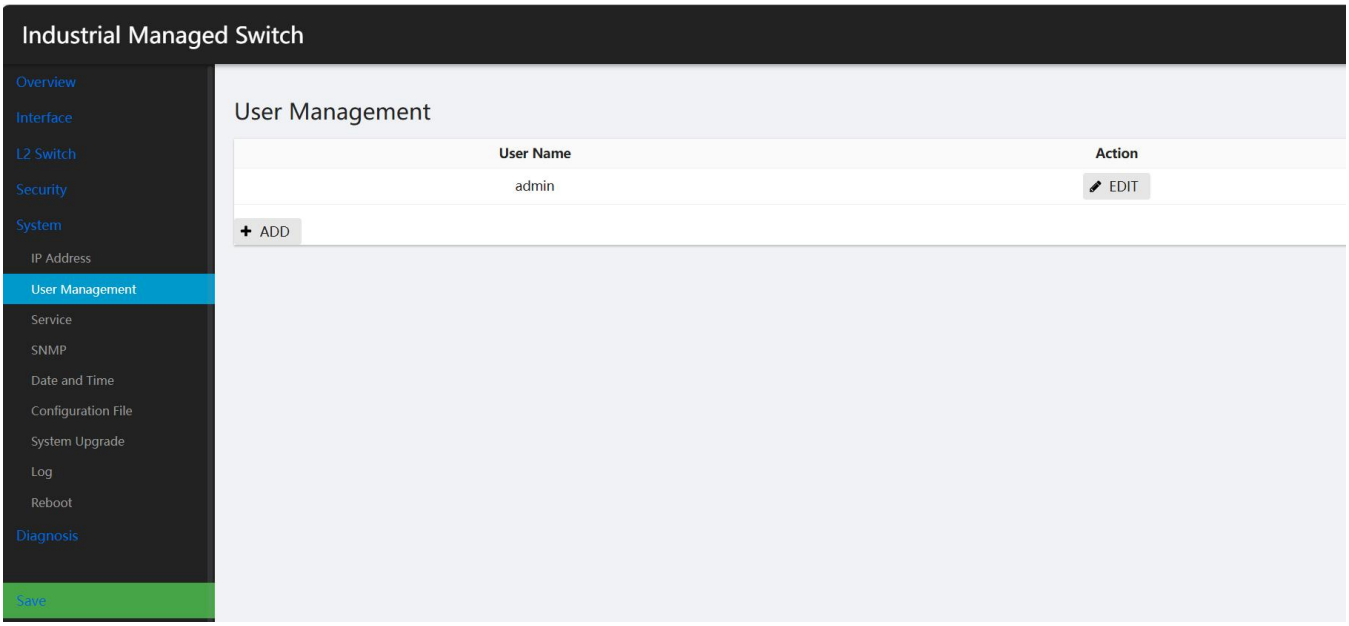
7.2 user management

attentio

- In order to improve the security of the device, please change the password as soon as possible, after the change of the password, please be sure to save, forget the password will lead to the inability to log in the device

Click the navigation bar [System] [User Management] to enter the user management interface, as shown in Figure 7-3 interface.

Figure 7-3 User Management Interface



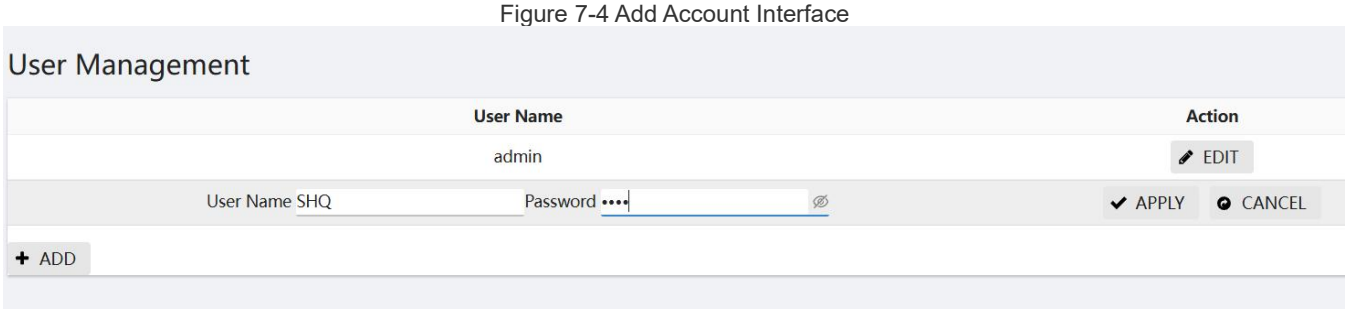
Add account steps:

Step 1: Click [System] [User Management] in the navigation bar to enter the user management interface.

Step 2: Click the [Add] button to enter the add account interface, as shown in Figure 7-4.

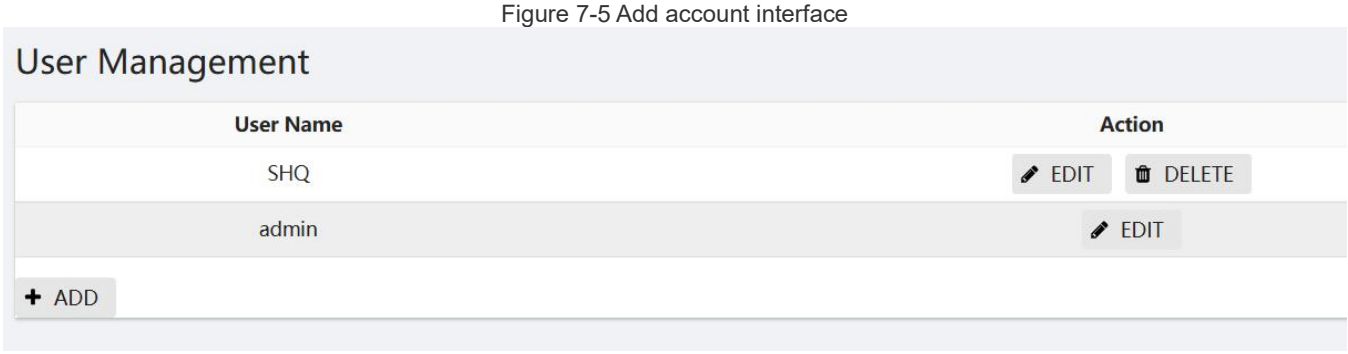
After logging into the device for the first time, please change the password as soon as possible, repeat the new password twice according to the prompts, as shown in Figure 7-4.The password consists of numbers and letters, the length of the password is 0-32 bytes, and the letters are case-sensitive.

Figure 7-4 Add Account Interface



Step 3: Click the [Save] button to complete the configuration, the interface automatically returns to the account display interface, as shown in Figure 7-5, you can see the newly created account.

Figure 7-5 Add account interface



Step 4: Click the [Save] button on the navigation bar to save the configuration.

7.3 Enable/disable services

Overview of service management:

1. Telnet service

Telnet protocol belongs to the application layer protocol in the TCP/IP protocol family and is used to provide remote login and virtual terminal functions in the network.

2. SSH Service

SSH stands for Secure Shell.When a user remotely logs in to a device through a network environment that is not secure, SSH can provide security by utilizing encryption and strong authentication to protect the device from attacks such as IP address fraud and plaintext password interception. 3.

3. HTTP Service

HTTP stands for Hypertext Transfer Protocol.It is used to transfer Web
page information over the Internet. HTTP is located at the application layer of the TCP/IP stack.
When HTTP service is enabled on the device, users can log in to the device via the HTTP protocol and access and control the device using Web functions.

