SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

USER MANUAL FOR

IESMG 304-2S A

Managed Giga Industrial Ethernet Switch

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

Contents

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

1 Web Management Overview

1.1 Introduction

We now introduce the device Web Management function, to facilitate the network administrator to perform operation and maintenance on the device intuitively by using Web UIs.

We also provide the CLI reference commands used to perform the corresponding Web Management operations。

The runtime environment for Web Management is as follow。

Figure 1-1

1.2 Login Web Management

The Web server service is enabled by default in the factory, and the IP address is 192.168.1.168. You need to enter the default user name (”admin”) and password (”admin”) when you log in at first time.We recommend that you change the login password immediately after you first login, to ensure the security.

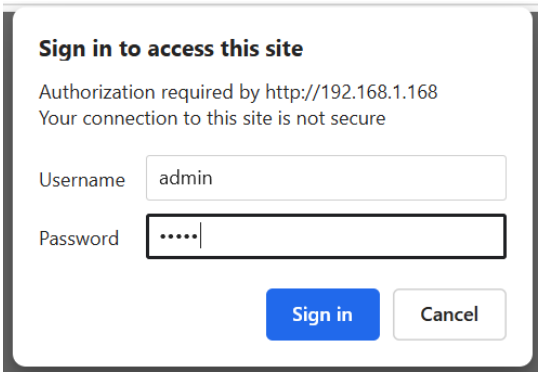
• Note: The steps to change password refer to the section User Management.

Here is how to log in the device via Web, taking switch for example:

1) Connect the gigabit Ethernet port on the device to PC via network cable (By default, all ports belong to VLAN 1).

2) Configure the IP address of PC, to ensure it is on the same network segment with the IP address of the default VLAN interface of the device (except the default IP address of device), for example, 192.168.1.100.

Chart Figure 1-2 User login



3) Start the browser on PC, enter "**192.168.1.168**" in the address bar and press Enter, to enter into the Web login page of device. Enter the default user name "admin" and password "admin", then click <Login> button to log in the Web Management.

1.3 Logout of Web Management

- When exiting the web network management, the system will not automatically save the current configuration. Therefore, it is recommended that users save the settings before exiting the web network management

  For information on saving configurations, please refer to the section Saving the Configurations.

On Web Management page, click the **Logout** button at the top right corner, to exit the Web Management and return to the login screen.

Chart Figure 1-3 Web logout

1.4 Layout of Web Management Page

The Web Management page divides into four sections: product model area, navigation bar, quick access ribbon and configuration area.

Figure 1-2 Web Management main screen

Introduction to web layout

1- product model: display the product model.

2- quick access ribbon: provide language switching, home page, logout, and help buttons.

3- navigation bar: organize the Web Management function menus as a navigation tree. The user can select the various function menus easily in the navigation bar, and the selections will display in the configuration area.

4- configuration area: the area that the user can select and view the configurations

1.5 General Functions

1.5.1 Configuration pages

There are two buttons at the bottom of each configuration page, as shown in the following figure:

Figure 1-3 Save and Reset buttons on configuration pages

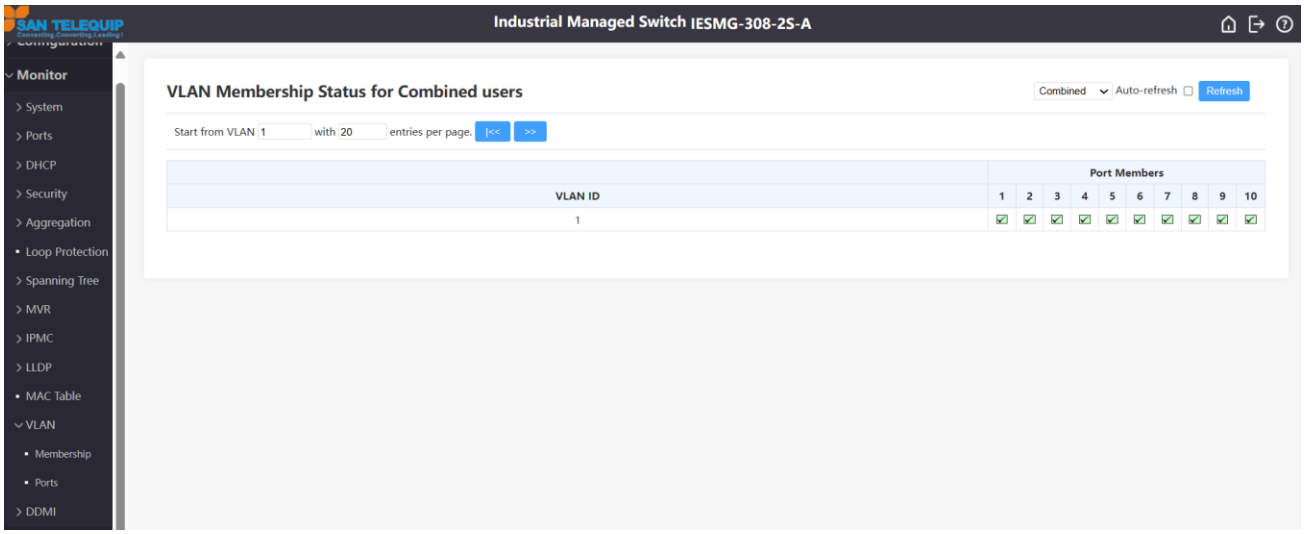
- Save: save the current page, and transfer the configuration information on this page to the switch, which is similar to typing the corresponding command in the switch CLI, and does not save the whole configuration of the switch. If you do not click the “Save” button, the modifications will not be applied in the switch side, and also will be disappeared after you switch to another page, which cannot be recovered. Therefore, always click this button after you complete the configurations
- Reset: reset the page to the last saved modifications (or to the default settings, if never saved).

1.5.2 Monitoring page

- Paging Display

  There is a paging area in some page, for example, VLAN Membership page, as shown in the following figure: You must click the “Refresh” button at the top right corner after making modification, to complete the refresh operation.

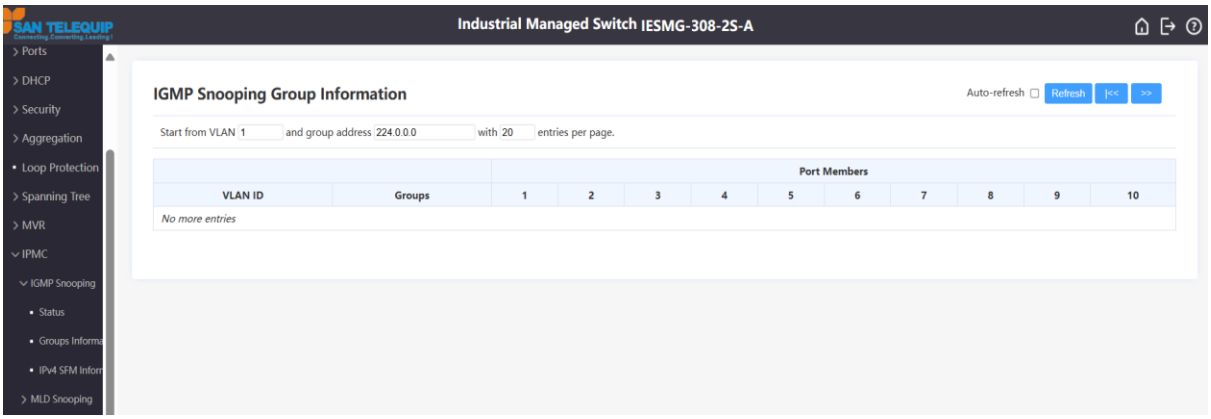
Figure 1-4 VLAN Membership Paging Display



This section consists of the following three areas:

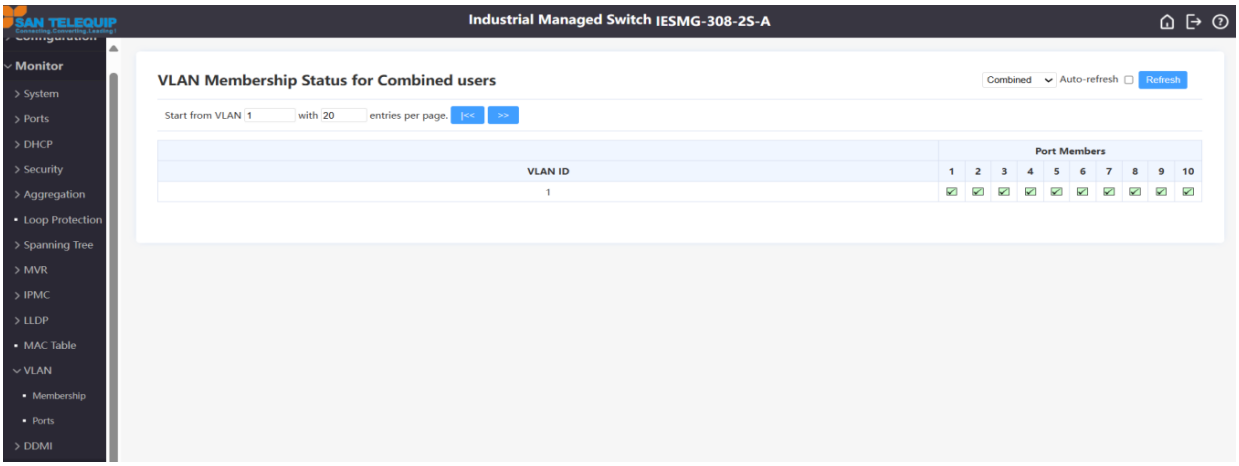
- The text boxes that display the items of the starting table entries, some table entries have more than one items, so there will also be more than one text boxes. The IGMP Snooping Group Information has two items, VLAN and group address, for example.

Figure 1-5 Display the multiple items of the starting table entries



- The textboxes that display the numbers of the entries per page (20, by default).The configurable value ranges from 1 to 99.
- Buttons used to switch the pages, located in the paging area or refresh area

Figure 1-6 Page switch buttons



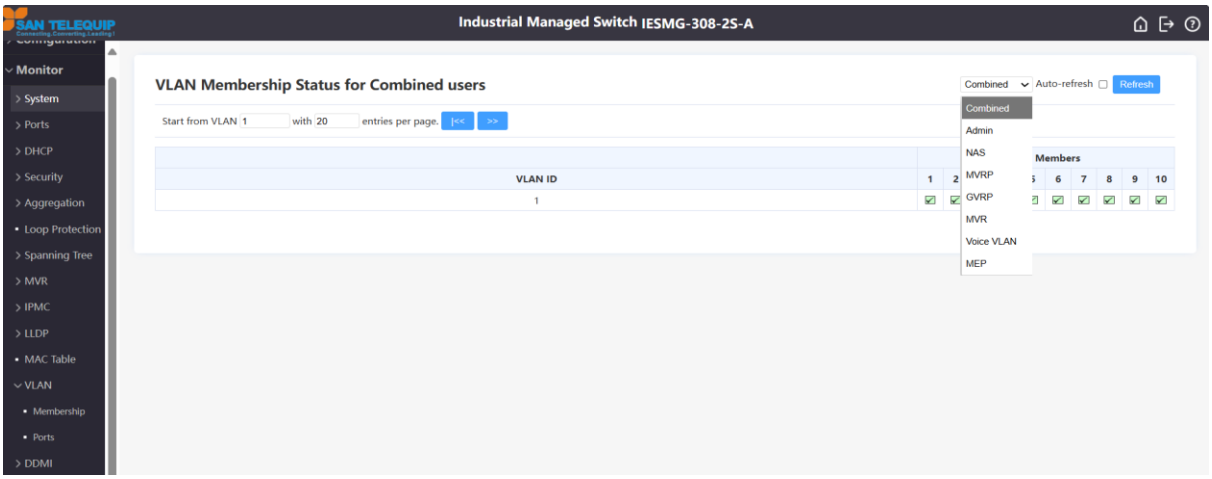
✧ "|<<": returns to the first page.

✧ ">>"goes to the next page.

■ Page Filtering

Some pages only display parts of the content that was filtered by some attributes, which is different from the paging display above. The ways of filtering include:

➢ by source, such as VLAN Membership page, in which the Combined represents all sources.



➢ by Port No. (see the" Detailed Port Statistics" page) or Server # (see the "RADIUS Statistics" page).

Figure 1-10 Detailed Port Statistics Page Filtering

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

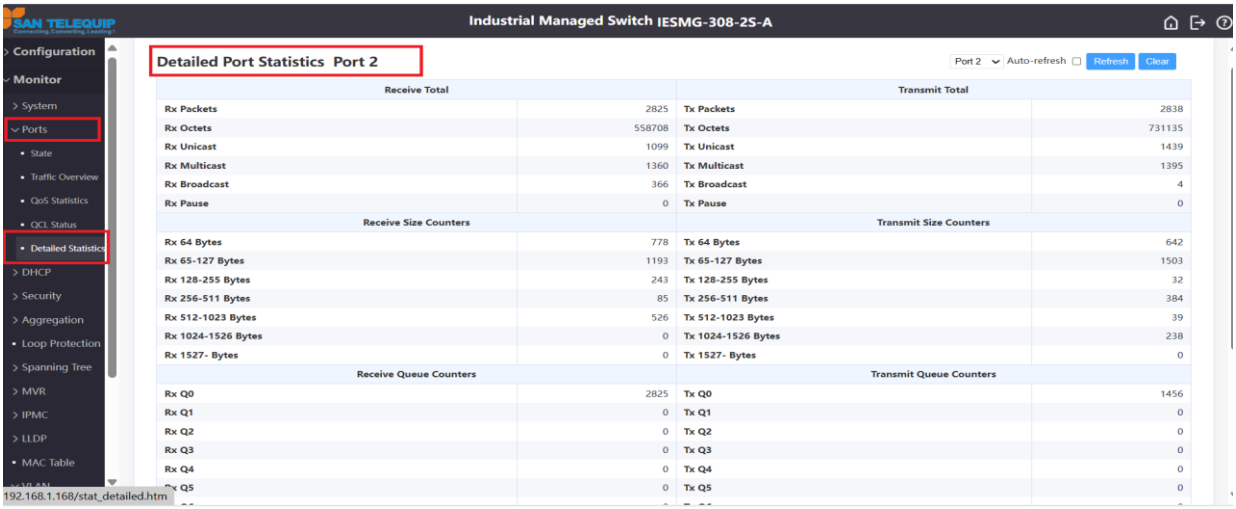
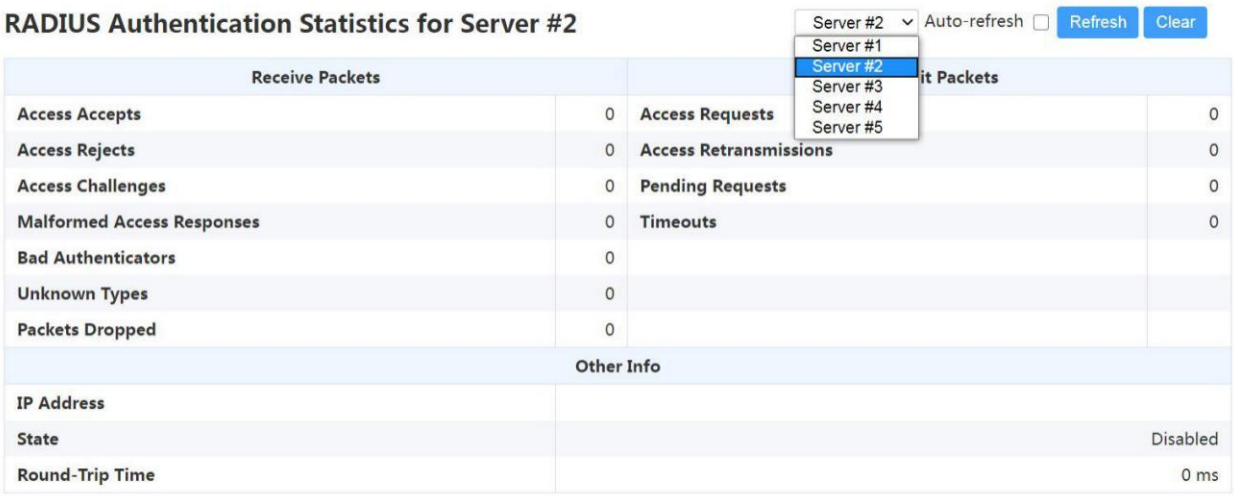


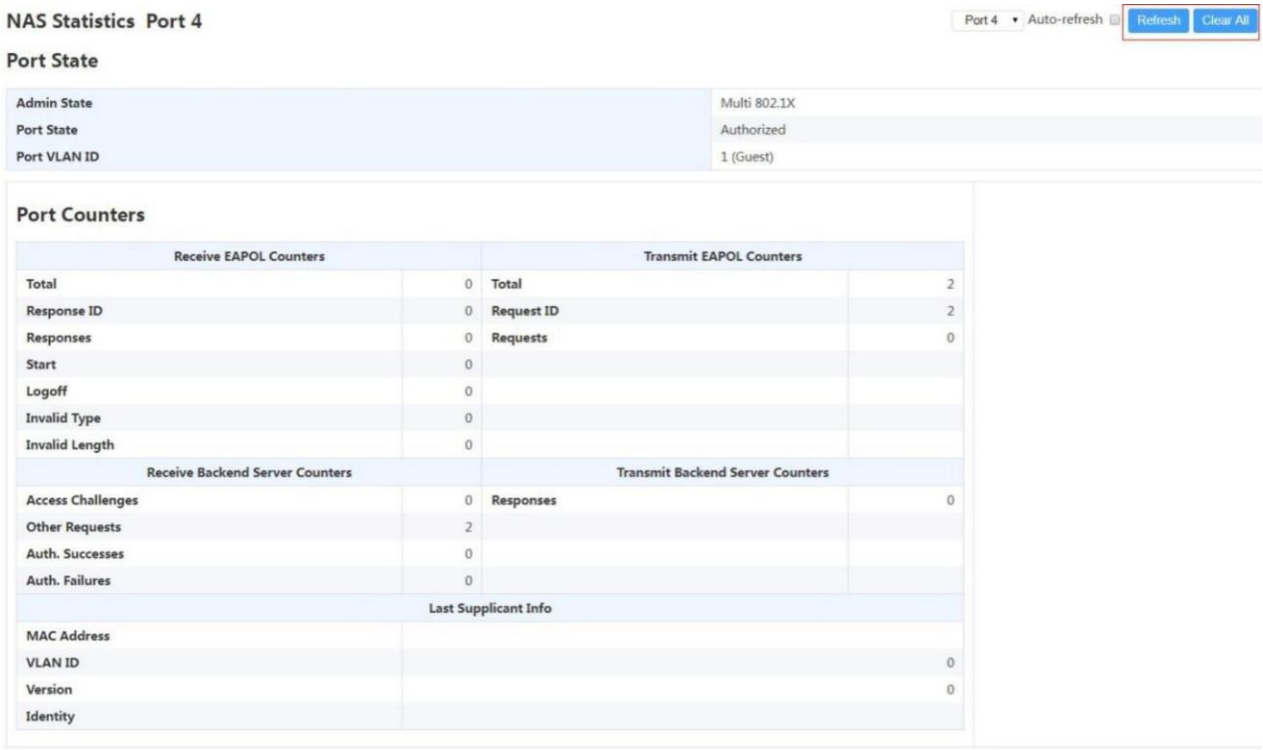
Figure 1-11 RADIUS Statistics Page Filtering



SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

- Refresh Area

The monitor page will display the status information or statistics, and there is also a refresh area, see the following port statistics page:
Figure 1-12 refresh area 1



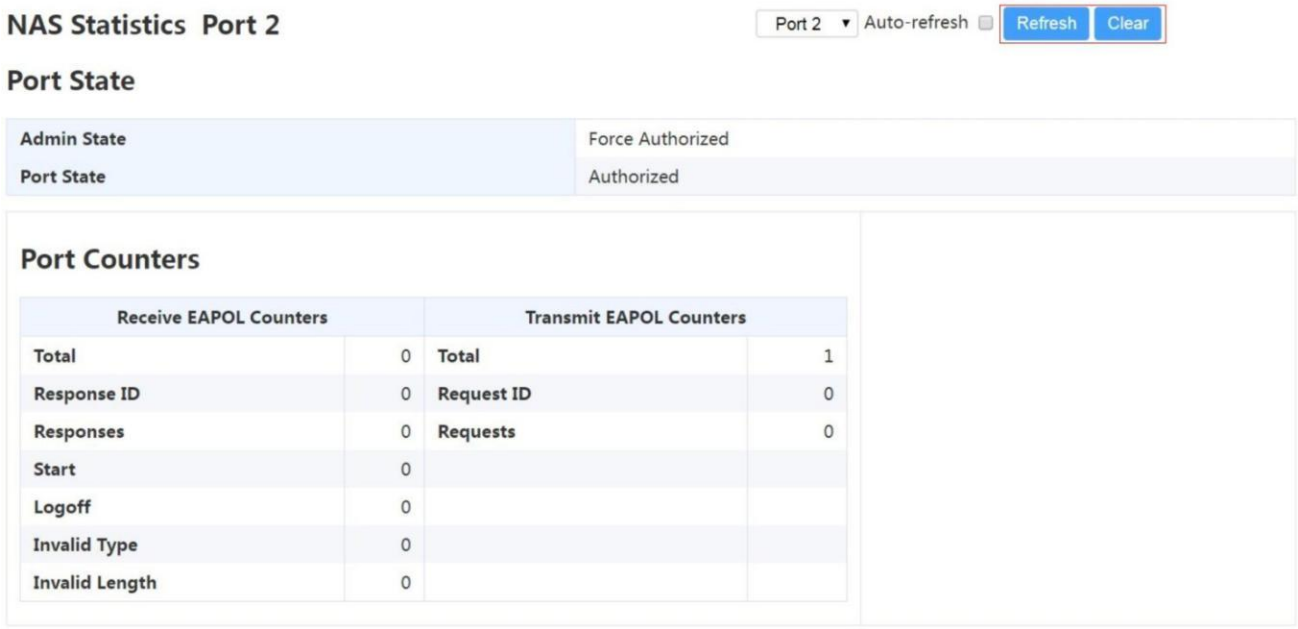
- Auto-refresh

  When checked, the system will be refreshed automatically every 3 seconds.
- Refresh

  The page will be refreshed immediately if you click this button
- Clear Area

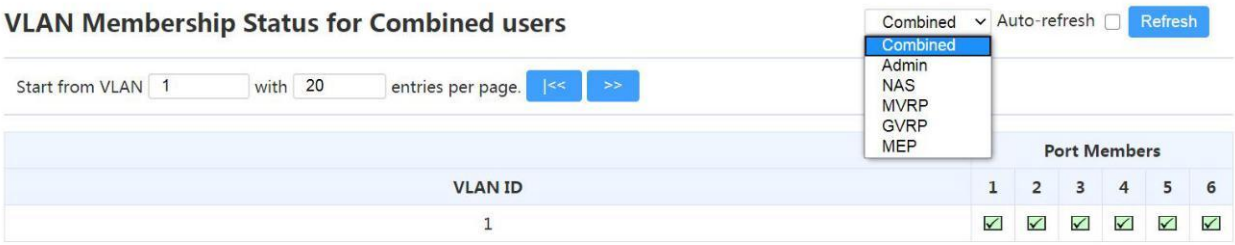
  If there are some filtered options on this page as above (by clients), there will be "Clear Current" and "Clear All" options. Obviously, "Clear Current" means to clear the statistics of the selected client, but "Clear All" means to clear the statistics of all clients.
  In the most case, there is no filter option on this page, in which will only display the "Clear" button.as shown in the following figure:

Figure 1-7 refresh area 2



There is no any clear buttons in the page in which the statistics don‘t exist.

Figure 1-8 refresh area 3



1.5.3 Save configuration

There are two types of configurations at the switch side: running-config and startup-config.The running-config represents the current configuration, but it will be reseted after the device restarts.

To keep the running-config being saved and still valid after the device restarts, you need to override the startup-config with it, as the configuration is applied to the running-config, whether by using CLI or via Web.

So, you must save the configuration after you complete the Web configuration, as described in the section “Save Configuration”.

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

2 System

2.1 Information

The system information contains the basic information of the device, such as the software version, hardware info, system time info, etc.You can configure the device support by configuring the subnodes sysContact, sysName and sysLocation of the MIB2 node in the Web interface.

2.1.1 Configure System Info

In the navigation bar dropdown menu, select **Configure**->**System**->**Information**, to enter into the configuration screen.

Figure 2-1 System Information Configuration

Item	Description
System Contact	Provides the contact information of the company and/or person who provides support for device, a maximum of 0-255 characters.
System Name	The name of the device, a maximum of 0-255 characters
System Location	The physical location where the device is installed, a maximum of 0-255 characters.

2.1.2 View System Information

In the navigation bar dropdown menu, select **Monitor**->**System**->**Information** to view the system information.

Figure 2-2 View System Information

2.1.3 CLI Reference Command

Command	switch(config)# snmp-server contact administrator
Description	Configure the system contact

Command	switch(config)# hostname switch
Description	Configure the system name

Command	switch(config)# snmp-server location telephone closet,3rd floor
Description	Configure the system location

2.2 IP

There is only one SVI interface (VLAN 1, IP 192.168.1.169/24) in the device by default.

The following operations may result in the current remote device access is disconnected, and cannot be reconnected again, please confirm the configuration is proper before modification:

- Modify the VLAN properties of the port, such as modifying the VLAN of the access port.
- Shutdown the port connected to the terminal that is being accessed.

2.2.1 Configure IP

- You need to redirect the Web page to new address to re-access the switch, after you modify the IP address.
- Please save your configuration after you modify the IP address, to ensure the configuration is still valid after reboot and powerdown

In the navigation bar dropdown menu, select **Configure**->**System**->**IP**, to enter into the configuration screen.
Figure 2-3 IP Configuration

- IP Interfaces

The IP interface configuration contains the IPv4 address setting and the IPv6 address setting, which are independent each other. The IPv4 address can be assigned via DHCP automatically, or can be configured statically, and IPv6 address only can be configured statically.
If the DHCP is turned on, the IPv4 address that was configured statically will be deleted automatically, except that the fallback is configured, as described below.

Item	Description
VLAN	Turn on/off the function that sends the logs to the sever.
Sever Address	The IP Address of the sever.
Log Level	The log level that sends to the sever (Informational<Notice<Warning<Error, from low to high).

Item	Sub-parameter	Description
Delete	None	The SVI interface will be deleted if selected.
VLAN	None	The VLAN ID corresponding to the SVI.
DHCPv4	Enable	Enable the DHCPv4 client if selected.If you enable this option, the system will use the DHCPv4 protocol to configure the IPv4 address and mask of the interface.
	Client ID	Client ID, displayed in the option 61 of the DHCPv4 message, has four types: ➢ Auto: the ID will be selected automatically, without any configuration.(The ID will be generated automatically depending on the system MAC address.) ➢ IF_MAC: use the MAC address of the configured port as ID. ➢ ASCII: use the configured string as ID. HEX: use the configured hexadecimal number as ID.
	Hostname	The current version does not support DNS, and therefore does not support the configuration of the hostname.The hostname is displayed in the option 12 of the DHCPv4 message, and will be generated by the system automatically,

		so this option is not available now.
	Fallback	Tries to get the number of the seconds of the DHCP lease.The configured IPv4 address will be used as the address of the IPv4 interface after the DHCP lease expired.Value 0 will disable the fallback, and the DHCP will continue to retry, until it gets the valid lease.The valid value is 0 to 4294967295 seconds. If this parameter is configured to a value other than 0, you must configure the IPv4 fallback address and mask,in order to use the IPv4 fallback address after the DHCP lease expired.
	Current Lease	For the DHCP interface that has an active lease, this column will display the current interface address that the DHCP sever provides.
IPv4	Address	The IPv4 address of the interface, in dot-decimal notation. If the DHCP is enabled, this field will configure the fallback address.If you do not want to perform the IPv4 operations on the interface, leave this field empty, or do not set the DHCP fallback address.
	Mask Length	IPv4 network mask, represented by the number of bits (the length of the prefix).The valid value ranges from 1 to 31 bits. If the DHCP is enabled, this field will configure the fallback address network mask.If you do not want to perform the IPv4 operations on the interface, leave this field empty, or do not set the DHCP fallback address.
IPv6	Address	The IPv6 address of the interface.An IPv6 address consists of 128 bits and is presented in eight 16-bit blocks. Each 16-bit block is converted to a four-digit hexadecimal number. Blocks are separated by colons (:).For example: FE80::215:c5ff:FE03:4dc7,where the :: is a special syntax, which can be used to represent one or more 16-bit consecutive zeroes, and can only be used once. If you do not want to perform the IPv6 operations on the interface, leave this field empty.
	Mask Length	IPv6 network mask, represented by the number of bits (the length of the prefix).For IPv6 addresses, the valid value ranges from 1 to 127 bits. If you do not want to perform the IPv6 operations on the interface, leave this field empty.

- IP Routes

For the layer 2 devices, you need to configure the default gateway via IP routes (ie. the default route).

Item	Description
Delete	The selected route will be deleted if selected.
Network	Destination IP network or host address of the route.The valid forms include dot-decimal notation or the valid IPv6 notations。The default route can use 0.0.0.0 or the :: symbol in the IPv6 standard notation
Mask Length	Destination IPv6 network or the host mask, represented by the number of bits (the length of the prefix).The valid value for IPv4 route ranges from 0 to 32, the valid value for IPv6 route ranges from 0 to 128.Only the mask of the default route has a length of 0.
Gateway	IP address of the IP gateway.The valid forms include dot-decimal notation or the valid IPv6 notations。The gateway and the network must be in the same network segment.
Distance (IPv4)	This distance value provides the priority information of the route protocols to the router.When there are two or more different protocols and they have the same destination, this value can be used to select the best path.This configuration item is unnecessary for the current device.
Next hop VLAN (IPv6)	The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.The given VID ranges from 1 to 4095, and will be valid when the corresponding IPv6 interface is enabled. If the IPv6 gateway address is a link local address, you must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not a link local address, the system will ignore the next hop VLAN of the gateway.

2.2.2 IP View IP

In the navigation bar dropdown menu, select **Monitor**->**System**->**IP Status** to view the IP information

Figure 2-4 IP Information

Item	Description
IP Interfaces	The type can be LINK, IPv4 or IPv6.The link-layer address represents the MAC address of the device.
IPv6 Routes	Display the IPv6 configuration and the generated routes.Configuring one IPv6 interface will generate one corresponding network route.
Neighbor Cache	The host information, ARP table and ND table that are interactive with the device.

2.2.3 CLI reference command

Command	switch(config)# interface vlan 10 switch(config)# no interface vlan 10
Description	Create/enter into the IP interface of VLAN; Delete the IP interface of VLAN;

Command	switch(config-if-vlan)# ip address 192.168.200.100 255.255.255.0 switch(config-if-vlan)# ipv6 address 64:64::5/64
Description	Configure the IPv4 address and mask; Configure the IPv6 address and mask;

Command	switch(config-if-vlan)# ip address dhcp switch(config-if-vlan)# ip address dhcp client-id GigabitEthernet 1/3 switch(config-if-vlan)# ip address dhcp client-id ascii dhcp switch(config-if-vlan)# ip address dhcp client-id hex 1234ABCD
Description	Configure the IPv4 address and mask of the interface via DHCPv4; the client ID is AUTO; Configure the IPv4 address and mask of the interface via DHCPv4; the client ID is IF_MAC; Configure the IPv4 address and mask of the interface via DHCPv4; the client ID is ASCII; Configure the IPv4 address and mask of the interface via DHCPv4; the client ID is HEX;

Command	switch(config-if-vlan)# ip address dhcp fallback 192.168.200.100 255.255.255.0 timeout 10
Description	Configure the IPv4 address and mask of the interface via DHCPv4, and configure the fallback address and fallback time at the same time

Command	switch(config)# ip route 1.1.1.0 255.255.255.0 192.168.1.1 100 switch(config)# no route 1.1.1.0 255.255.255.0 192.168.1.1

Description	Configure the IPv4 routing table entries and distance; Delete the IPv4 routing table entries;

Command	switch(config)# ipv6 route 11:22::34/64 interface vlan 6 fe80::11 switch(config)# no ipv6 route 11:22::34/64 interface vlan 6 fe80::11
Description	Configure the IPv6 routing table entries and the next hop VLAN; Delete the IPv6 routing table entries;

Command	switch# show interface vlan switch# show ipv6 route switch# show ip arp switch# show ipv6 neighbor
Description	View the IP Interfaces; View the IPv6 Routes; View the IPv4 neighbor cache; View the IPv6 neighbor cache;

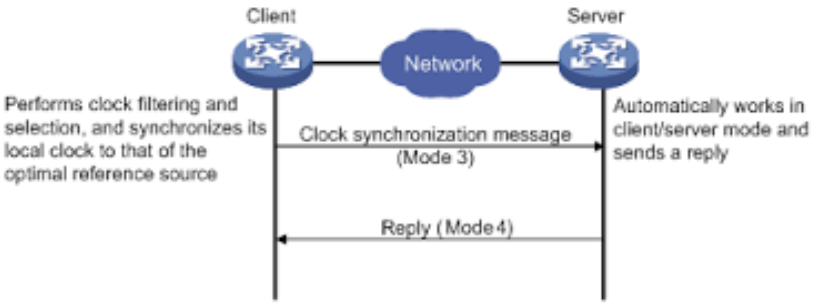
2.3 NTP

2.3.1 NTP Overview

NTP (Network Time Protocol) is a time synchronization protocol defined by RFC1305, used to synchronize time between the distributed time sever and the client.The NTP transfers the data via UDP message, and use the UDP port 123.

The standard NTP supports the server/client mode, peer mode, broadcast mode, and multicast mode, etc.This device only supports the server/client mode, and can only be used to the client,as described below:

Figure 2-5 NTP Server/Client mode



2.3.2 NTP Configure NTP

In the navigation bar dropdown menu, select **Configure**->**System**->**NTP**, to enter into the configuration screen.

Figure 2-6 NTP Configuration

Item	Description
Mode	Control the NTP function, disabled by default
Server 1~5	The IP address of the NTP server, can be used to view the time information in the system info to confirm if the NTP is effective.

2.3.3 CLI reference command

Command	switch(config)# ntp switch(config)# no ntp
Description	Turn the NTP on; Turn the NTP off.

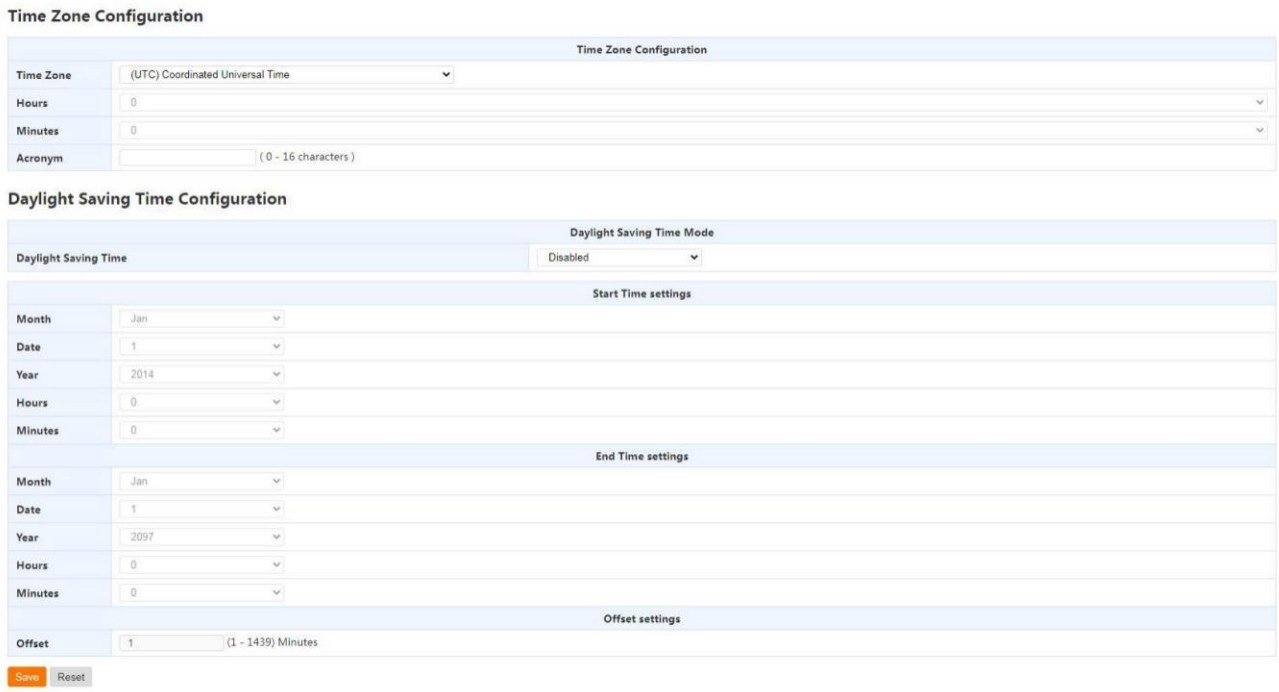
Command	switch(config)# ntp server 1 ip-address 120.25.115.20 switch(config)# ntp server 2 ip-address 1::1 switch(config)# no ntp server 1
Description	Configure the NTP address to IPv4; Configure the NTP address to IPv6; Delete the NTP sever address.