4. HTTPS Service

HTTPS (Hypertext Transfer Protocol Secure) is an HTTP protocol that supports the SSL (Secure Sockets Layer) protocol. HTTPS improves the security of the device in the following aspects through the SSL protocol:

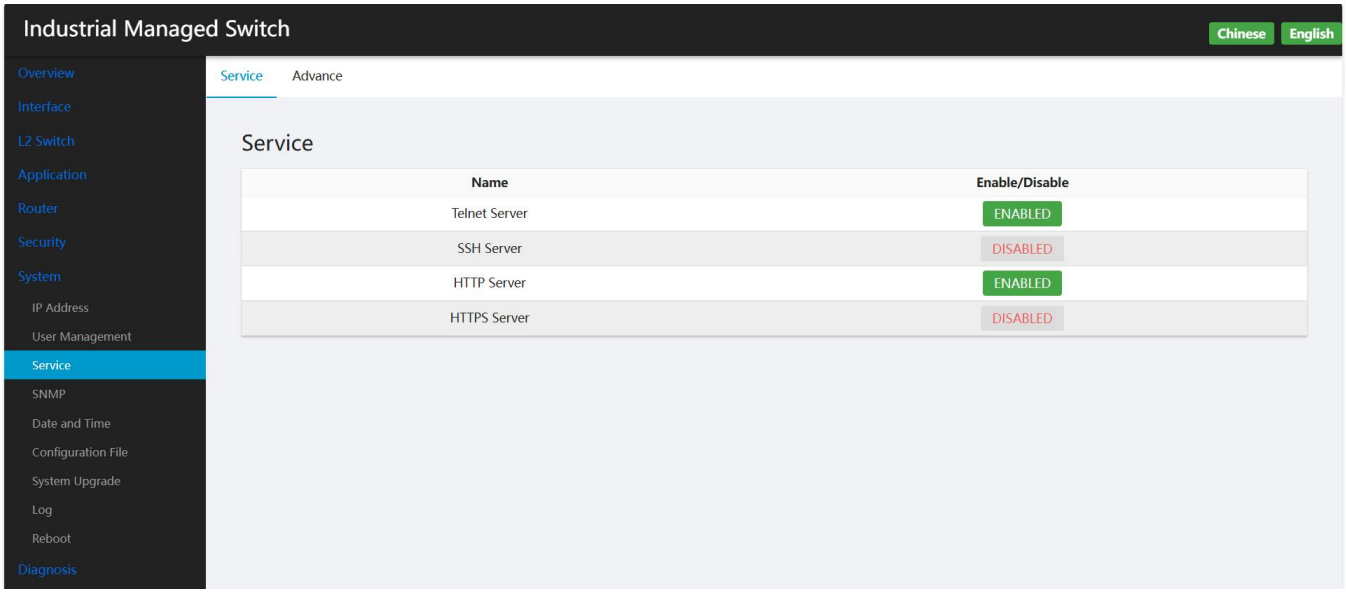
- The SSL protocol ensures that legitimate clients can access the device securely and prohibits illegal clients from accessing the device;
- The data interacting between the client and the device needs to be encrypted, which ensures the security and integrity of data transmission, thus realizing the security management of the device;
- The access control policy based on certificate attributes is formulated for the device to control the access rights of clients, which further avoids illegal clients from attacking the device.

Configuration steps.

(1) As shown in Figure 7-6, select [Maintenance] [System Settings] in the navigation bar to enter the configuration interface.

(2) Click the check box in front of the Service option and click the [Confirm] button to enable/disable the service.

Figure 7-6 Service Configuration Screen



7.4 SNMP

7.4.1 summarize

SNMP (Simple Network Management Protocol) is a network management standard protocol in the Internet, which is widely used to realize the access and management of managed devices by management devices.SNMP has the following characteristics:

-Supports intelligent management of network devices.Using the SNMP-based network management platform, network administrators can query the operational status and parameters of network devices, set parameter values, discover faults, complete troubleshooting, perform capacity planning and generate reports.

-Supports the management of devices with different physical characteristics. SNMP provides only the basic set of functions, making the management tasks relatively independent of the physical characteristics of the managed devices and networking technology, thus realizing the management of devices from different vendors.

7.4.2 SNMP working mechanisms of the United Nations

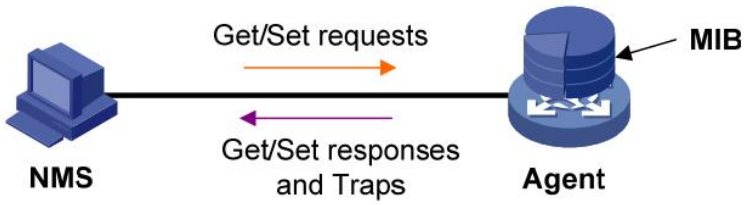
SNMP network consists of two elements, NMS and Agent.

NMS (Network Management System) is the manager of the SNMP network, which can provide a very friendly human-computer interface to facilitate network administrators to complete most of the network management work.

-Agent is the managed 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 messages 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. the MIB defines the hierarchical relationship between nodes and a series of attributes of an object, such as the object's name, access rights, and data type.Each Agent has its own MIB, and the managed device has its own MIB file, which can be compiled on the NMS to generate the MIB of the device.The NMS reads/writes the MIB nodes according to the access privileges to realize the management of the Agent.The relationship between the NMS, the Agent and the MIB is shown in Figure 7-7.

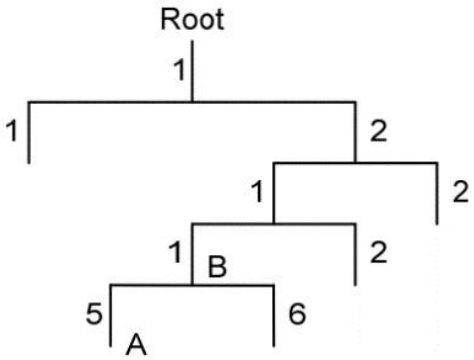
Figure 7-7 NMS, Agent, and MIB Relationships



MIB is organized according to a tree structure, which consists of many nodes, each node represents a managed object, which can be uniquely identified by a string of numbers representing a path starting from the root, which is called OID (Object Identifier).

As shown in Figure 7-8, managed object B can be uniquely identified with a string of numbers {1.2.1.1}, which is the OID of managed object B.

Figure 7-8 MIB Tree Structure



SNMP provides four basic operations to enable NMS and Agent interaction:

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

-SET operation: The 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 a Trap message to the NMS. the Agent does not require the NMS to send a response message.

The Agent does not require the NMS to send a response message, and the NMS does not respond to the Trap message.Trap operations are supported in SNMPv1, SNMPv2c, and SNMPv3.

7.4.3 SNMP protocol version

Currently, the Agent supports SNMPv1, SNMPv2c, and SNMPv3:

-SNMPv1 uses the Community Name authentication mechanism.SNMPv1 uses the Community Name authentication mechanism. The Community Name is similar to a password and is used to restrict communication between the NMS and the Agent.

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, which results in the NMS not

being able to access the Agent, and the alarm messages sent by the Agent will be discarded by the NMS.

The alarm messages sent by the Agent will also be discarded by the NMS.

-SNMPv2c also adopts the group name authentication mechanism. SNMPv2c extends the functions of SNMPv1: it provides more operation types, supports more data types, and provides richer error codes, which can distinguish errors in more detail.

-SNMPv3 uses USM (User-Based Security Model) authentication mechanism.The network administrator can set the authentication and encryption functions.Authentication is used to verify the legitimacy of the sender of the message to avoid access by illegal users; encryption encrypts the transmission message between the NMS and the Agent to avoid eavesdropping.The use of authentication and encryption can provide higher security for the communication between NMS and Agent.

clarification

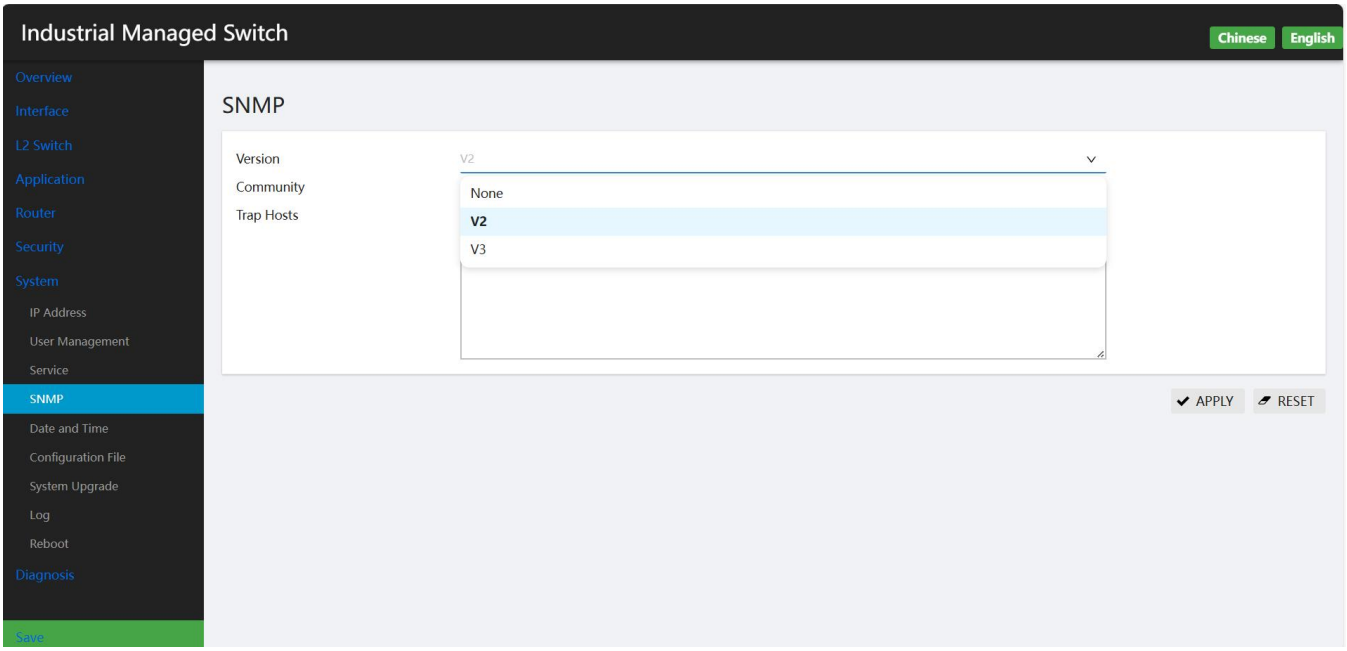
A prerequisite for a successful connection between the NMS and the Agent is that the SNMP version used by the

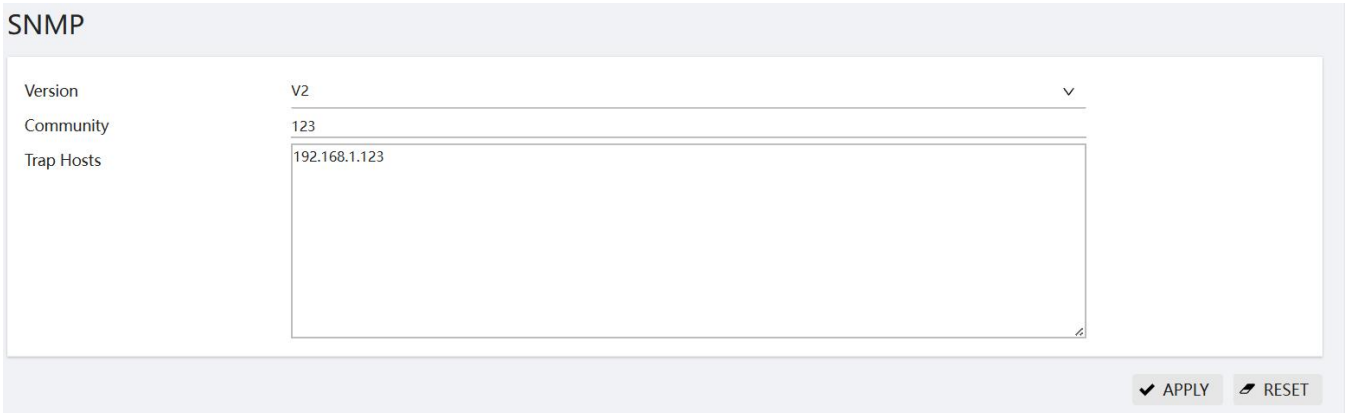
7.4.4 Deployment SNMP

(1) Select [System] [SNMP] in the navigation bar to enter the SNMP configuration interface.

(2) As shown in Figure 7-9, select the SNMP version, configure the user, authentication\encryption password, Trap host, and click the [Apply] button to complete the configuration.

Figure 7-9 NMS, Agent, and MIB Relationships





7.5 Date and time

To ensure that this device works in coordination with other devices, users need to configure the system time accurately.The Date and Time Setting module is used to display and set the system time on the Web network management and set the system time zone.The device supports manual configuration of system time and automatic synchronization of NTP (Network Time Protocol) server time.

NTP (Network Time Protocol) is a time synchronization protocol defined by RFC 1305 for time synchronization between distributed time servers and clients.The purpose of using NTP is to clock synchronize all devices with clocks within a network so that the clocks of all devices within the network remain consistent, thus enabling the devices to provide a variety of applications based on a uniform time.For a local system running NTP, it can both accept synchronization from other clock sources and act as a clock source to synchronize other clocks, and it can synchronize with other devices to each other.

7.5.1 View the current date and time of the system

(1) Select [System] [Date & Time] in the navigation bar to enter the date and time interface, as shown in Figure 7-10, and the parameter description is shown in Table 7-11.

(2) View the current date and time of the system displayed in real time on the page.

Figure 7-10 Date and Time Configuration Interface

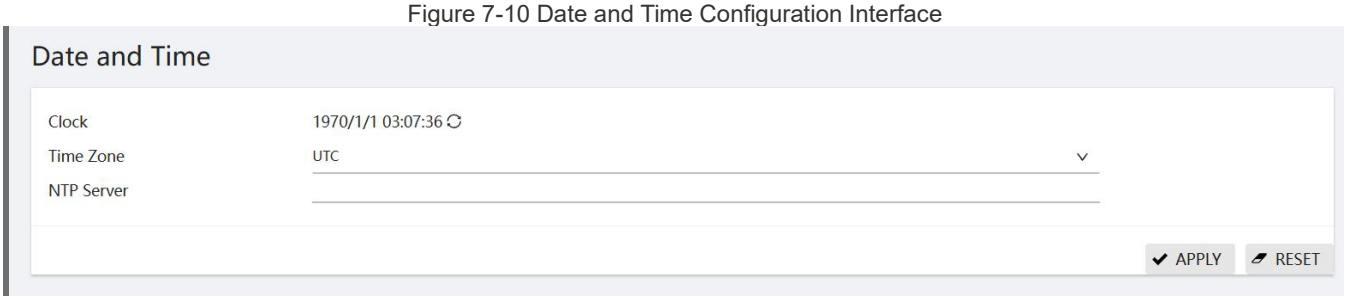


Table 7-11 NTP Parameter Descriptions

configuration item	clarification
time zones	Select Time Zone
dates	System date
timing	system time
NTP server IP	NTP server IP address