2.4 Time

2.4.1 Configure the Time

In the navigation bar dropdown menu, select **Configure**->**System**->**Time**, to enter into the configuration screen.

Figure 2-7 Configuring the Time



Item	Sub-parameter	Description
Time Zone Configuration	Time Zone	Select the standard time zone
	Acronym	Descriptor
Daylight Saving Time Configuration	Daylight Saving Time	Disabled: turn off this function Recurring: execute annually Non-Recurring: execute only once
	Start Time settings	The start time of the Daylight Saving Time
	End Time settings	The end time of the Daylight Saving Time
	Offset settings	The number of minutes in offset

2.4.2 CLI reference command

Command	switch(config)# clock timezone " 8 switch(config)# clock timezone china 8
Description	Configure the time zone; Configure the time zone and its acronym;

Command	switch(config)# clock summer-time " recurring 1 3 3 03:04 4 1 4 07:06 123 switch(config)# clock summer-time " date 3 1 2014 03:04 4 1 2097 07:06 100
Description	Configure the recurring start time, end time and offset time in which execute the daylight saving time every year; Configure the start time, end time and offset time in which execute the daylight

	saving time only once

2.5 Log

2.5.1 Configure the Log Server

In the navigation bar dropdown menu, select **Configure**->**System**->**Log**, to enter into the configuration screen.

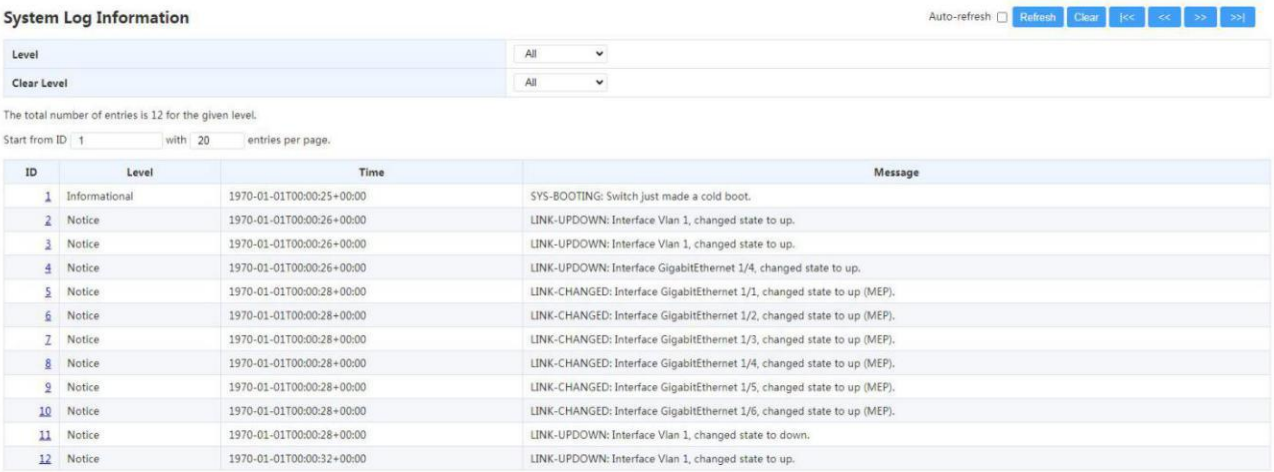
Figure 2-8 Configuring the Log Server

Item	Description
Server Mode	Turn on/off the function that sends the logs to the sever
Sever Address	The IP Address of the sever.
Log Level	The log level that sends to the sever (Informational<Notice<Warning<Error, from low to high).

2.5.2 View the Log Information

In the navigation bar dropdown menu, select **Monitor**->**System**->**Log** to view the log information

Figure 2-9 View the Log Information



2.5.3 View the Detailed Log Information

In the navigation bar dropdown menu, Select **monitor > system > detailed log**

Figure 2-10 Viewing the Single Log Information

2.5.4 CLI reference command

Command	switch(config)# logging on switch(config)# no logging on
Description	Turn on the Log Server; Turn off the Log Server;

Command	switch(config)# logging host 192.168.6.22 switch(config)# no logging host
Description	Configure the IPv4 address of the log server; Delete the IPv4 address of the log server

Command	switch# show logging switch# show logging 48
Description	Show the log information; Show the detailed information of the single log;

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

3 Port

3.1 Port Configuration

In the navigation bar dropdown menu, select **Configure**->**Port**, to enter into the configuration screen

Figure 3-1 Port Configuration

Item	Description
Port	The port number of the panel
Link Status	The current status of the port link, the green indicator indicates the link is up, and the red indicator indicates the link is down.
Speed	It is divided into configuration rate and current actual rate. When the rate is configured as auto, the capacity notification configured in duplex mode / rate mode shall prevail. When it is not auto, it means that it is forced to be set to the configured rate duplex mode
Duplex mode/ Speed mode	Port capability notification, which takes effect when speed configured is auto
Flow control	off by default. When the flow control function is turned on, curr RX indicates whether the opposite end flow control signal is received, and curr TX indicates whether or not to send the flow control signal. When the port is 100m full duplex, the flow control function is not supported and it is automatically closed
Max.frame size	The max. packet length forwarded by the port ranges from 1518 to 9600 bytes, including FCS field
Spillover conflict mode	When port conflict is detected, discard indicates discarding message when the number of conflicts reaches 16 times, restart indicates that when the number of conflicts reaches 16 times, restart detection
Frame length check	Check whether the Ethernet / length field in the message is consistent with the actual message data length

3.2 View port information

3.2.1 Port status

In the navigation bar dropdown menu, select **Monitoring > port > status**, to enter into the view screen

Figure 3-2 Port status display

The green light indicates port link, and if it is not on, port down. Click the port to automatically jump to the port message statistics details page

3.2.2 Overview of Port message statistics

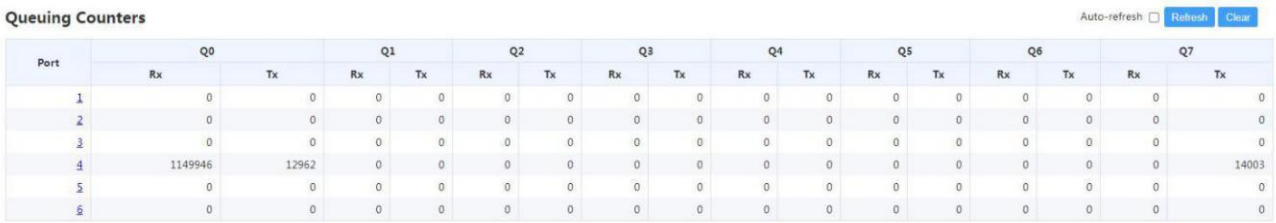
In the navigation bar dropdown menu, select Monitoring > port > traffic, to enter into the view screen.

Figure 3-3 Port statistics overview

3.2.3 Port queue message statistics

In the navigation bar dropdown menu, select Monitoring > port >QoS, to enter into the view screen

Figure 3-4 Port QoS statistics



Item	Description
Port	Panel port number, click the port number to enter the port message statistics details page
Qn	Port queue ID
Rx/Tx	Statistics of messages received and sent by queue

3.2.4 Port message statistics details

In the [Navigation Bar] drop-down menu, select: Monitor -> Port -> Detailed Port Statistics, enter the view interface.

Figure 3-5 Port message statistics details

Detailed Port Statistics Port 4

Port 4 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	1157687	Tx Packets	27514
Rx Octets	113081322	Tx Octets	6272987
Rx Unicast	28161	Tx Unicast	13479
Rx Multicast	293050	Tx Multicast	14032
Rx Broadcast	836476	Tx Broadcast	3
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	742009	Tx 64 Bytes	7133
Rx 65-127 Bytes	314236	Tx 65-127 Bytes	14255
Rx 128-255 Bytes	54063	Tx 128-255 Bytes	482
Rx 256-511 Bytes	20609	Tx 256-511 Bytes	3502
Rx 512-1023 Bytes	21829	Tx 512-1023 Bytes	300
Rx 1024-1526 Bytes	4941	Tx 1024-1526 Bytes	1842
Rx 1527- Bytes	0	Tx 1527- Bytes	0

Item	Description
Receive Sum	Receiving statistics list, including number of messages, bytes, unicast, multicast, broadcast, flow control message, etc
Sent Sum	sending statistics list, including number of messages, bytes, unicast, multicast, broadcast, flow control message, etc
Receive size count	Receiving statistics list based on message length
Send size count	Sending statistics list based on message length
Receive queue count	Receive queue statistics list
Send queue count	send queue statistics list
eceive error count	Statistics of receiving error packets, including discarding message, CRC error, too short, too long, fragmented message, long packet with CRC error, filtering message, etc
Send error count	Statistics of sending error, including discarded packets, discarded packets due to collision detection, etc

3.3 CLI reference command

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter port configuration

Command	switch(config-if)# speed auto switch(config-if)# duplex auto
Description	Configure port speed automatic, and ability to inform all supported capabilities; Configure port duplex auto, capability notification for all supported capabilities

Command	switch(config-if)# speed auto 100 1000 switch(config-if)# speed 1000 switch(config-if)# duplex full
Description	Configure port speed automatic, capacity notification support 100M / 1000m; Configure port speed to be 1000M as forced Configure port duplex force to full

Command	switch(config-if)# flowcontrol on switch(config-if)# flowcontrol off
Description	Turn on flow control Turn off flow control

Command	switch(config-if)# mtu 9600
Description	Configure port maximum frame size

Command	switch(config-if)# excessive-restart switch(config-if)# no excessive-restart
Description	Configure the port overflow conflict mode to restart Configure the port overflow conflict mode to discard

Command	switch(config-if)# frame-length-check switch(config-if)# no frame-length-check
Description	Enable frame length check Disable frame length check

Command	switch# show interface * status switch# show interface GigabitEthernet 1/3 status
Description	View all port status View the specified port status

Command	switch# show interface * statistics priority switch# show interface GigabitEthernet 1/3 statistics priority
Description	View port queue message statistics View the message statistics of the specified port queue

Command	switch# show interface * statistics

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

	switch# show interface GigabitEthernet 1/3 statistics
Description	View port message statistics details View the message statistics details of the specified port

4 DHCP

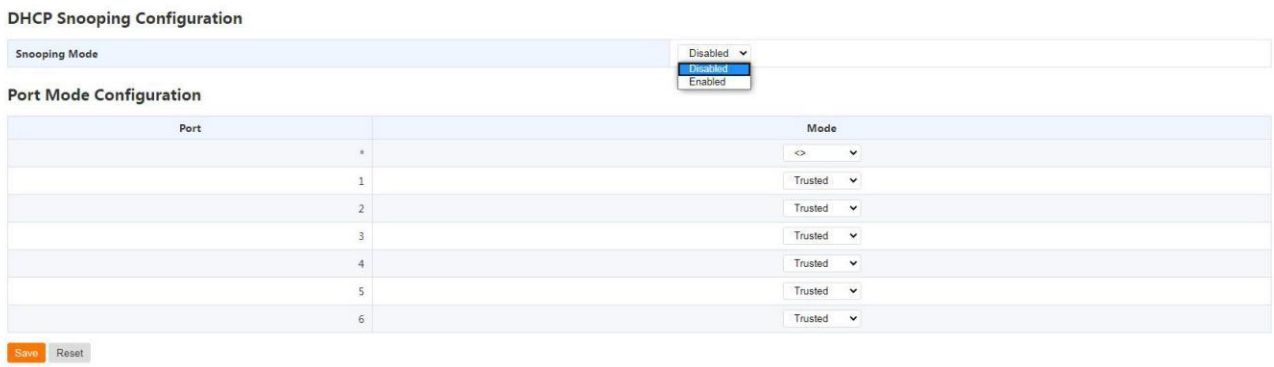
4.1 Snooping

DHCP snooping generates a DHCP snooping table by monitoring the DHCP request response message, which records the relationship among MAC address, VLAN ID, port and IP address. The data table can be used for secure access control functions, mainly "IP source guard" and "ARP inspection". The former controls the access of IP messages, and illegal IP messages are not allowed to access the network; the latter controls the access of ARP messages, and illegal ARP messages are not allowed to access the network. Therefore, the DHCP snooping function and the secure access control function often act on the access device at the same time.
At the same time, DHCP snooping can also prevent the DHCP server from cheating, and it can be achieved through its "trust port" function

- Received DHCP request message, only forwarded to trust port
- Only DHCP reply messages received from the trust port can be forwarded

4.1.1 Configure Snooping

In the navigation bar dropdown menu, select **Configure->DHCP->Snooping**, to enter into the view screen
Figure 4-1 DHCP Snooping configuration



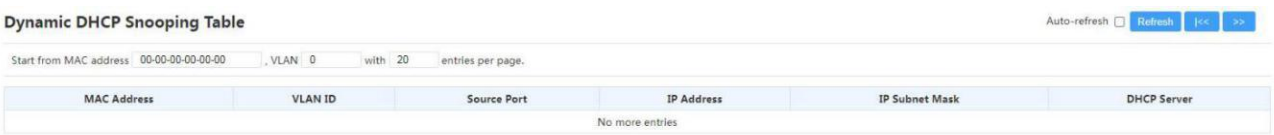
- Global enable

  The DHCP snooping global mode is disabled by default. Only when it is enabled can the function take effect
- Configure the trusted port

  Specify whether the port is trusted or untrusted. By default, all ports are trusted

4.1.2 Snooping View snooping

In the navigation bar dropdown menu, select **Monitor->DHCP->Snooping**, to enter into the page
Figure 4-2 DHCP Snooping table display



Item	Description
MAC address	MAC address of the DHCP client corresponding to the table entry
VLAN ID	VLAN ID used by the request IP of the DHCP client corresponding to the table entry
Source port	The DHCP client corresponding to the table entry corresponds to the panel port of the switch
IP address	The IP address requested by the DHCP client corresponding to the table entry
IP subnet mask	The IP subnet mask requested by the DHCP client corresponding to the table entry
DHCP server	IP address of DHCP server

4.1.3 CLI reference command

Command	switch(config)# ip dhcp snooping switch(config)# no ip dhcp snooping
Description	DHCP Snooping； DHCP Snooping；

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# ip dhcp snooping trust switch(config-if)# no ip dhcp snooping trust
Description	Configure port as DHCP trusted port Configure port as DHCP snooping untrusted port

Command	switch# switch# show ip dhcp snooping table
Description	View DHCP snooping Table

4.2 Client

DHCP client function is described in the section "configure IP"

4.3 Statistics Information

4.3.1 View statistics information

This page counts the sending and receiving of DHCP messages of various DHCP related functions. Currently, only DHCP snooping and DHCP client are valid.
In the navigation bar dropdown menu, select **Monitor->DHCP->Detailed statistics,**to enter into the page

Figure 4-3 DHCP statistics information display

Parameter	Description
RX/TX Discover	Option 53, value 1
RX/TX Offer	Option 53, value 2
RX/TX Request	Option 53, value 3
RX/TX Decline	Option 53, value 4
RX/TX ACK	Option 53, value 5
RX/TX NAK	Option 53, value 6
RX/TX Release	Option 53, value 7
RX/TX Inform	Option 53, value 8
RX/TX Lease Query	Option 53, value 10
RX/TX Lease Unassigned	Option 53, value 11
RX/TX Lease Unkown	Option 53, value 12
RX/TX Lease Active	Option 53, value 13
RX Discarded Checksum Error	DHCP message dropped by IP / UDP checksum error
RX Discarded from Untrust	DHCP message dropped from untrusted port

The first check box is used to select the DHCP application, and combined represents all applications
The second check box is used to select the port

4.3.2 CLI reference command

Command	switch# show ip dhcp detailed statistics snooping switch# show ip dhcp detailed statistics snooping interface GigabitEthernet 1/3
Description	View port DHCP Snooping statistics; View DHCP Snooping statistics on the specified port;

Command	switch# show ip dhcp detailed statistics client switch# show ip dhcp detailed statistics client interface GigabitEthernet 1/3

Description	View port DHCP client statistics View DHCP client statistics on the specified port;

5 SECURITY

5.1 Switch

5.1.1 User

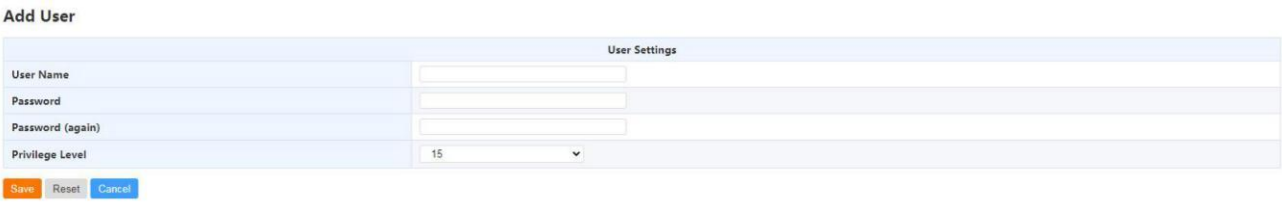
The default user name of the system is "admin", without password protection. Please change the password as soon as possible after the management user logs in, and keep the password properly, so as to avoid the situation of unable to log in due to forgetting the password. The device does not support password retrieval.