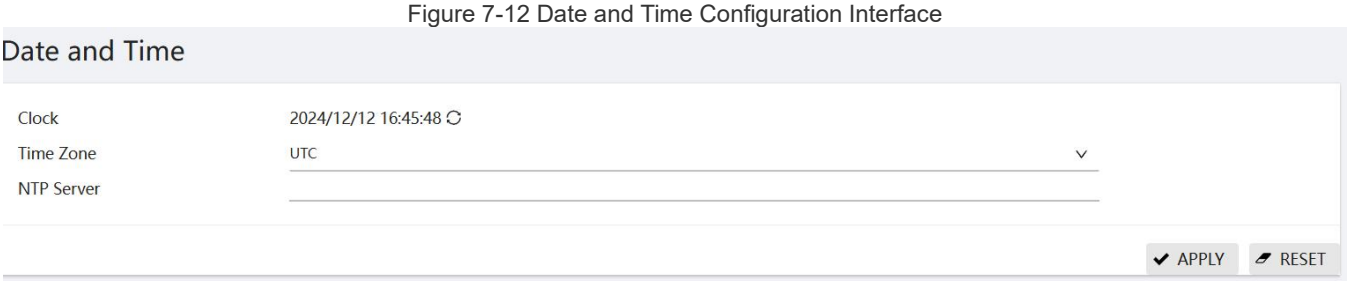
7.5.2 Manually configure the system's date and time

（1）Select [System] [Date/Time] in the navigation bar to enter the time management interface.

（2）Click the Synchronize button behind the clock and then click the [Apply] button, as shown in Figure 7-12, which synchronizes the switch time and PC time.

（3）Click the [Save] button on the navigation bar to save the current configuration.

Figure 7-12 Date and Time Configuration Interface



clarification

- For devices without built-in RTC, the time and date will revert to factory settings after the device reboots, and you need to reconfigure the time and date.

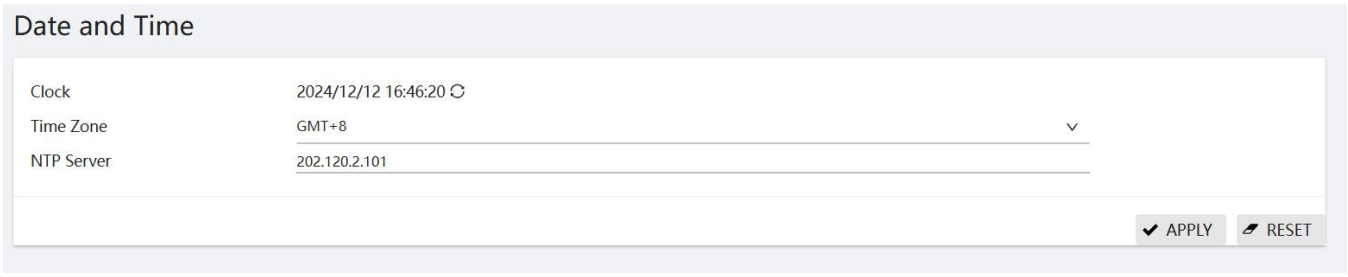
7.5.3 Configuring Network Time

(1) Select [System] [Date & Time] in the navigation bar to enter the time management interface.

(2) Enter the corresponding server address in the NTP Server IP text box and click [Apply] to complete the configuration, as shown in Figure 7-13.

(3) Click the [Save] button in the navigation bar to save the current configuration.

Figure 7-13 Date and Time Configuration Screen



clarification

- It is required that the device must be able to access the NTP server.

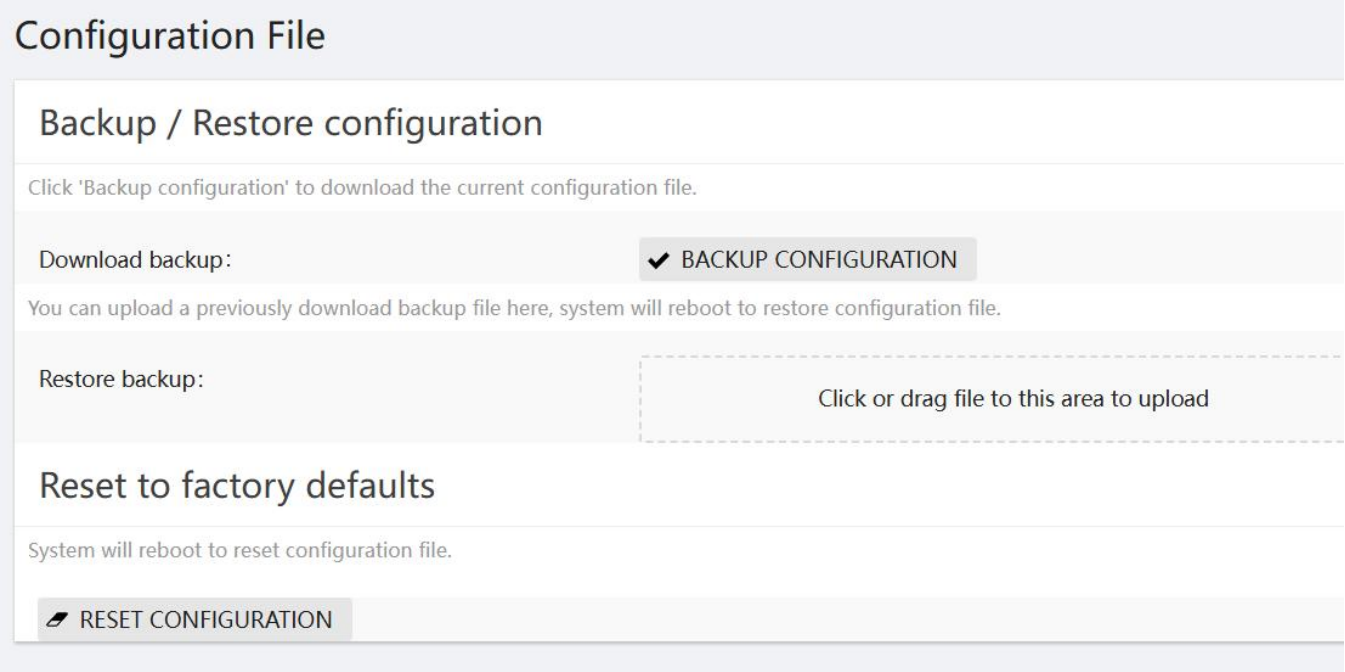
- After the configuration is completed, the device will automatically synchronize the time information from the server, the first time to complete the time synchronization takes about 4-8 minutes.
- For devices without built-in RTC, the time and date will be restored to factory settings after reboot, and devices that have been previously configured with an NTP server will automatically synchronize with the NTP server. The time and date will be restored to the factory settings after reboot for devices without built-in RTC.

7.6 configuration file

Configuration backup function, you can realize to download the configuration of the local machine to the computer for restoring the configuration or importing it to other devices.

Select [Configuration File] in the [System] drop-down menu in the navigation bar to enter the configuration file management interface, as shown in Figure 7-14 interface.

Figure 7-14 Configuring Backup



Click the [Backup Configuration] button to bring up the "File Download" dialog box and save the configuration file locally.

7.6.1 Configuration Recovery

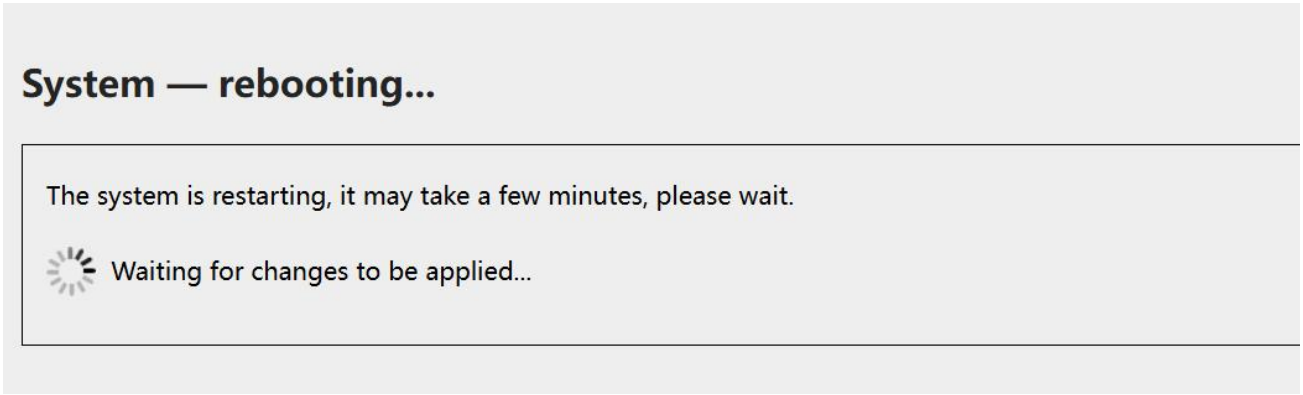
Configuration recovery function, which enables fast import of configuration files into the local machine.

Upload the downloaded backup configuration, the system will reboot automatically during the configuration restoration process.

Restore Backup:Select FileNo file selected √ Upload Configuration

As shown in Figure 5-25, click the [Select File] button, select the configuration file with the suffix .conf that needs to be imported, and click the [Upload Configuration] button. The device will automatically reboot during the import configuration process and wait for the interface as shown in Figure 7-15.

Figure 7-15 Configuration Recovery Waiting Screen



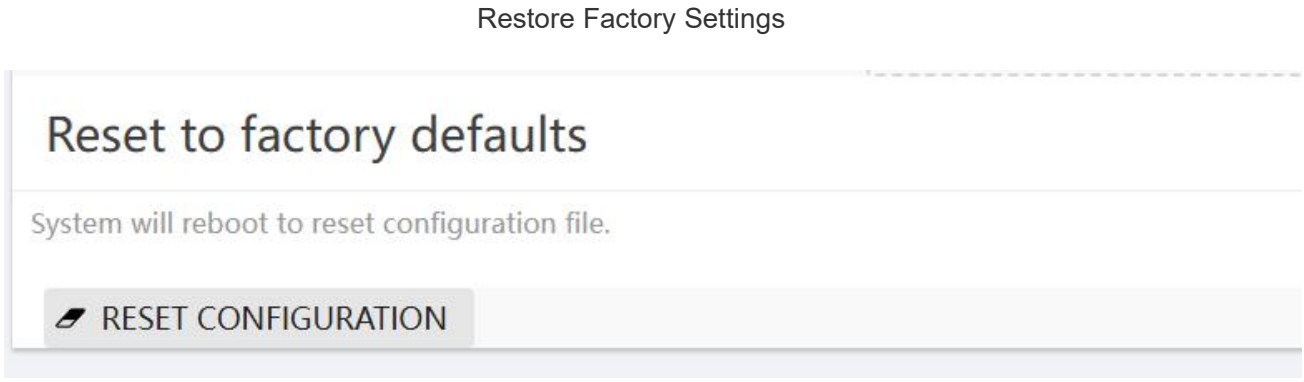
7.6.2 Restore Factory Settings

The Restore Factory Configuration module provides functions to restore all configurations in the device to the factory default configuration, delete the current configuration files, and reboot the device.

Step 1: Select [System] → [Profile Management] in the navigation bar.

Step 2: Click the [Restore Settings] button, as shown in Figure 7-16.

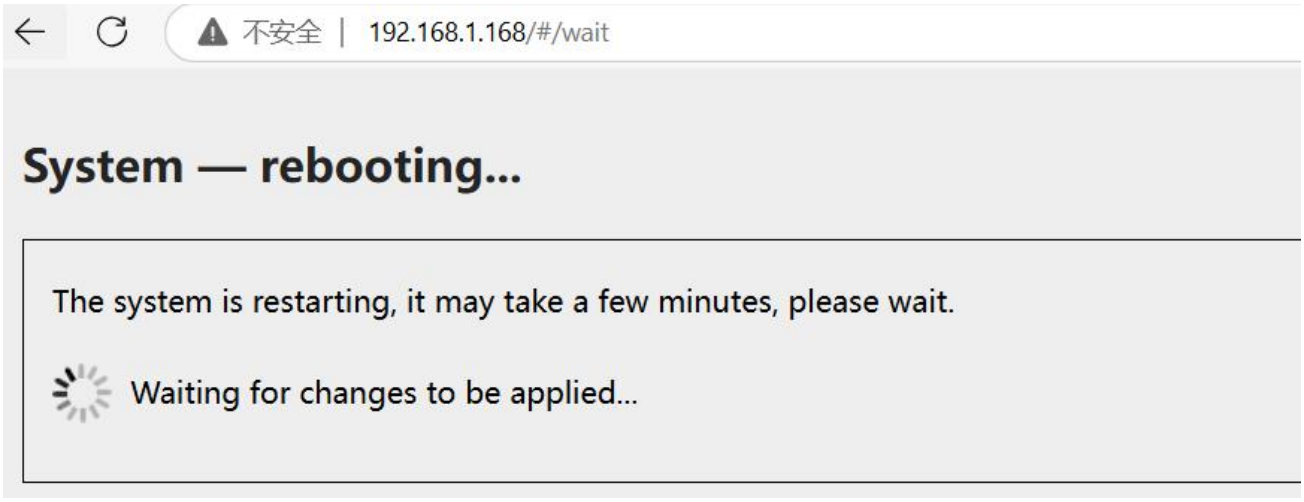
Figure 7-16 Restore Factory Settings Screen



The system will reboot automatically during the process of restoring factory settings

Step 3: Wait for the device reboot to complete, as shown in Figure 7-17. After the device reboot is complete, log in using the default IP, user name, and password.

Figure 7-17 Configuration Recovery Waiting Screen



The Software Upgrade module provides the ability to obtain a target application file from the local host and set that file as the startup file to be used the next time the device boots.

attention (heed)!

-The software upgrade will take some time. Do not perform any operations on the Web during the software upgrade process, as this may cause the software upgrade to be interrupted.

-The device will reboot automatically after the upgrade is completed.

Step 1: Select [System] -> [Firmware Upgrade] in the navigation bar to enter the "Upgrade Firmware" page, as shown in Figure 7-18.

Firmware Upgrade Interface 7-18

Step 2: Click the [Choose File] button and select the corresponding upgrade file in the pop-up dialog box, the upgrade file is in .bin format.Step 3: Click [Upgrade] or [Save Configuration & Upgrade] button to start the software upgrade.