In the navigation bar dropdown menu, select **Configuration->Security->Switch->User,**to enter into the page

5.1.1.1 Configure user

Figure 5-1 configure user

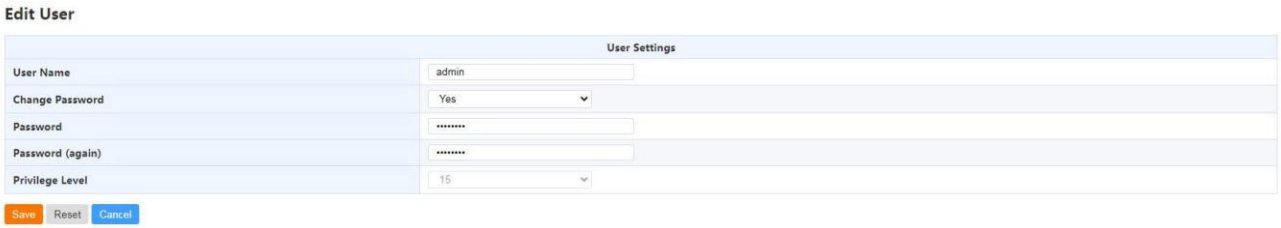
Click the "add user" button to enter the new user configuration interface
Figure 5-2 Add user



Item	Description
User name	User name, supports combination of numbers, letters and underscores, and the length range is 1-31 characters
Password	Support all keyboard output characters, including spaces, length range 0-31, 0 means no password is set
Password (duplicate)	consistent with the same password above
priority	The device is divided into 16 priorities of 0-15 for users, and the commands that users with different priorities can execute are different. Level 0 is the lowest level, and level 15 is the highest level. All commands can be executed. The user priority must be higher than the module read / write priority before the command can be executed

- Edit user

In the configuration user interface, click the user name directly to enter the user editing interface
Figure 5-3 Edit user



Support password and priority edit operation, support delete user operation

5.1.1.2 CLI reference command

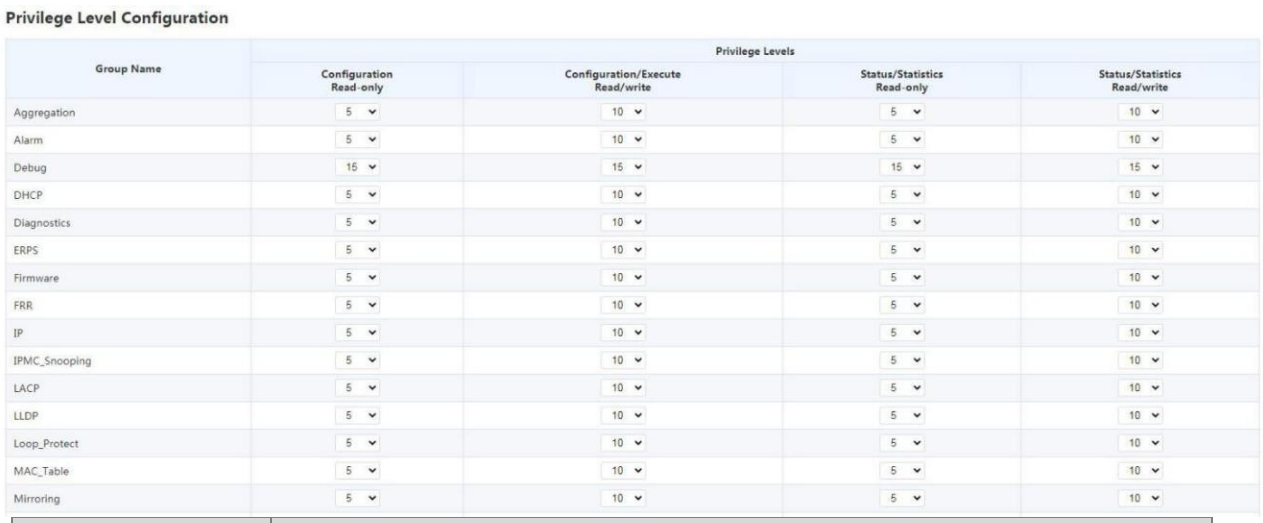
Command	switch(config)# username user1 privilege 13 password unencrypted password1 switch(config)# no username user1
Description	Add user Delete user

5.1.2 Priority

5.1.2.1 Configure Priority

The device supports setting its configuration read / write and status read / write priority independently for a specific group. If the priority of login user is greater than that of group operation item, corresponding operation can be performed. If the user priority is 5 and the group "aggregation" is configured / read / write priority is 10, the user cannot write to: configuration > link aggregation > static page.

In the navigation bar dropdown menu, select **Configuration->Security->Switch->Priority,**to enter into the page
Figure 5-4 configure module priority



item	Description

Group name	Function module name
Configure-read only	When the user priority is lower than the module priority, the page display is not supported
Configure / execute, read / write	When the user priority is lower than the read / write priority of the module, the page does not support configuration, and the read / write priority of the module should be higher than the read-only priority
Status / statistics read only	The read permission priority of monitoring interface is not supported when the user priority is less than the read permission priority of the module
Status / statistics read / write	Read / write privilege priority of the monitoring interface. When the user priority is lower than the read / write privilege priority of the module, the page does not support configuration, and the read / write priority of the module should be higher than the read-only priority

5.1.2.2 CLI reference command

Command	switch(config)# web privilege group Debug level configRoPriv 10 configRwPriv 10 statusRoPriv 5 statusRwPriv 10 switch(config)# no web privilege group Debug level
Description	Configure module priority Recovery module default priority

5.1.3 Authentication method

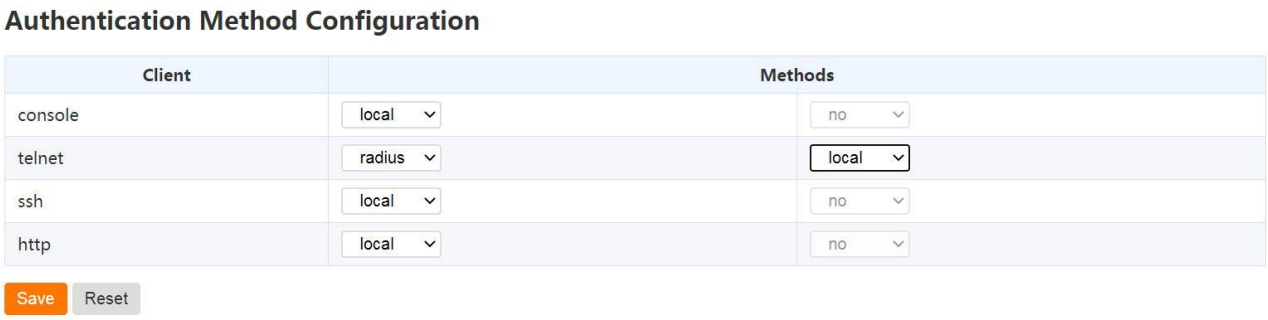
5.1.3.1 Configure authentication method

When the user logs in to the network equipment for management, if the server authentication (radius) is set on the line, the user authentication needs to be carried out through the remote radius server. If local authentication is set on the line, it is necessary to authenticate the user's management authority according to the user name and password through the local user database. In order to improve network security, the device supports turning off authentication to prevent illegal user attacks.

Both radius and local methods can be opened at the same time.

In the navigation bar dropdown menu, select Configuration->Security->Switch->Authentication method,to enter into the page

Figure 5-5 Configure authentication method



Item	Description
Client	Supported authentication methods
Method	select radius to open server authentication, select local to open local authentication, and select no to close authentication

5.1.3.2 CLI reference command

Command	switch(config)# aaa authentication login ssh radius local switch(config)# no aaa authentication login ssh
Description	Configure authentication method Turn off authentication method

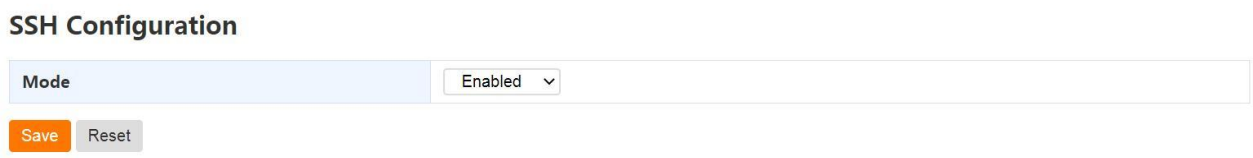
5.1.4 SSH

5.1.4.1 Configure SSH

- SSH authentication, please use SSH2 protocol
- On the client side of SSH2, for the "key exchange" content, please select the "Diffie Hellman" option

In the navigation bar dropdown menu, select **Configuration->Security->Switch->SSH,**to enter into the page

Figure 5-6 SSH authentication



Item	Description
Mode	Enabled SSH authentication, disabled SSH authentication

5.1.4.2 CLI reference command

Command	switch(config)# ip ssh switch(config)# no ip ssh
Description	Turn on SSH Turn off SSH

5.1.5 HTTPS

5.1.5.1 Configure HTTPS

In the navigation bar dropdown menu, select **Configuration->Security->Switch->HTTPS,**to enter into the page

Chart Figure 5-7 HTTPS authentication

Item	Description
Mode	Enable HTTPS mode
redirect automatically	Enable switch. When it is turned on, the HTTP connection will be automatically redirected to the HTTPS connection
Certificate maintenance	None means no operation; delete means to delete the current certificate, upload means to upload the certificate; generate means to re produce the certificate. Only when the HTTPS mode is turned off can certificate maintenance be performed.
Certificate pass phrase	When upload is selected for certificate maintenance, enter the pass phrase
Certificate upload	Select certificate upload mode, web browser or web address
File upload / website	The web browser selects the local upload file, and the URL is the input URL
Certificate status	Display the current certificate status, including presented, generating and not

5.1.5.2 CLI reference command

Command	switch(config)# ip http secure-server

	switch(config)# no ip http secure-server
Description	Enable HTTPS mode Disable HTTPS mode

Command	switch(config)# ip http secure-redirect switch(config)# no ip http secure-redirect
Description	Enable automatic redirection of HTTPS Disable automatic redirection of HTTPS

Command	switch(config)# ip http secure-certificate delete switch(config)# ip http secure-certificate generate switch(config)# ip http secure-certificate upload http://192.168.6.100/cert-test.pem
Description	Delete current HTTPS certificate Generate a self signed RSA certificate Upload the HTTPS certificate;

Command	switch# show ip http
Description	View HTTPS configuration status

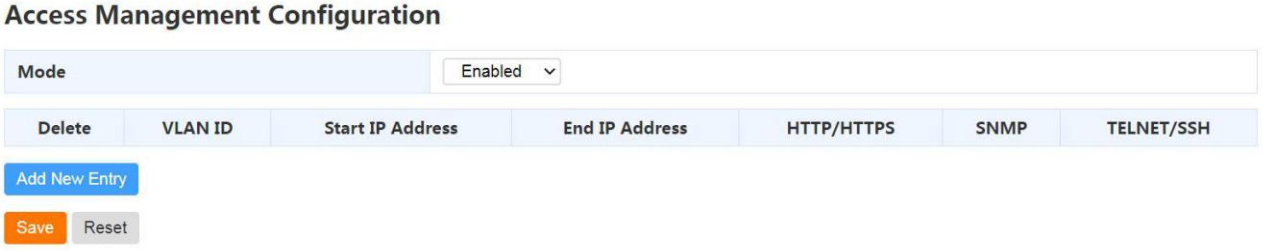
5.1.6 Access management

5.1.6.1 Configure access management

Access management function limits the IP address range of access users to improve access security according to different access modes. The device can be configured with up to 16 access security policies. Access users can access the device normally if they only need to meet any access security policy.

In the navigation bar dropdown menu, select **Configuration->Security->Switch->Access management,**to enter into the page

Chart Figure 5-7 Access management



Item	Description

Mode	Enable Global mode
VLAN ID	the rule in security policy
Starting IP address	
End IP address	
HTTP/HTTPS	Choose at least one security policy access mode and multiple security policy access modes
SNMP	
TELNET/SSH	

5.1.6.2 View access management statistics

In the navigation bar dropdown menu, select **Monitor->Security->Switch->access management statistics,**to enter into the page

Figure 5-8 access management statistics

5.1.6.3 CLI reference command

Command	switch(config)# access management switch(config)# no access management
Description	Turn on access management Turn off access management

Command	switch(config)# access management 2 1 192.168.64.10 to 192.168.64.100 telnet switch(config)# no access management 2
Description	Add access management Delete access management

Command	switch# show access management switch# show access management statistics
Description	View access management status View access management statistics

5.1.7 SNMP

5.1.7.1 Overview

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 features

- Support the intelligent management of network equipment. Using SNMP based network management platform, network administrators can query the running status and parameters of network devices, set parameter values, find faults, complete fault diagnosis, carry out capacity planning and generate reports.
- It supports the management of devices with different physical characteristics. SNMP only provides the basic function set, which makes the management task relatively independent of the physical characteristics and networking technology of the managed devices, so as to realize the management of devices from different manufacturers.

5.1.7.2 SNMP Working mechanism

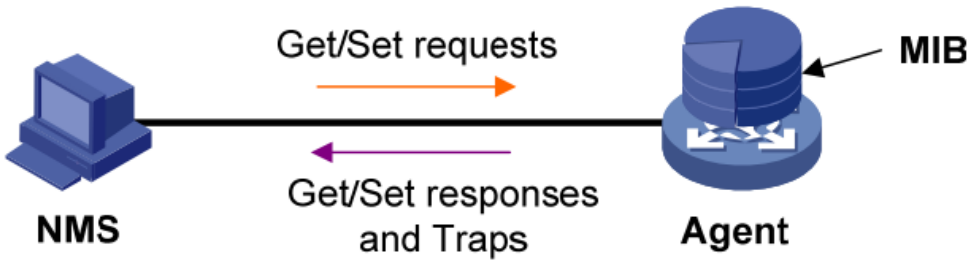
SNMP network includes NMS and agent

- NMS (network management system) is the manager of SNMP network. It can provide a very friendly man-machine interface, which is convenient for network administrators to complete most of the network management work
- Agent is the manager of SNMP network, which is responsible for receiving and processing the request message from NMS. In some emergency situations, such as the change of interface state, the agent will actively send alarm information to NMS

When NMS manages devices, it usually pays attention to some parameters, such as interface status, CPU utilization, etc. the set of these parameters is called MIB (management information base). These parameters are called nodes in MIB. MIB defines the hierarchical relationship between nodes and a series of attributes of objects, such as object name, access permission and data type. Each agent has its own MIB. All managed devices have their own MIB files. By compiling these MIB files on NMS, the MIB of the device can be generated. NMS performs read / write operations on MIB nodes according to the access rights, so as to realize the management of agents. The relationship among NMS, agent and MIB is as follows.

error reporting notes

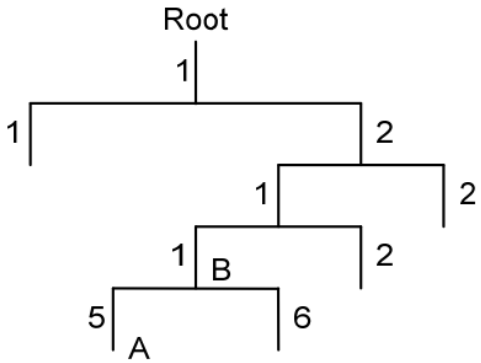
Figure 5-9 the relationship among NMS, agent and MIB



MIB is organized according to the tree structure. It is composed of many nodes. Each node represents the managed object. The managed object can be uniquely identified by a string of numbers representing the path from the root. This string of numbers is called oid (object identifier).

As shown in the figure below, managed object B can be uniquely determined by a string of numbers {1.2.1.1}, which is the OID of managed object B

Figure 5-10 MIB tree structure



SNMP provides four basic operations to realize the interaction between NMS and agent

- Get operation: NMS uses this operation to query the value of one or more nodes in agent MIB
- Set operation: NMS uses this operation to set the value of one or more nodes in agent MIB
- Trap operation: the agent uses this operation to send trap information to NMS. Agent does not require NMS to send response message. NMS will not respond to trap messages. SNMPv1, snmpv2c and SNMPv3 all support trap operation

5.1.7.3 SNMP Version

At present, agent supports SNMPv1, snmpv2c and SNMPv3

- Community name authentication mechanism is adopted in SNMPv1. The community name is similar to a password and is used to restrict the communication between NMS and agent. If the community name set by NMS is different from that set on the managed device, NMS and agent can't establish SNMP connection, so NMS can't access agent, and the alarm information sent by agent will be discarded by NMS.

- Snmpv2c also uses group name authentication mechanism. Snmpv2c extends the functions of SNMPv1: it provides more operation types, supports more data types, and provides more error codes to distinguish errors in detail
- The USM (user based security model) authentication mechanism is adopted in SNMPv3. Network administrators can set authentication and encryption functions. Authentication is used to verify the legitimacy of message sender and avoid the access of illegal users; encryption is to encrypt the transmission message between NMS and agent to avoid eavesdropping. With the functions of authentication and encryption, higher security can be provided for the communication between NMS and agent.

Note: The prerequisite for successful connection between NMS and agent is that NMS and agent use the same version of SNMP

5.1.7.4 SNMP Security

SNMPv1 and SNMPv2 versions use authentication names to identify whether they are authorized to use MIB objects. In order to manage the device, the authentication name of NMS must be consistent with one of the authentication names defined in the device.

An authentication name can have the following properties

- Read-only: provides read access to all MIB variables for the authorized management workstation
- Read-write: provides the authorized management workstation with read and write access to all MIB variables

On the basis of SNMPv2, SNMPv3 determines which security mechanism to use for data processing through security model and security level; at present, there are three types of security models available: SNMPv1, snmpv2c and SNMPv3

The following table shows the security models and security levels available at present

Security model	Security level	Identify	Encryption	Description
SNMPv1	noAuthNoPriv	Authentication name	无	Confirm the validity of data by authentication name
SNMPv2c	noAuthNoPriv	Authentication name	无	Confirm the validity of data by authentication name
SNMPv3	noAuthNoPriv	User name	无	Confirm the validity of data by user name
SNMPv3	authNoPriv	MD5 or SHA	无	Provide data authentication mechanism based on HMAC-MD5 or HMAC-SHA
SNMPv3	authPriv	MD5 or SHA	DES	Provide data authentication mechanism based on HMAC-MD5 or HMAC-SHA and data encryption mechanism based on CBC-DES

5.1.7.5 SNMP engine identification

Engine ID is used to uniquely identify an SNMP engine. Since each SNMP entity contains only one SNMP engine, it will uniquely identify an SNMP entity in a management domain. Therefore, as an entity, SNMPv3 agent must have a unique engine ID, namely engine ID.

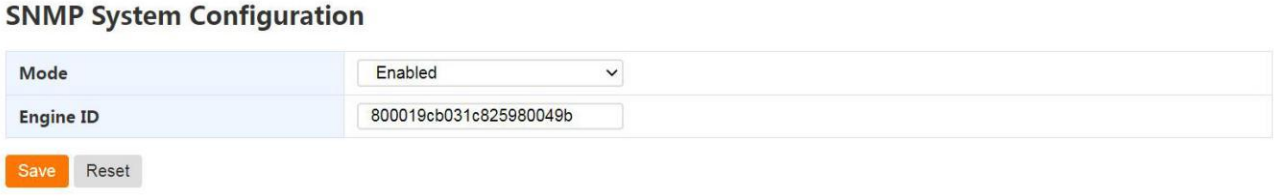
The engine ID is an octet string, 5-32 bytes long. The format of engine identification is defined in rfc3411

- The first four bytes identify the manufacturer's private enterprise number (assigned by IANA) and are represented by HEX
- The fifth byte indicates how to identify the remaining bytes
- 0：Reserved
- 1：The last 4 bytes are an IPv4 address
- 2：The last 16 bytes are an IPv6 address
- 3：The next 6 bytes are a MAC address
- 4：Text, up to 27 bytes, defined by the manufacturer
- 5：Hexadecimal value, up to 27 bytes, defined by the manufacturer
- 6-127：Reserved
- 128-255：Vendor specific format

5.1.7.6 SNMP configuration

5.1.7.6.1 SNMP system configuration

In the navigation bar dropdown menu,
select Configuration**->Security->Switch->SNMP->SYSTEM ,**to enter into the page
Figure 5-11 SNMP system configuration



Item	Description
Mode	SNMP system Global enable/disable
Engine ID	SNMPv3 engine ID Valid only if configured as SNMP v3

	By default, the initial engine ID is generated based on the device information

5.1.7.6.2 SNMP community configuration

In the navigation bar dropdown menu,
select **Configuration->Security->Switch->SNMP->COMMUNITY,**to enter into the page
Only SNMP v1 and SNMPv2 are valid.
Chart Figure 5-13 SNMP community configuration

Item	Description
Delete	Select and delete the corresponding table item when saving next time
Community name	Community name
Community secret	Community character string
source IP	The server IP range that the community is allowed to use
Source mask length	The length of the server IP mask that the community is allowed to use

- You need to add the permission setting of the corresponding community name in the SNMP group configuration before you can access it normally. By default, the system configures the access rights of public and private users.