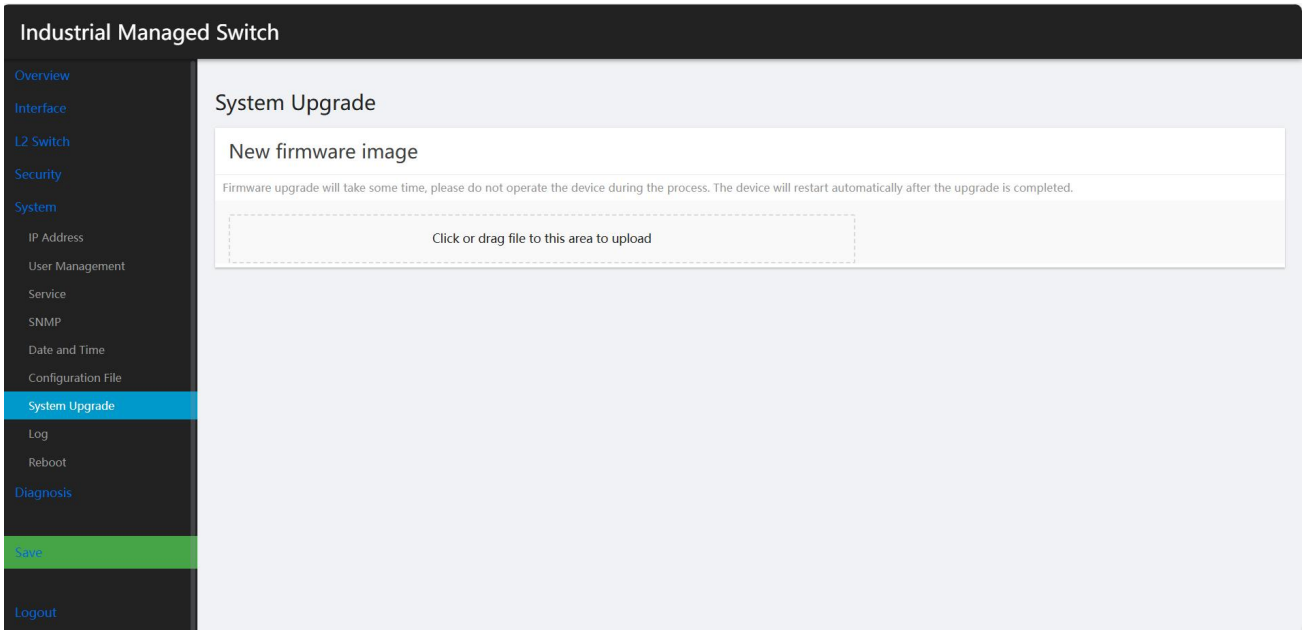
7.7 Logging/Diagnostics

Since each function module has its own corresponding operation information, in general, the user needs to view the display information module by module. In order to collect more information at one time during daily maintenance or in case of system failure, the device supports the diagnostic information module. When the user generates a diagnostic information file, the system will save the current running statistics of multiple function modules in a file named "backup-SWITCH-year-mon-day -log", which can be viewed by the user to locate the problem faster.

Step 1: Select [System] → [Log/Diagnostics] in the navigation bar as in Figure 7-19.

Step 2: Click the [Backup Log] button to bring up the "File Download" dialog box and save the log file locally.

Figure 7-19 Logging/Diagnostics Screen



7.7.1 Syslog server

7.7.1.1 summarize

During operation, the device will experience various state changes such as link status UP, DOWN, etc., and will also encounter events such as processing exceptions.The system log provides a series of

services that will automatically generate fixed-format messages when the status changes or events occur, and these messages will be recorded on the device log file.It supports displaying on the serial port, remote login terminal, and can also be sent to 1~3 groups of log servers on the network for administrators to analyze the network situation and locate problems.

In order to facilitate the administrator to read and manage the log messages, these log messages can be timestamped and graded according to the priority of the log messages.

7.7.1.2 Configuring the Syslog Server

Select [Maintenance] [Syslog Server] in the navigation bar to enter the Syslog Server Configuration interface, as shown in Figure 7-20, and the parameter descriptions are shown in Table 7-21.

Figure 7-20 Syslog Server Page

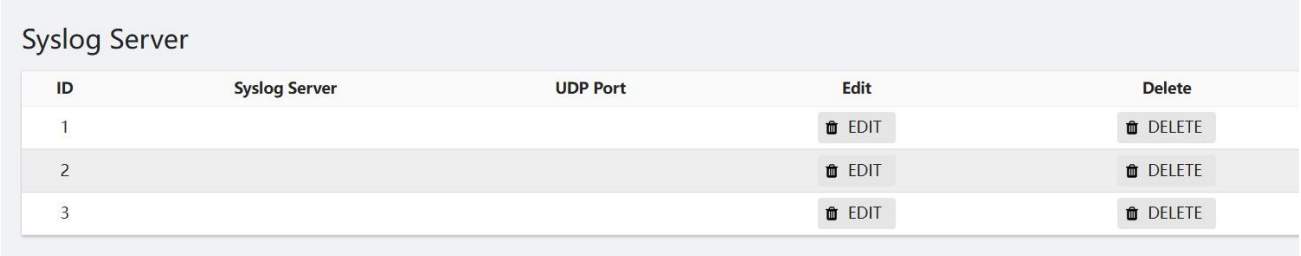


Table 7-21 Syslog Server Parameter Descriptions

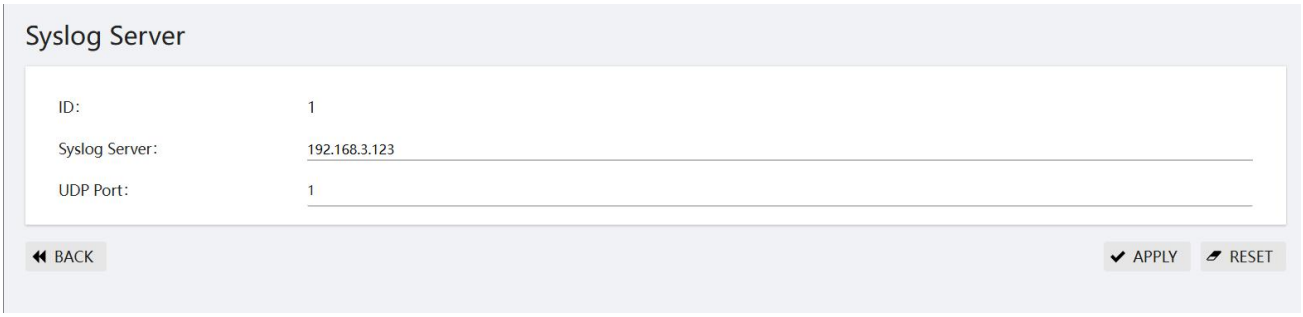
configuration item	clarification
ID	ID number of the server
Syslog server	Configure the IP address of the remote server, supports up to 3 remote server configurations
UDP port	Supports remote server UDP protocol port configuration, range <1-65535>; when no UDP port parameter is configured, the default port number is 514

Procedure.

(1) Select [System] [Log] [Syslog Server] in the navigation bar to enter the Syslog server configuration interface.

(2) Click the [Edit] button on the form to enter the Syslog server creation interface, fill in the parameters according to the requirements, as shown in Figure 7-22, click the [Apply] button to complete the configuration.

Figure 7-22 Syslog Server Configuration Interface



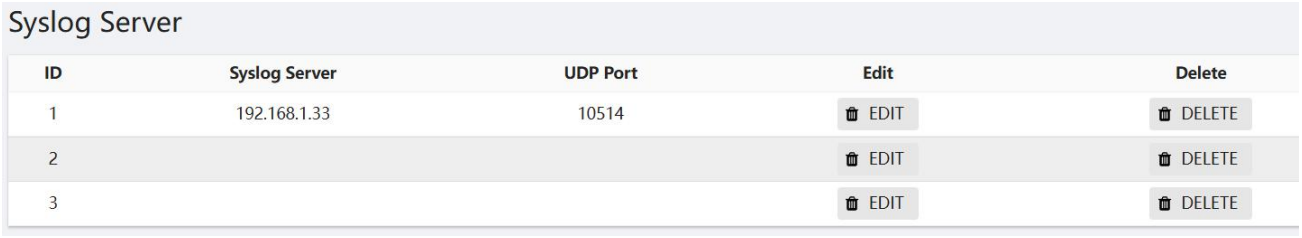
Configuration Example:

The device Syslog sends to the remote server, the device IP is 192.168.1.240, the remote server IP is 192.168.1.33, and the UDP port number is 10514.