- Community configuration only works for SNMPv1 and SNMPv2. If SNMPv3 needs to be configured, SNMP users and groups need to be configured。

- In practical application, when configuring the read / write community, if the device configuration community name is inconsistent with the community secret, the community secret shall prevail。

- If you don't care about the IP of the community server, please configure the source IP to 0.0.0.0 and the length of the source mask to 0

5.1.7.6.3 SNMP user configuration

In the navigation bar dropdown menu,
select **Configuration->Security->Switch->SNMP->USER,**to enter into the page
Only valid for SNMP v3
Figure 5-12 SNMP user configuration

Item	Description
Delete	Select and delete the corresponding table item when saving next time
Engine ID	User's engine ID Whether the user is a local user can be judged by whether the engine ID is a local engine ID The local engine ID refers to the engine ID configuration in the system configuration
User name	User name string
Security Level	Configure user security level
Authentication protocol	Authentication protocol type
Authentication password	Password string for authentication
Privacy agreement	Types of information encryption protocols
Privacy password	The key of information encryption.

Note: need to add the permission setting of the corresponding user name in the SNMP group configuration before you can access it normally

5.1.7.6.4 SNMP group configuration

In the navigation bar dropdown menu,
select **Configuration->Security->Switch->SNMP->GROUP,**to enter into the page
Figure 5-13 SNMP group configuration

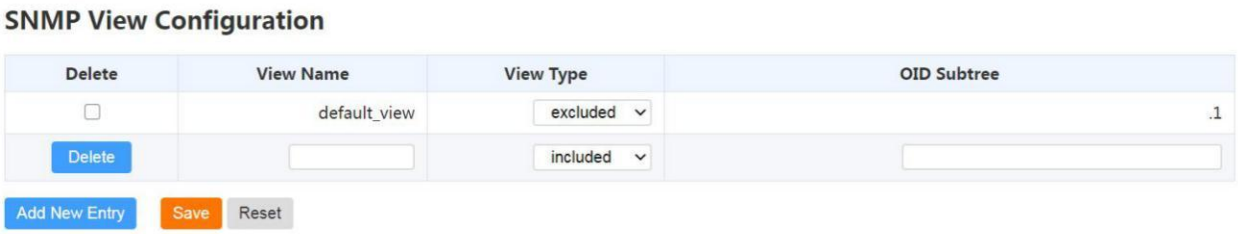
Item	Description
Delete	Select and delete the corresponding table item when saving next time
Security model	Configure security model version V1: SNMP V1 compatible security model

	V2c: Security model compatible with SNMP V2 Usm: User based security model of SNMP V3
Security name	V1 / V2C is the corresponding community name V3 is the user name
Group name	SNMP group name string

• You need to add the relevant configuration of the corresponding group name in the SNMP access control configuration before normal access

5.1.7.6.5 SNMP view configuration

In the navigation bar dropdown menu,
select **Configuration->Security->Switch->SNMP->VIEW,**to enter into the page
Figure 5-14 SNMP view configuration



Item	Description
Delete	Select and delete the corresponding table item when saving next time
View name	View name string
View types	Included: Which OID subtrees are included Excluded: Which OID subtrees to remove
OID subtree	OID subtree information

5.1.7.6.6 SNMP access control configuration

Web path: **Configuration->Security->Switch->SNMP->ACCESS**
Figure 5-15 SNMP access configuration

Item	Description
Delete	Select and delete the corresponding table item when saving next time
Group name	SNMPv3 group name
Security	Configure security model version

model	V1: Security model compatible with SNMP v1 V2c: Security model compatible with SNMP V2 Usm: User based security model of SNMP V3 Any: All security models are valid
Security level	Configure the security level. The security level from big to small is "auth, priv" > "auth, nopriv" > "noauth, nopriv".
Read view name	Read view name None means no view
Write view name	Write view name None means no view

- The configurable group name in SNMP access control comes from SNMP group configuration. First add the group name in SNMP group configuration, and then configure the security and view of the group in SNMP access control.

- The security level of the groups associated with SNMPv1 and SNMPv2 users must contain "noauth, nopriv", otherwise they cannot be accessed

- The security level in SNMP access control is higher than the SNMP user security level. If the security level of SNMPv3 user is less than the access control security level of the group, the SNMP user will not be able to access it. For example, the security level of access control is "auth, nopriv". SNMPv3 users with "noauth, nopriv" under the group where the access control is located cannot access SNMPv3 users, and SNMPv3 users of "auth, nopriv", "auth, priv" can access.

- In the security model of SNMP access control, the same group name allows multiple different security models. When different security models of the same group have intersection (such as any, USM), but the configured security level is inconsistent, the one with lower security level will take effect. That is to say, when SNMPv3 users satisfy multiple access controls at the same time, they only need to satisfy the security level of one of them

- The configurable read and write views in SNMP access control come from the SNMP view configuration. First add a view to the SNMP view configuration, and then associate the view in SNMP access control

---

5.1.7.6.7 SNMP Trap configuration

Web path: **Configuration->Security->Switch->SNMP->Trap**

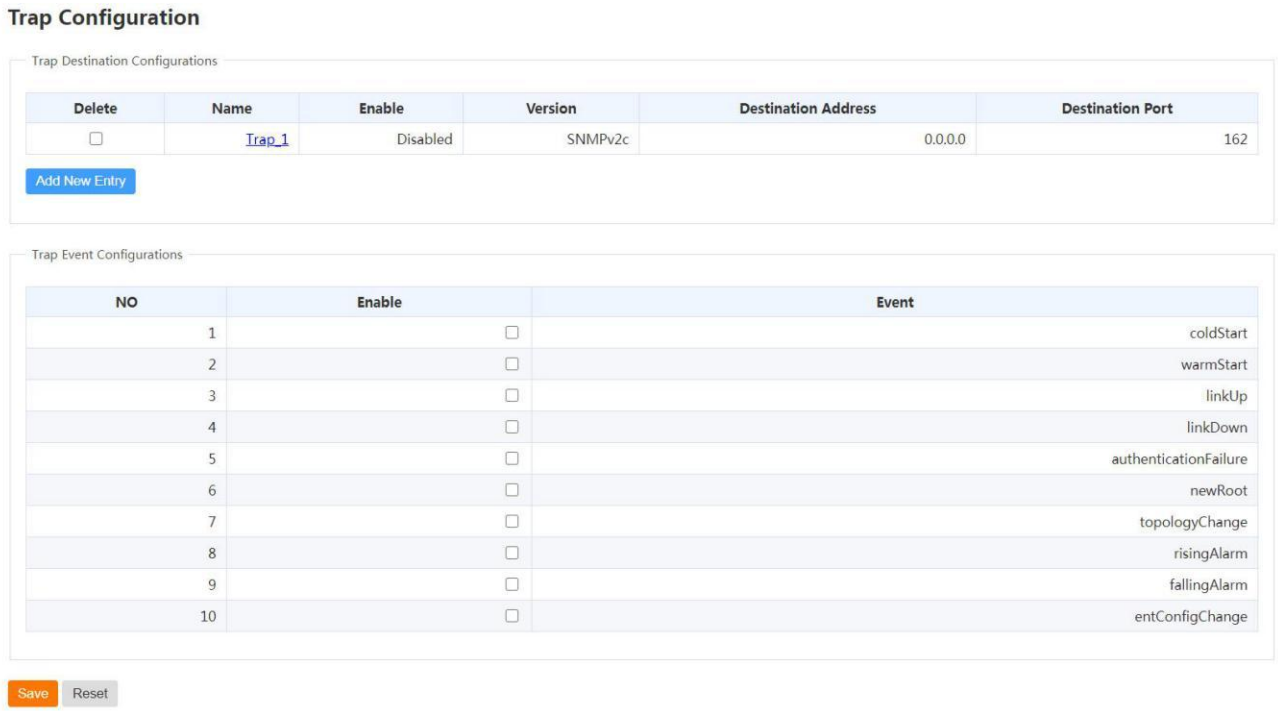
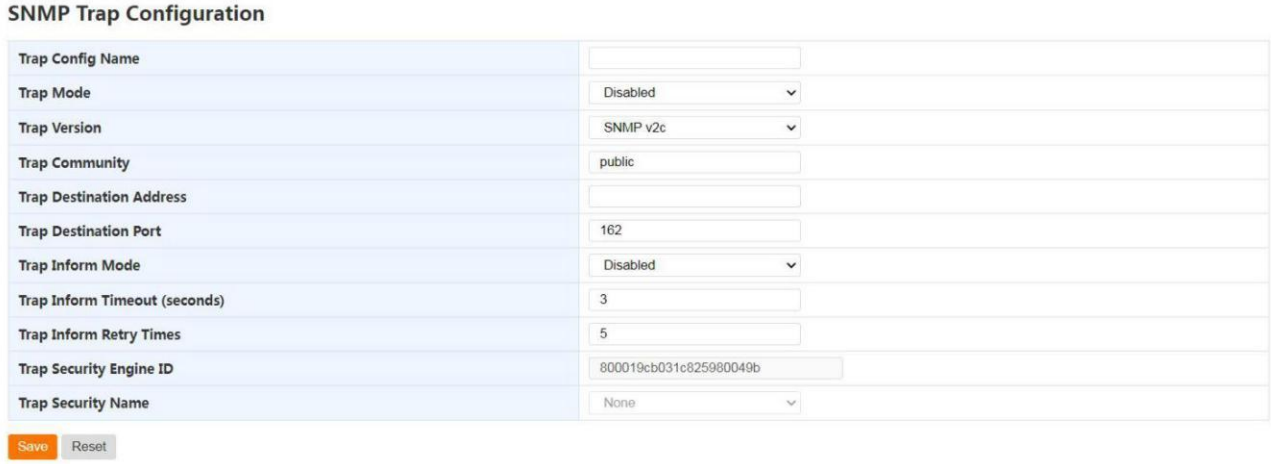


Figure 5-16 SNMP Trap configuration

Click the [add new entry] button to enter the trap destination configuration interface
Figure 5-17 SNMP Trap destination configuration



Item	Description
Trap name	Configuration name string. 1-32 bytes

Trap mode	Current trap configuration on/off status
Trap version	Protocol versions currently supported by trap Ensure that the trap server supports this version
Trap Community	Trap community Only SNMPv2 is valid
Trap destination address	Trap server IP address
Trap target port	Trap server listening port
Trap notification mode	Enable / disable trap notification mode Only SNMPv2 is valid
Trap notification timeout (seconds)	Notification message timeout setting
Trap notification retransmission times	Notification message timeout retransmission times setting
Trap detection security engine ID	Enable / disable automatic detection of trap server security engine ID Only SNMP v3 is valid
Trap security engine ID	When the detection security engine ID is turned on, the system will automatically fill in this field without configuration Only SNMP v3 is valid
Trap security name	Trap communication security name Only SNMP v3 is valid

5.1.7.7 CLI reference command

Command	switch(config)# snmp-server switch(config)# no snmp-server switch(config)# snmp-server engine-id local 800019cb037cec9b010051 switch(config)# no snmp-server engine-id local
Description	Turn on SNMP service Turn off SNMP service Configure SNMP engine ID Restore SNMP default engine ID

Command	switch(config)# snmp-server community user ip-range 0.0.0.0 0.0.0.0 user1 switch(config)# no snmp-server community user
Description	Add SNMP community configuration Delete SNMP community configuration

Command	switch(config)# snmp-server user v3user engine-id 800019cb037cec9b010050 switch(config)# snmp-server user v3user engine-id 800019cb037cec9b010050 md5 password switch(config)# snmp-server user v3user engine-id 800019cb037cec9b010050 md5 password priv des password

	switch(config)# no snmp-server user v3user engine-id 800019cb037cec9b010050
Description	Add SNMP “NoAuth, NoPriv”user configuration Add SNMP “Auth,NoPriv”user configuration Add SNMP “Auth,Priv”user configuration Delete SNMP user configuration

Command	switch(config)# snmp-server community user ip-range 0.0.0.0 0.0.0.0 user1 switch(config)# no snmp-server security-to-group model v2c name test
Description	Add SNMP group configuration Delete SNMP group confirmation

Command	switch(config)# snmp-server view v3_view .1.3.6.2 include switch(config)# no snmp-server view v3_view .1.3.6.2
Description	Add SNMP view configuration Delete SNMP view configuration

Command	switch(config)# snmp-server access v3_rw_gourp model v3 level noauth read default_view write default_view switch(config)# snmp-server access v3_rw_gourp model v3 level auth read default_view write default_view switch(config)# snmp-server access v3_rw_gourp model v3 level priv read default_view write default_view switch(config)# no snmp-server view v3_view .1.3.6.2
Description	Add SNMP “NoAuth,NoPriv”access control Add SNMP “Auth, NoPriv”access control Add SNMP “Auth, Priv”access control Delete SNMP access control configuration

Command	switch (config)# snmp-server host traphost switch (config)# no snmp-server host traphost
Description	Create/Entry SNMP Trap destination configuration Delete Trap destination configuration

Command	switch(config-snmps-host)# shutdown switch(config-snmps-host)# no shutdown switch(config-snmps-host)# version v2 public switch(config-snmps-host)# version v3 engineID 800019cb037cec9b010050 user3 switch(config-snmps-host)# host 192.168.1.101 162 informs switch(config-snmps-host)# informs retries 5 timeout 3

Description	Turn off SNMP Trap Enable SNMP Trap Configure SNMP Trap is SNMPv2,and community configuration The version of SNMP trap is SNMPv3, and the engine ID and security name are configured Configure the target address, target port and notification mode (information, traps) of the SNMP trap Configure the notification retransmission times and notification timeout of the SNMP trap

Command	switch(config)# snmp-server view v3_view .1.3.6.2 include switch(config)# no snmp-server view v3_view .1.3.6.2
Description	Enable SNMP trap linkup event Close SNMP trap linkup event

Command	switch# show snmp switch# show snmp host switch# show snmp trap
Description	View SNMP configuration information (including system, community, group, view and access control) View SNMP trap destination configuration View SNMP trap event configuration

5.1.7.8 SNMP configuration case

5.1.7.8.1 SNMPv2 configuration

- Case requirement

Add SNMPv2 users, the read group is v2read, and the write group is v2write. Only 192.168.1.0/24 can be accessed by users

- Operation steps

1. Add SNMP read / write community

Figure 5-18 add SNMP read、write community configuration

SNMPv1/SNMPv2 Community Configuration

Delete	Community name	Community secret	Source IP	Source Prefix
☐	public	public	0.0.0.0	0
☐	private	private	0.0.0.0	0
☐	v2user1	v2read	192.168.1.0	24
☐	v2user2	v2write	192.168.1.0	24

Add New Entry | Save | Reset

2. Add SNMP group configuration and use default_ ro_ group、default_ rw_ Group

Figure 5-19add SNMP group configuration

3. The client adds the SNMPv2 user, and the reading group is v2read; the writing group is v2write. Determine that access IP is limited to 192.168.1.0/24 network segments.

5.1.7.8.2 SNMPv3 configuration

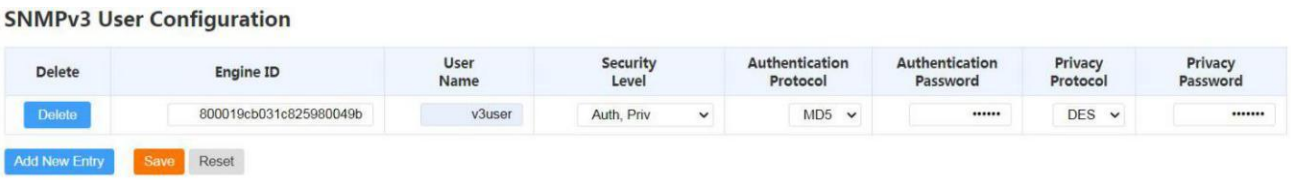
- Case needs

Add SNMPv3 user, security level is “Auth,Priv”

- Operation steps

1. Add SNMP user, configure security level as “Auth,Priv”, meanwhile configure the corresponding protocol and password

Figure 5-20add SNMP user configuration



2. Add SNMP Group configuration, security model is usm. Use the default_rw-group.

Figure 5-23 Add SNMP group configuration

SNMP Group Configuration

Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	v2c	v2user1	default_ro_group
☐	v2c	v2user2	default_rw_group
Delete	usm	v3user	default_rw_group

Add New Entry | Save | Reset

3. When client add the SNMPv3 user, security level is “Auth,Priv”, meanwhile input correspondingly protocol,password.

If need to fill in the context name field, please leave it blank

---

5.1.8 RMON

5.1.8.1 Overview

ROMN (Remote Network Monitoring) is used for managing local area networks and process sites from a central point. In RMON, network monitoring data includes a set of statistical data and performance indicators, which can be used to monitor network utilization for network planning, performance optimization and network error diagnosis. RMON is mainly used for process monitoring and management from the management device to the monitored management device.

RMON defines multiple RMON groups. Our company supports statistical group, history group, alarm group and event group. The following is a brief introduction to the four groups:

- Statistics Group

Statistics is used to monitor and count the traffic information of Ethernet interface. It is the accumulated value from the creation of table items to the current stage. The statistics contents include discarded packets, broadcast packets, multicast packets, CRC errors, size blocks, conflicts, etc. the statistics results will be saved in the Ethernet statistics table for the administrator to view at any time

- History Group

History group is used to collect network traffic information regularly, record the accumulated value and bandwidth utilization of network traffic information in each cycle, and save it in the history control table for later processing by the administrator. It contains two groups:

- The history control group is used to set the sampling interval, sampling data source and other control information
- The Ethernet history group provides the administrator with the historical data of statistical information such as network segment traffic, error packets, broadcast packets, utilization and collision times.

■ Alarm Group

The alarm group is used to monitor the specified MIB (management information base) object. When the value of the MIB object exceeds the set upper limit value or is lower than the set lower limit value, an alarm will be triggered, and the alarm will be treated as an event

■ Event Group

Event groups are used to define how events are handled. When the monitored MIB object reaches the alarm condition, an event will be triggered. There are four processing methods for the event

- None: no action
- Log: record the event related information in the log table, so that the administrator can view it at any time
- Trap: Send trap message to the network management to inform the occurrence of the event
- Log and trap: record the event related information in the log record table, and send trap messages to the network management

5.1.8.2 Statistics

■ Configuration

From the [navigation bar] drop-down menu to select configuration > Security > Switch > RMON > statistics

Figure 5-21 ROMN Statistics Configuration

- Delete: select and delete the corresponding table item next time
- ID: the unique identification of the table item, ranging from 1 to 65535

- Data source: indicates the port to be monitored. The text box to be filled in consists of: switch ID * 1000000 + port number. The switch ID of non stack system is 1, so port 4 needs to fill in 1000004
- Add new table item: add a new table item

■ Status Overview

From the [navigation bar] drop-down menu to select : Monitor->Security->Switch->RMON->Statistics

Figure 5-22 RMON Statistic status overview

Item	Description
ID	Statistical table item ID
Data source	The ID of the port to monitor. (switch ID * 1000000 + port number), for example, port 4 is 1000004
Discard	Total number of events that the probe dropped packets due to lack of resources
Byte	Total number of bytes of received message (including bad message data)
Message	Total number of received messages (including bad messages, broadcast messages and multicast messages)
Broadcast	The total number of normal messages received pointing to the broadcast address
Multicast	The total number of normal messages received pointing to the multicast address
CRE Error	The total number of received messages (excluding frame start bit but including FCS) between 64-1518 bytes, but with FCS error. Alignment errors are also included
Under size	The total number of messages whose length is less than 64 bytes
Oversize	Total number of messages received with message length over 1518 bytes
Frag.	Total number of received CRC error messages with message length less than 64 bytes
Jabb.	Total number of messages received CRC error with message length greater than 1518 bytes
Coll.	The total number of packet losses due to conflicts
64bytes	The total number of messages with the length of 64 bytes received
65~127	The total number of messages with the length of 64-127 bytes received
128~255	The total number of messages with the length of 128-255 bytes received
256~511	The total number of messages with the length of 256-511 bytes received

512~1023	The total number of messages with the length of 512-1023 bytes received
1024~1588	The total number of messages with the length of 1024-1588 bytes received

5.1.8.3 History

- Configuration

From the [navigation bar] drop-down menu to select:
Configuration-> Security-> Switch-> RMON-> History

Figure 5-23 RMON History configuration

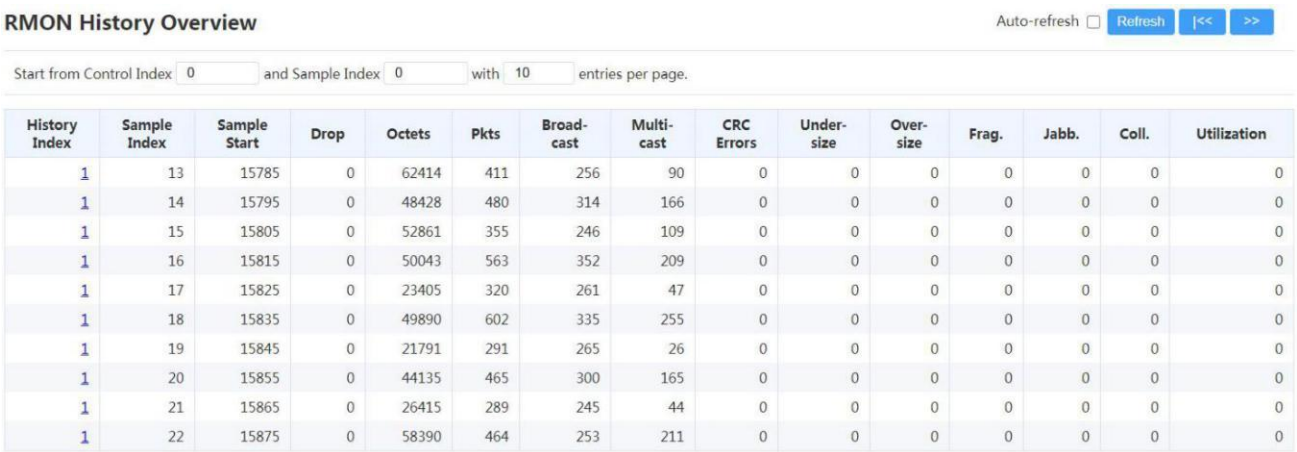
Item	Description
Delete	Select and delete the corresponding table item when saving next time
ID	The unique identifier of this entry, ranging from 1-65535.
Data source	The ID of the port to be monitored. (Switch ID * 1000000 + port number), for example, port 4 is 1000004.
Interval	Indicates the time interval (in seconds) for sampling historical statistical data. The range is 1 to 3600, and the default value is 1800 seconds.
Buckets	Represents the largest data entry associated with this history control entry stored in RMON. The range is 1 to 3600, and the default value is 50.
Buckets Granted	Represents the number of authorized management data entries of this history control entry stored in RMON. It is not configurable, and is allocated according to the configuration value system.

- Display

➢ Overview

From the [navigation bar] drop-down menu to select:
Monitor-> Security-> Switch-> RMON-> History

Figure 5-24 RMON History Overview



Item	Description
History ID	ID of the history control table entry
Sample ID	Indicates the ID of the data entry associated with the control table item
Sample start	The beginning time of testing the sample start, which is expressed as the number of seconds from the start of the device to the current time
Discard	The total number of events during this sampling interval that caused the probe to drop packets due to lack of resources
Byte	The total number of bytes of messages received during this sampling interval (including bad message data)
Messages	Total number of messages received during this sampling interval (including bad message, broadcast message and multicast message)
Broadcast	The total number of normal messages to the broadcast address received during this sampling interval
Multicast	The total number of normal messages to multicast addresses received during this sampling interval
CRC Error	The total number of messages received during this sampling interval (excluding frame start bits, but including FCS) between 64-1518 bytes, but FCS errors. Alignment errors are also included
Under size	The total number of messages less than 64 bytes received during this sampling interval
Over size	The total number of messages more than 1518 bytes received during this sampling interval
Frag.	The total number of CRC error messages with message length less than 64 bytes received during this sampling interval
Jabb.	The total number of CRC error messages with message length greater than 1518 bytes received during this sampling interval
Coll.	The total number of packet losses due to collisions during this sampling interval
Utilization rate	The best estimate of the average physical layer network utilization on this port during this sampling interval, in percent

- Details

Click history ID to display the details of the data entry determined by the corresponding history ID + sample ID

Figure 5-25 Detailed RMON History

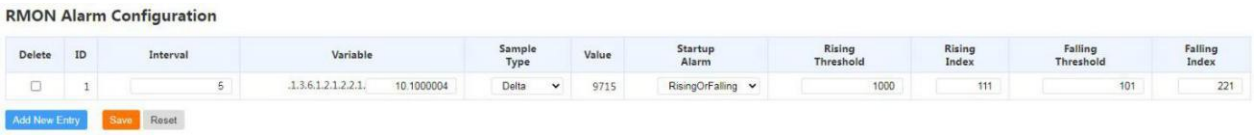
As above, details with history ID 1 and sample ID 119 are shown

5.1.8.4 Alarm

- Configuration

From the [navigation bar] drop-down menu to select:
Configuration->Security->Switch->RMON->Alarm

Figure 5-26 RMON ALARM Configuration



Item	Description
Delete	Select and delete the corresponding table item when saving next time
ID	The table item is uniquely identified, ranging from 1 to 65535
Interval	The sampling time interval (seconds) is used to compare the rising threshold and the falling threshold. The range is 1 to 2 ^ 31-1
variable	It consists of two parts ➢ The first section: sampling type, which indicates the data to be sampled, with the range of 10-21. 10: Represents InOctets, the number of bytes received by the interface, including frame spacing. 11: Represents InUcastPkts, the number of unicast packets received by the interface. 12: Represents InNUcastPkts, the number of non-unicast packets (that is, broadcast or multicast) received by the interface. 13: Represents InDiscards, the number of received but discarded packets (even if normal packets are discarded). 14: Represents InErrors, the number of error packets received by the interface. 15: Represents InUnknownProtos, the number of packets discarded because the interface receives an unknown protocol or does not support the protocol. 16: Represents OutOctets, the number of bytes sent by the interface,

	including frame spacing. 17: Represents OutUcastPkts, the number of unicast packets sent by the interface. 18: Represents OutNUcastPkts, the number of non-unicast packets (that is, broadcast or multicast) sent by the interface. 19: Represents OutDiscards, the number of packets discarded in the output phase on the interface (even if normal packets are discarded). 20: Represents OutErrors, the number of packets that the interface cannot output due to packet errors. 21：Represents OutQLen, the length of the output queue of the interface (in the unit of message, it indicates the queue status of the message when the interface is output). ➢ The second section: data source, the ID of the port to be monitored (switch ID * 100000 + port number), for example, port 4 is 100004.
Sample type	Sample the selected variable and calculate the method to compare with the waterline. The possible sample types are ➢ Absolute value: directly use the sampled value to compare with the waterline ➢ Difference: the difference between the values of two adjacent samples is compared with the waterline
Value	Last sampled value, not configured
Start alarm	Type of start alarm ➢ Rise: when the absolute value or difference (depending on the sample type) of the sample is greater than the rise waterline for the first time, the alarm will be triggered ➢ Descent: when the absolute value or difference (depending on the sample type) of the sample is less than the descent waterline for the first time, the alarm will be triggered ➢ Rise or fall: the alarm can be triggered when the absolute value or difference (depending on the sample type) of the sample is greater than the rising waterline or less than the falling waterline for the first time
Rising waterline	The value is 1-2147483647, which is larger than the descending waterline
Rising ID	Rise event ID, the corresponding ID when the rise alarm is triggered. Value 1-65535
Descent waterline	The value is 1-2147483647 and less than the rising waterline
Descent ID	Descent event ID, the corresponding ID when the descent alarm is triggered. Value 1-65535

■ Display

From the [navigation bar] drop-down menu to select:
Monitor-> Security-> Switch-> RMON-> ALARM

Figure 5-27 RMON Alarm Overview

The above is the overview information. Click the corresponding ID to enter the details page of the corresponding alarm

Figure 5-28 Detailed RMON History

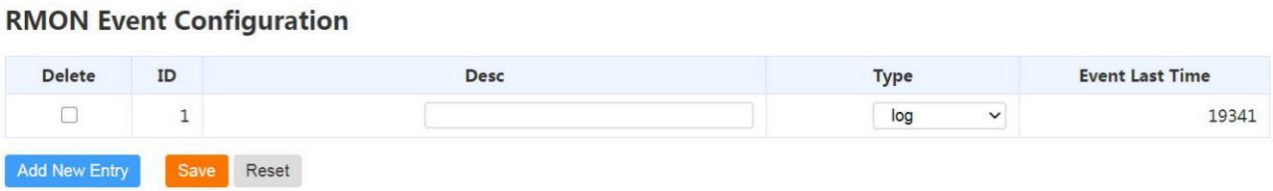
There is no difference between the information page configuration page information displayed on these two pages

5.1.8.5 EVENT

- Configuration

From the [navigation bar] drop-down menu to select:
Monitor-> Security-> Switch-> RMON-> Event

Figure 5-29 RMON Event Configuration



Item	Description
Delete	Select and delete the corresponding table item when saving next time
ID	The table item is uniquely identified, ranging from 1 to 65535
Description	Event description, string length is 0 to 127, default is empty string
Types	Represents the processing type of the event. The possible types are: None: no SNMP log or SNMP trap Log: creates an SNMP log entry when the - event is triggered Trap: send SNMP trap when trigger - event Log and trap: create SNMP log entry and send SNMP trap when event is triggered
The time when the most recent event occurred	The time when the event was last triggered by this event entry. The time is expressed as the number of seconds from the start of the device to the current time. Not configured.

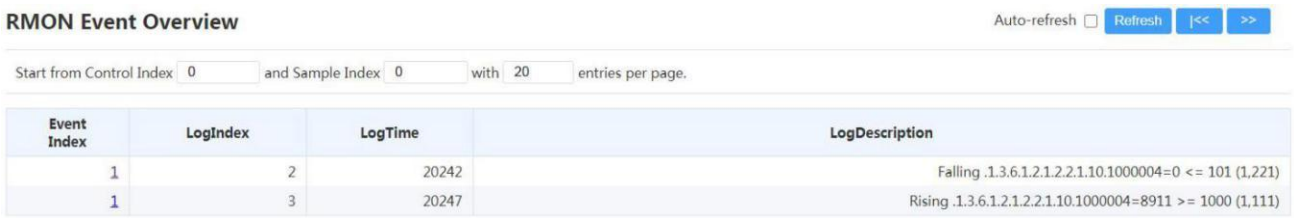
Note

• If want the alarm trap to take effect, you must configure the destination trap in the SNMP trap configuration, and open the two trap events rising alarm and falling alarm in the SNMP trap event.

■ Display

From the [navigation bar] drop-down menu to select:
Monitor-> Security-> Switch-> RMON-> Event

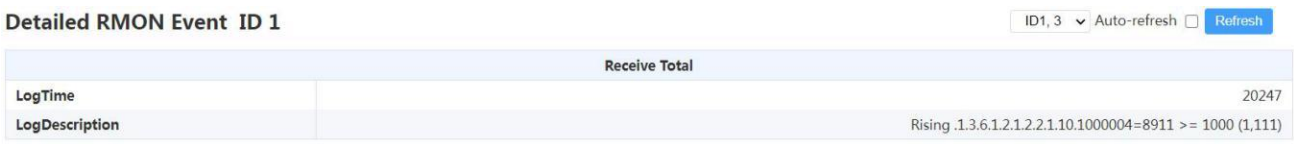
Figure 5-30 RMON Event Overview



Item	Description
Event ID	Indicates the ID of the event target
Log ID	An event may be triggered many times, and each trigger will generate a log entry, which represents the ID of the log entry
Log time	The time when the log entry was generated. The time is expressed as the number of seconds from the start of the device to the current time
Log Description	Log content, which records the corresponding alarm event. Where startup indicates the first trigger of the alarm.

Click the event ID above to enter the log entry details page corresponding to the event ID + log ID

Figure 5-31 Detailed RMON Event



5.1.8.6 CLI reference command

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter Configuration Port

Command	switch(config-if)# rmon collection stats 22 switch(config-if)# no rmon collection stats 22 switch(config-if)# rmon collection history 34 buckets 50 interval 5

	switch(config-if)# no rmon collection history 34
Description	Add RMON port statistics configuration; Delete RMON port statistics configuration; Add historical configuration of RMON port; Delete the historical configuration of the RMON port;

Command	switch(config)# rmon alarm 1 ifInNUcastPkts 1000002 5 delta rising-threshold 1000 111 falling-threshold 100 222 falling switch(config)# no rmon alarm 1 switch(config)# rmon event 1 log trap description test switch(config)# no rmon event 1
Description	Add RMON Alarm configuration Delete RMON Alarm configuration Add RMON Even configuration Delete RMON Even configuration

Command	switch# show rmon statistics switch# show rmon history switch# show rmon alarm switch# show rmon event
Description	Print RMON statistics Print RMON History Print RMON Alarm Print RMON event location and related logs

5.2 NETWORK

5.2.1 Port security

Port security can reduce the risk of system instability caused by single port attack by restricting the number of legitimate users. Users can configure the maximum number of users to access the port according to the empirical value. When the number of users exceeds the user limit within a certain period of time, the port security violation will be triggered. There are three types of processing: protect, restrict and shutdown

- Protect: When the number of MAC addresses learned by the port exceeds the user limit, the violation will be triggered. Only messages whose source MAC is the learned MAC address of the port are allowed to be released
- Restrict: When the number of MAC addresses learned by the port exceeds the user limit, the violation will be triggered. More than the number of MAC addresses are marked as violation addresses, and the number of violation addresses does not exceed the configured violation limit. Illegal address will be deleted after hold time. Only messages whose source MAC is the learned MAC address (excluding the illegal address) of the port are allowed to be released.

- Shutdown: Shutdown: when the number of MAC addresses learned by the port reaches the user limit, any new MAC address will trigger violation, and the port will be shut down. All the previously learned security addresses will be cleared, the port will not be available, and all messages will not be released.

5.2.1.1 Configure port security

From the [navigation bar] drop-down menu to select:
Configuration-> Security-> Network-> Port Security

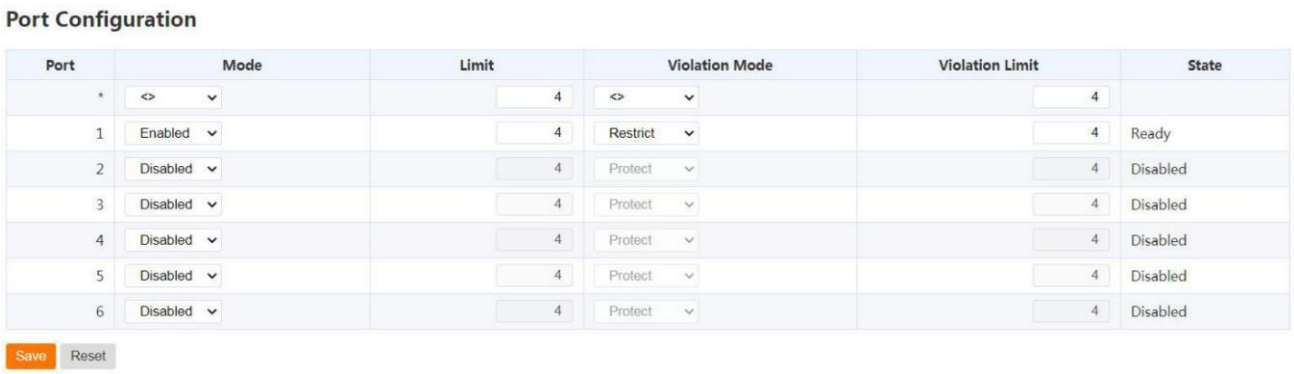
- System configuration

Figure 5-32 Port security system configuration

Item	Description
Enable Aging	Enable aging enable switch, default off
Aging cycle	The aging period of the port's normal Mac, ranging from 10 to 10000000 seconds, is 3600 seconds by default. This parameter is meaningful only when aging is enabled
Duration	Determine the retention time of the illegal MAC address in the MAC table, ranging from 10 to 10000000 seconds, and the default is 300 seconds

- Port Configuration

Figure 5-33 Port configuration



Item	Description
Port	Port No. on the pannel
Mode	The port enables the port security function, which is off by default
User Limited	The maximum number of users on the port, ranging from 1 to 1023, is 4 by default
Violation mode	Protect, restrict, and shutdown. For details, see the previous description. The default is protect
Violation Limited	When restrict is used in violation mode, it indicates the maximum number of

	allowed violation Macs. The range is 1-1023, and the default is 4.
Status	Disabled: Port security shutdown Ready: The port is opened safely, but the number of users does not reach the user limit Limite Reached: The number of users has reached the limit Shutdown: The port is opened safely, the violation mode is shutdown, and the number of users exceeds the user limit。

Note

• After opening port security, the MAC addresses learned by the port become static addresses (for the MAC address table module), and normal MAC (when the number of users does not exceed the user limit) is controlled according to the port security "aging cycle" (Aging is not activated by default), the offending MAC (when the behavior is Restrict and the number of users exceeds the limit) controls the time in the table entry according to the "duration" of port security.