Step 1: Select [System] [Log] [Syslog Server] in the navigation bar to enter the Syslog server configuration interface.

Step 2: Click the [Edit] button on the form to enter the Syslog server creation interface, fill in the parameters according to the requirements, and click [Apply] to complete the configuration, as shown in Figure 7-23.

Figure 7-23 Syslog Server Configuration Interface



Step 3: Click the [Save] button on the navigation bar to save the configuration.

8 diagnostic

8.1 network tool

8.1.1 summarize

Ping

By using the ping utility, the user can check whether the device at the specified IP address is reachable and test whether the network connection is faulty. ping is successfully executed as follows:

(1) The source device sends an ICMP echo request (ECHO-REQUEST) message to the destination device.

(2) The destination device receives the request message and sends an ICMP reply (ECHO-REPLY) message to the source device.

(3) The source device receives the ECHO-REPLY message and displays the relevant statistics.

The output information of ping is categorized as follows:

- The object of ping can be the IP address or host name of the destination device. If the host name of the destination device is unrecognizable, a prompt message is output on the source device.
- If the source device does not receive the ICMP echo response message from the destination device within the timeout period, the prompt message and the statistics of the ping process message are output; if the source device receives the response message within the timeout period, the number of bytes of the response message, the serial number of the message, the TTL (Time to Live), the

response time, and the number of bytes of the ping process message are output.ping process message statistics. ping process message statistics include the number of messages sent, the number of response messages received, the percentage of unresponsive messages, and the minimum, average, and maximum values of the response time.

Trace route

By using the trace route utility, users can view the Layer 3 devices through which messages are transmitted from the source device to the destination device.When the network fails, users can use this command to analyze the network node that fails. trace route is executed as follows:

(1) The source device sends a message with a TTL of 1 to the destination device.

(2) The first hop (that is, the first Layer 3 device reached by the message) responds with a TTL timeout ICMP message (which contains the IP address of the first hop), so that the source device gets the address of the first Layer 3 device.

(3) The source device resends a TTL of 2 to the destination device.

(4) The second hop responds with a TTL timeout ICMP message, and the source device gets the address of the second Layer 3 device.

(5) The above process continues until it finally reaches the destination device, and the source device gets the addresses of all the Layer 3 devices it has passed from it to the destination device.

The execution object of the trace route can be the IP address or host name of the destination device, and if the host name of the destination device is not recognizable, the source device gets the addresses of all the Layer 3 devices it has passed from it to the destination device.

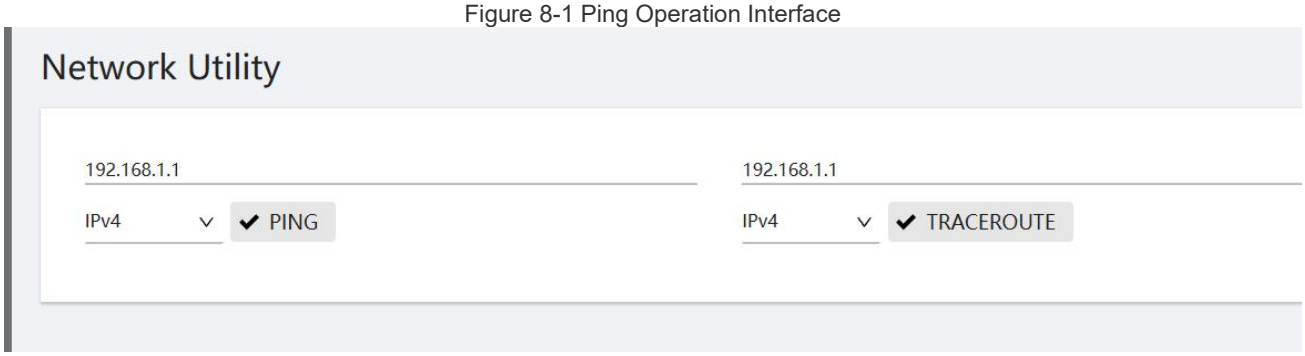
If the host name of the destination device is not recognized, a message is output on the source device.

8.1.2 ping gentle trace route operate

Ping operate

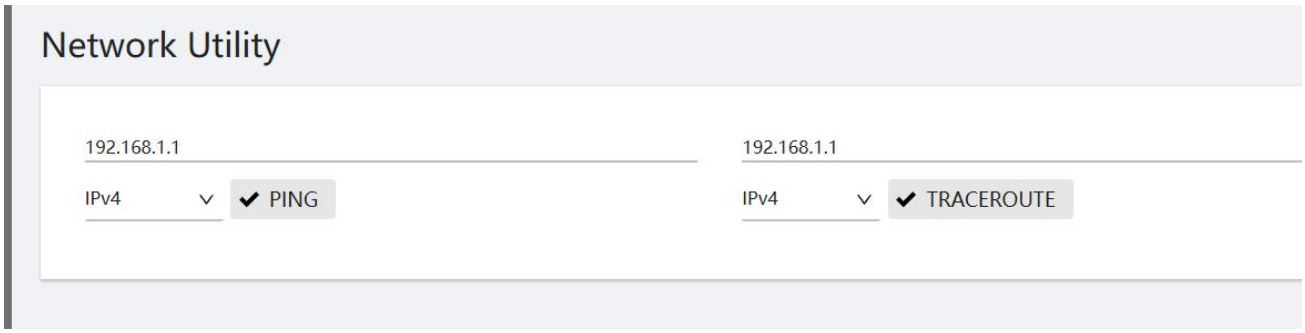
(1) Select [Diagnostics] [Network Tools] in the navigation bar to enter the ping/trace route page, as shown in Figure 8-1.Enter the IP address to be pinged in the ping operation IP address field and click the [Apply] button.

Figure 8-1 Ping Operation Interface



（2）View the returned results of the ping operation in the message box below, as shown in Figure 8-2.

Figure 8-2 Returned results of a ping operation



Trace route operate

(1) Select [Diagnostics] [Network Tools] in the navigation bar to enter the ping/trace route page, as shown in Figure 8-3.Enter the IP address to be pinged in the ping operation IP address field and click the [Apply] button.

Figure 8-3 Trace Route Operation Interface

（2）View the returned results of the ping operation in the message box below, as shown in Figure 8-4.

Figure 8-4 Trace Route Operation Return Results

8.2 power-down alarm

8.2.1 summarize

Dying-gasp function for the moment of disconnecting the device power supply, relying on the device's internal capacitors and other energy storage devices power supply for 10-20ms time, to support the device to send out the power-down alarm message.

According to the definition in 802.3ah, when a device power-down event occurs, the device sends out an OAM event message to its connected devices. Since OAM is a point-to-point protocol, the power-down event message will not continue to be forwarded after it reaches the next device that supports OAM.The device that receives the power-down event will output a power-down LOG alert message.