• When the violation mode is configured as Shutdown, when the shutdown of the violation port is triggered, it can be restored by closing the port security or changing the safety violation mode to Protect or Restrict.

5.2.1.2 View port security information

In the [Navigation Bar] drop-down menu, select: Monitoring -> Security -> Network -> Port Security -> Switch to enter the global view interface.

Figure 5-37 View port security information

Port Security Switch Status

Auto-refresh ☐ Refresh

User Module Legend

User Module Name	Abbr
Port Security (Admin)	P
802.1X	8

Port Status

Clear	Port	Users	Violation Mode	State	MAC Count		
					Current	Violating	Limit
Clear	1	P-	Restrict	Ready	0	0	4
Clear	2	--	Disabled	Disabled	-	-	-
Clear	3	--	Disabled	Disabled	-	-	-
Clear	4	--	Disabled	Disabled	-	-	-
Clear	5	--	Disabled	Disabled	-	-	-
Clear	6	--	Disabled	Disabled	-	-	-

- User module description

  There are currently two modules that will use the port security function, one is the port security module, and the other is the 802.1X module. The abbreviation is shown here.
- Port status

Item	Description
Clear	Click to clear all port security MAC addresses of this port. It can be clicked only when the MAC address of the port is not 0.
Port	Panel port number, click to enter the port MAC address information view interface.
User	Explain which user module/user module the MAC address corresponds to.
Status	Disabled: the port is safely closed. Ready: the port is securely enabled, but the number of users has not reached the user limit. Limited Reached: port security is enabled, and the number of users reaches the user limit. Shutdown: the port is safely opened, the violation mode is Shutdown, and the number of users exceeds the user limit.
MAC count/current	The current MAC address number of the port.
MAC count/violation	The current number of illegal MAC addresses of the port.
MAC count/limit	The number of port users configured by the user is limited.

Click the corresponding port in the above figure, or select from the [Navigation Bar] drop-down menu: Monitoring -> Security -> Network -> Port Security -> Port to enter the port view interface.

Item	Description
Clear	Click to clear the corresponding user information.
VLAN ID	The VLAN ID corresponding to the user.
MAC address	MAC address corresponding to the user.
Status	Forwarding：Indicates that the user is a normal user. Violating：Indicates that the user is a violation user.
Aging/Keeping	For normal users, it indicates the remaining aging time. If aging is not turned on, it will be displayed as "-". For offending users, it indicates the remaining hold time.

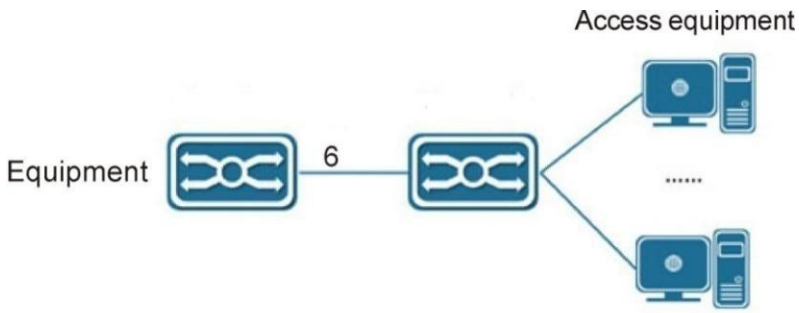
5.2.1.3 Typical configuration cases of port user restrictions

- Case requirements

In the system environment, port 4 is connected to the access device to expand the number of terminal access. During normal operation, there should be no more than 10 users

accessing the 8 ports. If more than 10 users may be accessing illegal users or the terminal may initiate a MAC address flooding attack, the device needs to automatically perform preventive operations to avoid affecting the operation of the entire device.

Figure 5-38 port user restriction case



■ Operation Steps

Port user limit configuration interface, system configuration, global enable port speed limit function; port configuration enable 6 port user limit function, user limit is 10, select the behavior Shutdown.

Chart Figure 5-39 Port Security Case Configuration

Port Security Configuration Refresh

Global Configuration

Aging Enabled	☑
Aging Period	3600 seconds
Hold Time	300 seconds

Port Configuration

Port	Mode	Limit	Violation Mode	Violation Limit	State
*	<>	4	<>	4	
1	Disabled	4	Protect	4	Disabled
2	Disabled	4	Protect	4	Disabled
3	Disabled	4	Protect	4	Disabled
4	Disabled	4	Protect	4	Disabled
5	Disabled	4	Protect	4	Disabled
6	Enabled	10	Shutdown	4	Ready

Save Reset

Simulate the MAC address flooding attack on the terminal to trigger a port violation. Through the viewing interface, port 8 is in the Shutdown state.

Chart Figure 5-40 Port Security Case Status

Port Security Switch Status Auto-refresh ☐ Refresh

User Module Legend

User Module Name	Abbr
Port Security (Admin)	P
802.1X	8

Port Status

Clear	Port	Users	Violation Mode	State	MAC Count		
					Current	Violating	Limit
Clear	1	--	Disabled	Disabled	-	-	-
Clear	2	--	Disabled	Disabled	-	-	-
Clear	3	--	Disabled	Disabled	-	-	-
Clear	4	--	Disabled	Disabled	-	-	-
Clear	5	--	Disabled	Disabled	-	-	-
Clear	6	P-	Shutdown	Ready	0	0	10

5.2.1.4 CLI Reference Command

Command	switch(config)# port-security aging switch(config)# port-security aging time 3600 switch(config)# port-security hold time 300
Description	Enable port security address aging; Configure the port security address aging cycle; Configure the port security violation address duration;

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# port-security switch(config-if)# no port-security switch(config-if)# port-security maximum 5 switch(config-if)# port-security violation shutdown switch(config-if)# port-security maximum-violation 4
Description	Turn on port security; Turn off port security; Configure port security user limit number; Configure port security violation mode; Configure the number of port security violation limits;

Command	switch# clear port-security dynamic address 00-bb-60-2e-01-e4 vlan 1
Description	Clear the port security address;

Command	switch# show port-security switch# show port-security address
Description	Print port security status; Print port security address information;

5.2.2 NAS

5.2.2.1 802.1X Agreement overview

The IEEE802 LAN/WAN committee proposed the 802.1X protocol in order to solve the problem of wireless LAN network security. Later, the 802.1X protocol was widely used in Ethernet as a common access control mechanism for LAN ports, mainly to solve the problems of authentication and security in the Ethernet.
The 802.1X protocol is a port-based network access control protocol (port based network access control protocol). "Port-based network access control" means that at the port level of the LAN access device, the accessed user equipment is authenticated to control access to network resources.

5.2.2.1.1 802.1X architecture

The 802.1X system is a typical Client/Server structure, as shown in the figure below, including three entities: client (Client), device (Device, also called NAS) and authentication server (Server).

Chart Figure 5-41 802.1X architecture

The client is an entity located at one end of the LAN segment and is authenticated by the device at the other end of the link. The client is generally a user terminal device, and the user can initiate 802.1X authentication by starting the client software. The client must support EAPOL (Extensible Authentication Protocol over LAN).

- The device end is another entity located at one end of the LAN segment, which authenticates the connected client. The device side is usually a network device that supports the 802.1X protocol. It provides a port for the client to access the LAN. The port can be a physical port or a logical port.
- The authentication server is an entity that provides authentication services for the device. The authentication server is used to implement authentication, authorization, and accounting for users, and is usually a RADIUS (Remote Authentication Dial-In User Service) server.

5.2.2.1.2 802.1X authentication method

The 802.1X authentication system uses EAP (Extensible Authentication Protocol) to realize the exchange of authentication information between the client, the device and the authentication server.

- Between the client and the device, the EAP protocol message uses the EAPOL encapsulation format and is directly carried in the LAN environment.
- There are two ways to exchange information between the device and the RADIUS server. One is that the EAP protocol message is relayed by the device and carried in the RADIUS protocol using the EAPOR (EAP over RADIUS) encapsulation format; the other is that the EAP protocol message is terminated by the device and adopts the password authentication protocol (PAP). , Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) attribute messages interact with the RADIUS server for authentication.

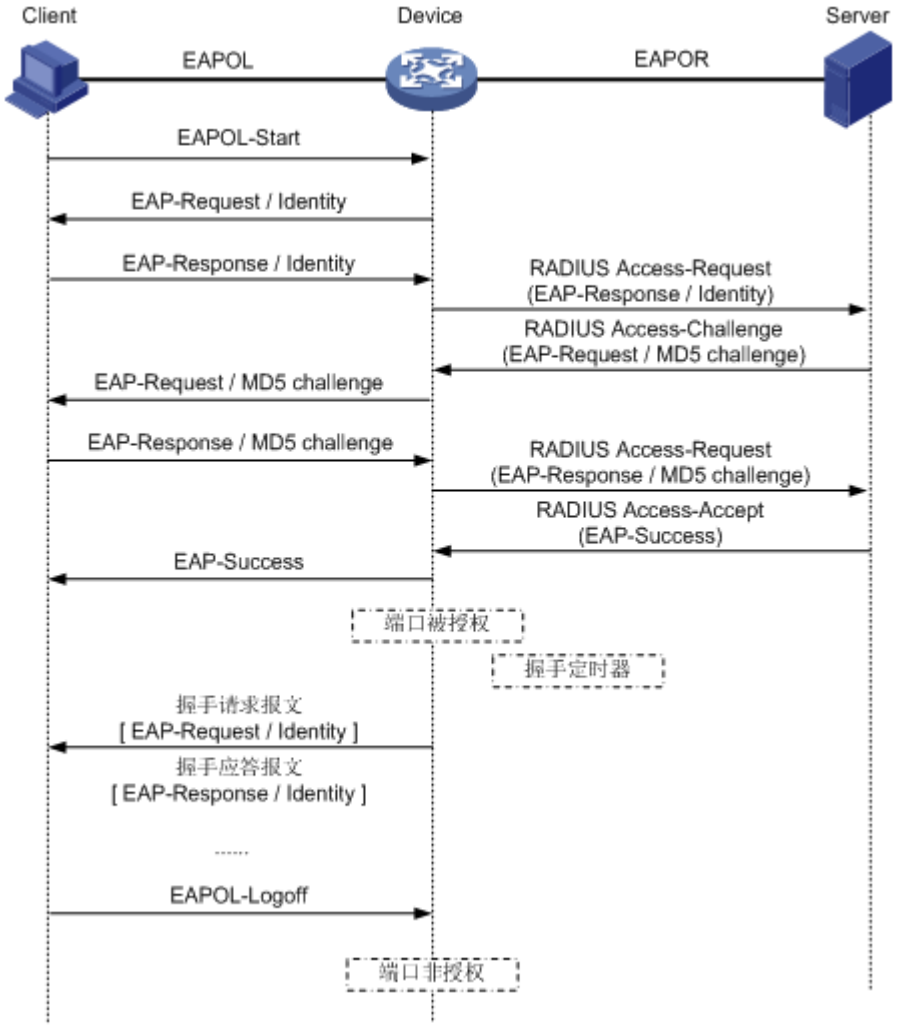
5.2.2.1.3 802.1X authentication process

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 processes of the two authentication methods take the client's initiative to initiate authentication as an example.

- EAP relay mode

This method is stipulated 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

extended authentication protocol packets can traverse the complex network to the authentication server. 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 messages and protect RADIUS messages carrying EAP-Message, respectively.
The following uses EAP-MD5 as an example to introduce the basic business process.
Chart Figure 5-42 802.1X EAP relay authentication



The certification process is as follows:
1) When the user needs to access the network, open the 802.1X client program, enter the user name and password that have been applied for 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, and 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 user name.

3) The client program responds to the request sent by the device and sends the user name information to the device through a data frame (EAP-Response/Identity message). The device sends the data frame sent by the client to the authentication server for processing after packet processing (RADIUS Access-Request packet).
4) After the RADIUS server receives the user name information forwarded by the device, it compares the information with the user name table in the database, finds the password information corresponding to the user name, and encrypts it with a randomly generated encryption word. The encrypted word is sent to the device through a RADIUS Access-Challenge message, and the device is forwarded to the client program.
5) After the client program receives the encrypted word (EAP-Request/MD5 Challenge message) from the device, it uses the encrypted word to encrypt the password part (this kind of encryption algorithm is usually irreversible) to generate EAP -Response/MD5 Challenge messages are sent 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 message is returned (RADIUS Access-Accept packet and EAP-Success packet).
7) The device changes the port to the authorized state after receiving the authentication pass message, allowing the user to access the network through the port. During this period, the device side will monitor the user's online status by periodically sending handshake messages to the client. By default, the two handshake request messages are not answered by the client, and the device will let the user go offline to prevent the user from going offline due to abnormal reasons and the device cannot perceive it.
8) The client can also send an EAPOL-Logoff message to the device to actively request to go offline. The device changes the port status from authorized status to unauthorized status, and sends an EAP-Failure message to the client.

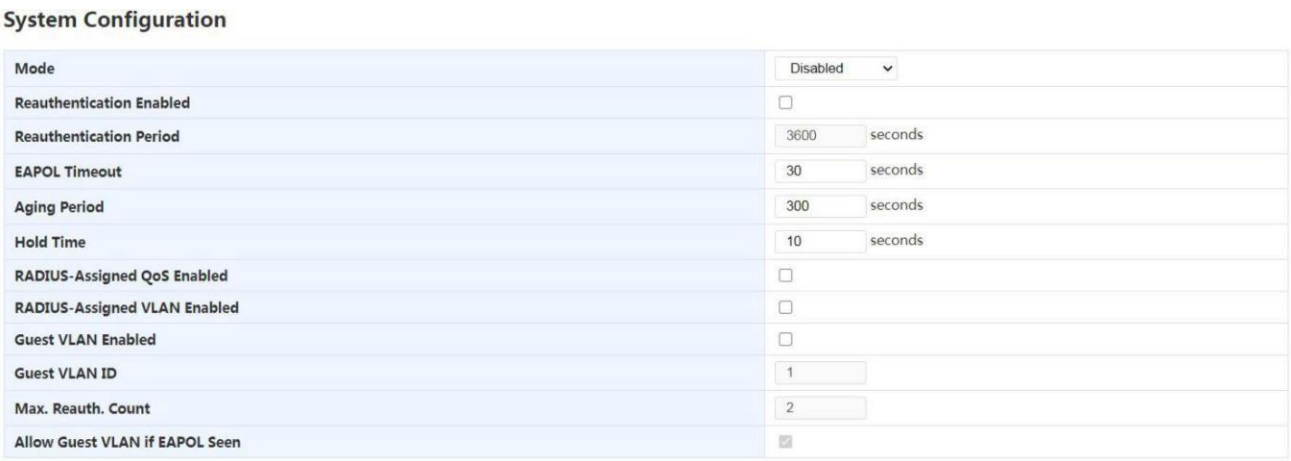
5.2.2.2 Configure NAS

NAS (Network Access Server) is a function of network access control for users, which can be either IEEE 802.1X-based authentication or MAC-based authentication.
The IEEE 802.1X standard defines a port-based access control process that prevents unauthorized access to the network by requiring users to submit credentials for authentication first. One or more central servers (back-end servers) determine whether to allow users to access the network. These back-end (RADIUS) servers are configured on the "Configuration→Security→AAA" page.
MAC-based authentication allows multiple users to be authenticated on the same port, and does not require users to install special 802.1X supplicant software on their systems. The switch uses the user's MAC address to authenticate the back-end server. Intruders can

create fake MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.
In the [Navigation Bar] drop-down menu, select: Configuration -> Security -> Network -> NAS to enter the configuration interface.

■ System Configuration

Chart Figure 5-43 NAS system configuration



Item	Description
Mode	Indicates whether NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed to forward frames.
Re-authentication enable	If selected, after the interval specified in the re-authentication period, the requester/client that has successfully passed the authentication will be re-authenticated. The re-authentication of 802.1X-enabled ports can be used to detect whether a new device has been plugged into the switch port or whether the supplicant is no longer connected. For MAC-based authentication, re-authentication is only useful when the RADIUS server configuration has been changed. It does not involve communication between the switch and the client, so it does not mean that the client still exists on the port.
Recertification cycle	Determine the time period (in seconds) for connecting clients that must be re-authenticated. This option is active only when the "Re-Authentication Enable" check box is selected. The valid value range is 1 to 3600 seconds.
EAPOL timeout	Determine the time to resend the request identification EAPOL frame. The valid value range is 1 to 65535 seconds. This has no effect on ports based on MAC authentication.
Aging cycle	This setting applies to the following modes, that is, the mode that uses the port security function to protect the MAC address: • Single user 802.1X •Multi-user 802.1X • MAC-based authentication. When the NAS module uses the port security module to protect the MAC address, the port security module needs to periodically check whether the

	corresponding MAC is active. If no activity is seen within a given period of time, the resource needs to be released. This parameter precisely controls this time period and can be set to a number between 10 and 1,000,000 seconds. If re-authentication is enabled and the port is in single-user 802.1X authentication or multi-user 802.1X authentication mode, the aging period is not important, because requesters who are no longer connected to the port will be deleted during the next re-authentication. However, if re-authentication is not enabled, the only way to release resources is to age the entries. For ports based on MAC authentication. Re-authentication does not result in direct communication between the switch and the client, so this does not detect whether the client is still connected, and the only way to release any resources is to age the entry.
Hold time	This setting applies to the following modes, that is, the mode that uses the port security function to protect the MAC address: • Single user 802.1X • Multi-user 802.1X • MAC-based authentication. If the client is denied access-either because the RADIUS server denies the client access, or because the RADIUS server request timeout (according to the timeout specified on the "Configuration→Security→AAA" page)-the client is placed on hold without authorization status. The hold timer does not count during the ongoing authentication. For the MAC-based authentication mode, the switch will ignore the new frame from the client during the hold time. The hold time can be set to a number between 10 and 1,000,000 seconds.
RADIUS designated QOS enable	RADIUS designated QoS provides a method for centralized control of traffic classes. The traffic from the successfully authenticated requester is distributed on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature. This check box provides a quick way to globally enable/disable RADIUS server-specific QoS functions. After selecting, the settings of each port will determine whether to enable RADIUS to specify the QoS class on the port. When unchecked, the RADIUS server-specified QoS class will be disabled on all ports.
RADIUS designated VLAN enable	RADIUS designated VLAN provides a centralized control method to assign VLANs on the switch for requesters who have successfully passed authentication. Incoming traffic will be classified and switched to the VLAN assigned by RADIUS. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature. This check box provides a quick way to globally enable/disable the VLAN function assigned by the RADIUS server. After selecting, the settings of each port will determine whether to enable RADIUS designated VLAN on the port. When unchecked, RADIUS server designated VLAN will be disabled on all ports

Guest VLAN enable	Guest VLAN is a special VLAN-usually with limited network access rights-after a timeout defined by the network administrator, clients that do not pay attention to 802.1X are placed on this VLAN. The switch follows a set of rules for entering and leaving the Guest VLAN. This check box provides a shortcut to globally enable/disable the Guest VLAN function. When selected, the settings of each port determine whether the port can be moved to the Guest VLAN. After unchecking, the function of moving all ports to Guest VLAN will be disabled
Guest VLAN ID	If the port moves into the Guest VLAN, the port VLAN ID of this port is set to this value. Only when the Guest VLAN option is globally enabled, can it be changed. The valid value is 1-4095.
Maximum number of request identification frames	Before considering entering the Guest VLAN, the number of times the switch sends EAPOL request identification frames without a response can be adjusted by this setting. This value can only be changed when the Guest VLAN option is globally enabled. Valid values are 1-255.
EAPOL is received and allowed to enter the Guest VLAN	The switch remembers whether EAPOL frames have been received on the port during the life cycle. Once the switch considers whether the port enters the Guest VLAN, it will first check whether this option is enabled or disabled. If disabled (unchecked; default), the switch will enter the guest VLAN only when no EAPOL frame is received on the port during the life of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if it receives EAPOL frames during the port life cycle. This value can only be changed when the Guest VLAN option is globally enabled.