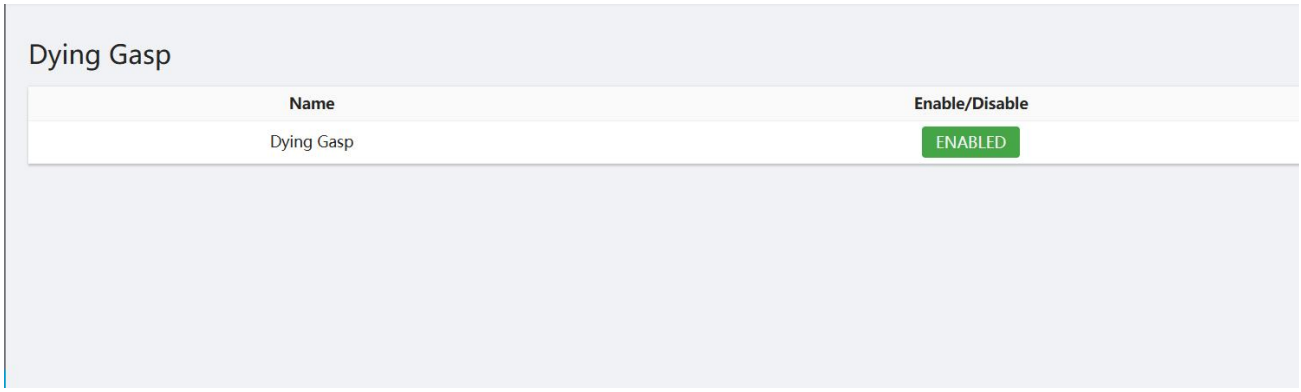
In addition to the OAM alert message, the power-down device will also send a trap message to the smmp server.

Node Information	digital
Mib files	DOT3-OAM-MIB.mib
oid	1, 3, 6, 1, 2, 1, 158, 1, 6, 1, 4
value	dyingGaspEvent(257)

8.2.2 Configure power-down alarms

Select [Diagnostics] [Dying Gasp] in the navigation bar to enter the Dying Gasp power-down alarm page, as shown in Figure 8-5, click the button under Enable/Disable to enable or disable the Dying Gasp function, which is off by default.

Figure 8-5 Dying Gasp Configuration Interface



8.3 Optical Module Information

Select [Diagnostics] [Optical Module Information] in the navigation bar to enter the Optical Module Information Monitoring page.As shown in Figure 8-6, you can query the digital diagnostic information of the optical module.

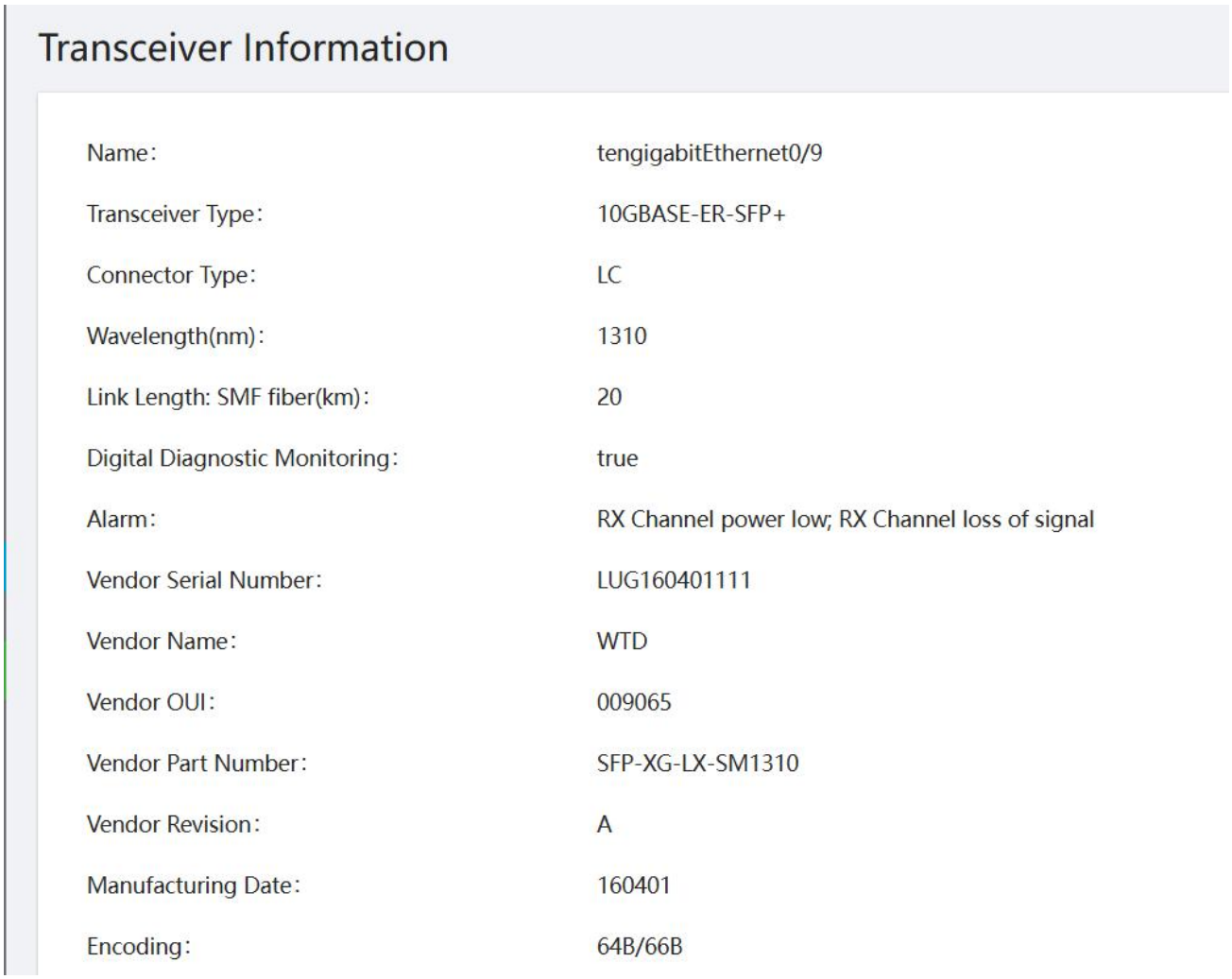
Figure 8-6 Optical Module Digital Diagnostic Information

Transceiver Information

Name	State	Transceiver Status	Temperature(℃)	Voltage(V)	Current(mA)	RX Power(dBm)	TX Power(dBm)	Detail
tengigabitEthernet0/9	Down	OK	25(OK)	3.2238(OK)	38.04(OK)	-40(ALARM)	-3.79(OK)	DETAIL
tengigabitEthernet0/10	Down	Transceiver absent	NA	NA	NA	NA	NA	DETAIL
tengigabitEthernet0/11	Down	Transceiver absent	NA	NA	NA	NA	NA	DETAIL
tengigabitEthernet0/12	Down	Transceiver absent	NA	NA	NA	NA	NA	DETAIL

Click the [Detailed] button to query the supplier, serial number, production date and other basic information of the optical module, as shown in Figure 8-7.

Figure 8-7 Optical Module Basic Information



9 preservation

Click the Save icon button in the upper right corner of the Web-based network management page (as shown in Figure 9-1) to save the current configuration to a configuration file, and the configuration remains valid after reboot or power-down reboot.

Figure 9-1: Preservation arrangement

There are two cases of saving configuration:

(1) Click the [OK] or [Apply] button in the current configuration interface, that is, the current configuration is saved to the memory.The saving at this time is not the configuration items are really saved to the configuration file, if the switch at this time, power failure and other faults, the interface configuration is invalid.

(2) Click the [Save] button below the navigation bar, then the system will automatically save the configuration of all pages to the configuration file.

10 deregister

procedure:

Click the Logout icon button on the navigation bar of the Web Manager page and click Logout to exit Web Manager.(As shown in Figure 10-1)

Figure 10-1 Exit of Web Webmaster