■ Port configuration

Before configuring the port management status as port-based 802.1X, single-user 802.1X, multi-user 802.1X, or MAC-based authentication, you need to disable STP on the corresponding port. (Configuration -> Spanning Tree -> CIST Port page, check and remove the check box of the port corresponding to "STP Enabled" in "CIST Common Port Configuration Table")

Chart Figure 5-44 NAS Port Configuration

Item	Description
Management	If NAS is globally enabled, the authentication mode of the control port is

status	selected here. The following modes can be used: ● Mandatory authorization In this mode, the switch will send an EAPOL Success frame when the port link starts, and any client on the port will be allowed to access the network without authentication. ● Force unauthorized In this mode, when the port link starts, the switch will send an EAPOL Failure frame, and any client on the port will be prohibited from network access. ● 802.1X based on port In 802.1X, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The verifier acts as an intermediary, forwarding requests and responses between the requester and the verification server. The frames sent between the requester and the switch are special 802.1X frames called EAPOL (EAP Over LANs) frames. The EAPOL frame encapsulates the EAP PDU (RFC3748). The frames sent between the switch and the RADIUS server are RADIUS packets. The RADIUS packet also encapsulates the EAP PDU with other attributes (such as the IP address of the switch, name, and the supplicant port number on the switch). EAP is very flexible because it allows different authentication methods such as MD5-Challenge, PEAP and TLS. What is important is that the authenticator (switch) does not need to know which authentication method is being used by the requester and the authentication server, or how many information exchange frames are required for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. After the authentication is completed, the RADIUS server will send a special data packet containing a success or failure indication. In addition to forwarding this decision to the requester, the switch also uses it to open or block traffic on the switch port connected to the requester. ● Single user 802.1X In port-based 802.1X authentication, once the requester is successfully verified on the port, the entire port is opened for network traffic. This allows other clients connected to the port (for example, through a hub) to piggyback on successfully authenticated clients and gain network access, even if they are indeed not authenticated. To overcome this security hole, you can use the single-user 802.1X authentication mode. Single-user 802.1X is not actually an IEEE standard, but it has many of the same features as port-based 802.1X. In single-user 802.1X, at most one requester can be authenticated on the port at a time. Normal EAPOL frames are used for communication between the requester and the switch. If multiple requesters are connected to a port, the requester that appears first when the port link appears will be the first requester. If the requester does not provide valid credentials within a certain period of time, another requester will have a chance to obtain it. After successfully verifying the requester, only the

	requester is allowed to access. This is the safest of all modes. In this mode, the port security module is used to protect the MAC address of the requester after successfully passing the authentication. ● Multi-user 802.1X Multi-user 802.1X-just like single-user 802.1X-is not an IEEE standard, but a variant with many of the same characteristics. In multi-user 802.1X, one or more requesters can be authenticated on the same port at the same time. Each requester is individually authenticated and protected in the MAC table using the port security module. In multi-user 802.1X, the multicast BPDU MAC address cannot be used as the destination MAC address of the EAPOL frame sent from the switch to the requester, because this will cause all requesters connected to the port to reply to the request sent from the switch. Instead, the switch uses the requester's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the requester. The exception is that there is no requester yet. In this case, the switch uses the BPDU multicast MAC address as the target to send an EAPOL request identification frame-to wake up any requester that may be on the port. You can use the port security restriction control function to limit the maximum number of requesters that can connect to the port. ● MAC-based authentication Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best practice method adopted by the industry. In MAC-based authentication, the user is called the client, and the switch acts as the requester on behalf of the client. The initial frame (any type of frame) sent by the client is snooped by the switch, and the switch uses the client's MAC address as the user name and password in the subsequent EAP exchange with the RADIUS server. The switch only supports MD5-Challenge authentication, so the RADIUS server must be configured accordingly. After the authentication is completed, the RADIUS server will send a success or failure indication, which causes the switch to use the port security module to open or block the traffic of the specific client. Only in this way can the frame from the client be forwarded on the switch. This authentication does not involve EAPOL frames, therefore, MAC-based authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over 802.1X-based authentication is that the client does not require special supplicant software for authentication. The disadvantage is that malicious users may spoof the MAC address-anyone can use a device whose MAC address is a valid RADIUS user. In addition, only the MD5-Challenge method is supported. You can use the port security restriction control function to limit the maximum number of clients that can connect to the port.
RADIUS designated QOS enable	When RADIUS specifies that QoS is globally enabled and is enabled on a given port (selected), the switch will respond to the QoS information carried in the RADIUS Access-Accept packet sent by the RADIUS server when the

	requester is successfully authenticated. If it exists and is valid, the traffic received on the requester port will be classified to the given QoS level. If the (re)authentication fails or the RADIUS Access-Accept packet no longer carries the QoS class or is invalid, or the requester no longer exists on the port, the QoS class of the port will be restored to the original QoS class immediately (the administrator can Change when RADIUS is specified. This option is only applicable to port-based 802.1X. RADIUS attribute (User-Priority-Table) used to identify the QoS class: RFC4675 defines the QoS class in the Access-Accept packet. Only the attribute that appears for the first time in the data packet is considered. The 8 bytes in the attribute value are all ASCII characters in the range "0"-"7". This attribute gives the mapping value of the user priority [0:7], the 0th byte gives the user priority after the message is mapped with priority 0, and the first byte gives the priority 1 The user priority after the packet mapping. And so on.
RADIUS designated VLAN enable	When the RADIUS designated VLAN is globally enabled and the corresponding port is enabled (selected), the switch will respond to the VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when the requester successfully passes the authentication. If it exists and is valid, the port VLAN ID of the port will be changed to this VLAN ID, the port will be set as a member of the VLAN ID, and the port will be forced to enter VLAN unaware mode. After allocation, all traffic arriving at the port will be classified and switched to the VLAN ID assigned by RADIUS. If the (re)authentication fails or the RADIUS Access-Accept packet no longer carries the VLAN ID or is invalid, or the requester no longer exists on the port, the VLAN ID of the port will be restored to the original VLAN ID immediately (the administrator can Change in the case of RADIUS assignment. This option only applies to single client mode, that is •Port-based 802.1X • Single user 802.1X For troubleshooting of VLAN assignment, please use the "Monitoring→VLAN→VLAN Member and VLAN Port" page. These pages show which modules cover the current port VLAN configuration. RADIUS attributes used to identify VLAN IDs: RFC2868 and RFC3580 define the attributes of VLAN ID in Access-Accept packets. • Tunnel-Medium-Type, Tunnel-Type and Tunnel-Private-Group-ID must exist at least once in the attributes of the Access-Accept data packet. The switch looks for the first group of attributes that have the same tag value and meet the following requirements (if Tag is used as 0, Tunnel-Private-Group-ID does not need to contain Tag): -Tunnel-Medium-Type must be set to the value of "IEEE-802" (ordinal number 6). -Tunnel-Type must be set to "VLAN" (serial number 13). -Tunnel-Private-Group-ID must be an ASCII string in the range of "0"-"9",

	which is interpreted as a decimal string representing the VLAN ID. The final value range is 1-4095.
Guest VLAN enable	When the Guest VLAN is globally enabled and the designated port is enabled (selected), the switch will consider moving the port to the Guest VLAN according to the rules listed below. This option is only applicable to EAPOL-based modes, namely: •Port-based 802.1X •Single user 802.1X • Multi-user 802.1X For troubleshooting of VLAN assignment, please use the "Monitoring→VLAN→VLAN Member and VLAN Port" page. These pages show which modules cover the current port VLAN configuration. When the port link of the Guest VLAN is enabled, the switch starts to send EAPOL Request Identity (request identification) frames. If the number of transmissions of these frames exceeds the limit value (see "Maximum Request Identification Frames" in "System Configuration") and no EAPOL frames are received at the same time, the switch will consider entering the Guest VLAN. The transmission interval of the EAPOL request identification frame is configured using the "EAPOL timeout period" (see "System Configuration"). If the option "Receive EAPOL allowed to enter the Guest VLAN" option is enabled, the port will now enter the Guest VLAN. If the option is disabled, the switch will first check its history to see if EAPOL packets have been previously received on the port (if the port link is disconnected or the management status of the port has changed, this history is cleared), If the EAPOL packet has not been received, the port will be moved to the Guest VLAN. Otherwise, it will not move to the Guest VLAN, but will continue to send EAPOL request identification frames at the rate given by the "EAPOL timeout period". After entering the Guest VLAN, the port will be deemed to have been authenticated, and all connected clients on the port will be allowed to access this VLAN. When entering the Guest VLAN, the switch will not send an EAPOL Success frame. In the Guest VLAN, the switch will monitor the EAPOL packet of this link. If an EAPOL packet is received, the switch will immediately remove the port from the Guest VLAN and start to verify the requester according to the port mode. If you disable the "Receive EAPOL allowed to enter the Guest VLAN" option and receive an EAPOL packet, the port will never return to the Guest VLAN.
Port status	The current status of the port. Can take one of the following values: Disabled globally: NAS Disabled globally. Link Down: NAS is globally enabled, but the port has no link. Authorization: The port is in a mandatory authorization state or a single requester mode, and the authorized party is the authorized party. Unauthorized: The port is in a forced unauthorized state or single supplicant mode, and the RADIUS server has not successfully authorized the supplicant.

	X authorized / Y unauthorized: The port is in multi-supplicant mode. Currently, X clients have been authorized, and Y clients have not been authorized. Port-based 802.1X and single-user 802.1X belong to the single supplicant mode; multi-user 802.1X and MAC-based authentication belong to the multiple supplicant mode.
Reboot	There are two buttons in each row. These buttons are only enabled when the NAS is globally enabled and the management status of the port is in 802.1X-based mode or MAC-based authentication mode. Clicking these buttons will not cause the setting changes on the page to take effect. **Re-authentication:** Arrange re-authentication (based on 802.1X mode) whenever the quiet period of the port expires. For MAC-based authentication, re-authentication will be tried immediately. This button is only valid for clients that have successfully passed authentication on the port, and will not cause instantaneous unauthorized access to the client. **Reinitialization:** Force the reinitialization of the client on the port, thereby immediately re-authenticating. During the re-authentication process, the client will be transferred to an unauthorized state.

5.2.2.3 View NAS

In the [Navigation Bar] drop-down menu, select: Monitoring -> Security -> Network -> NAS, the two NAS display sub-menus will be expanded. Respectively "switch" and "port"

- Switch

Chart Figure 5-45 NAS switch status display

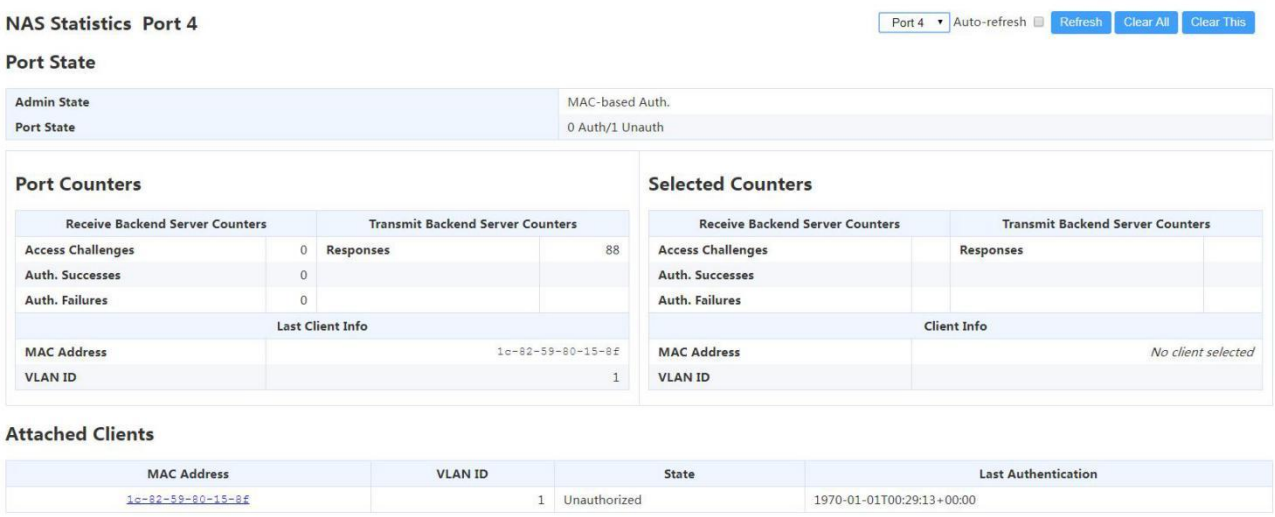
Item	Description
Port	Switch port number. Click to jump to the detailed NAS statistics of this port.
Management status	The current management status of the port. For details, please refer to the NAS configuration of the port.
Port status	For the current status of the port, please refer to the NAS configuration of the port for details.
Last source	For EAPOL-based authentication, it refers to the source MAC address carried in the most recently received EAPOL frame. For MAC-based authentication, it refers to the source MAC address carried in the latest frame received from a new client.
Last ID	For EAPOL-based authentication, it refers to the user name (requester

	identity) carried in the EAPOL frame in the most recently received response. For MAC-based authentication, it refers to the source MAC address of the latest frame received from a new client.
QOS classification	If "RADIUS specifies QOS" is enabled, the QoS class assigned to the port by the RADIUS server. If it is not assigned, it is displayed as "-".
VLAN Port	The VLAN ID that the NAS puts the port into. If the port VLAN ID is not covered by the NAS, this field is empty. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the Guest VLAN, "(Guest)" will be appended to the VLAN ID.

- Port

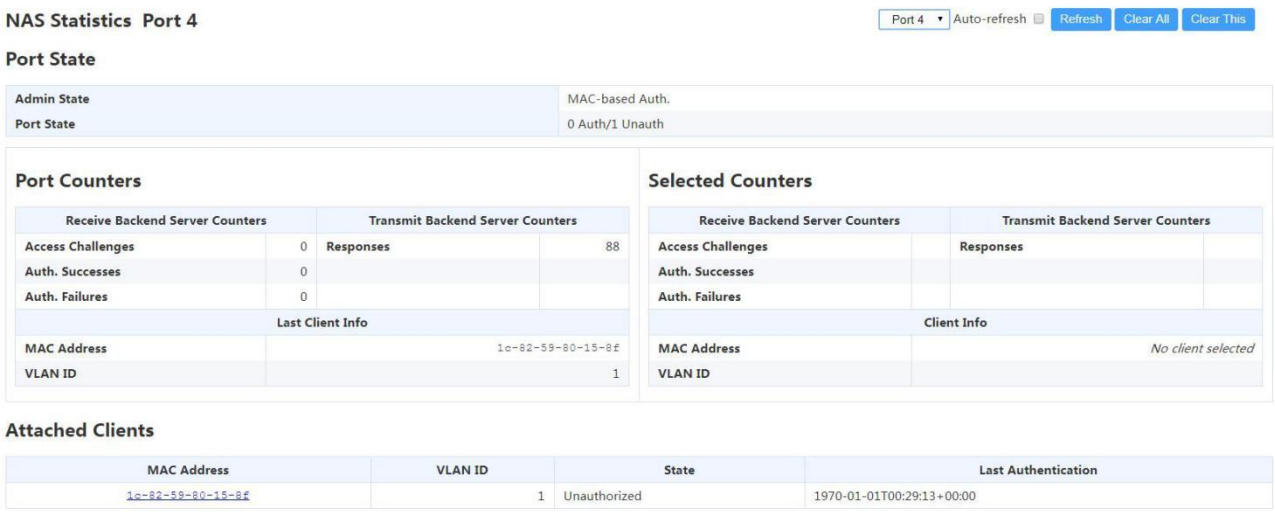
This page provides detailed NAS statistics for specific switch ports running EAPOL-based IEEE 802.1X authentication. For ports based on MAC authentication, it only displays statistics of the selected back-end server (RADIUS authentication server). Use the port selection box to select the port details to display. For different management states, the corresponding information displayed on the port is different. For single-user authentication modes, namely port-based 802.1X and single-user 802.1X, the display is divided into two parts:
Port status and port count.

Chart Figure 5-46 NAS port status and count display 1



For multi-user authentication mode, namely multi-user 802.1X and MAC-based authentication, the display is divided into four parts:
Port status, port count, selected count, and associated requester (for multi-user 802.1X) or associated client (for MAC-based authentication).

Chart Figure 5-47 NAS port status and count display 2



- Port status

  The information in this table is a subset of the information displayed in each row based on the port on the "Switch" page, and will not be described in detail.

- Port count

  Port count information is divided into three parts: EAPOL count, back-end server count and last requester information.

- EAPOL count

  EAPOL count can be used in the following management states:
  • Mandatory authorization
  • Mandatory unauthorized
  • Port-based 802.1X
  • Single user 802.1X
  • Multi-user 802.1X

EAPOL count			
Direction	**Name**	**IEEE name**	**Description**
RX	**Frame**	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that the switch has received.
RX	**Response ID**	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL response identification frames that the switch has received.
RX	**Response**	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames that the switch has received (except for response identification frames)
RX	**Start**	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames received by the switch.
RX	**Logoff**	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that the switch has received.
RX	**Invalid**	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames received by the switch that cannot identify the frame type.
RX	**Length Error**	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames received by the switch with invalid packet body length field.
TX	**Frames**	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type transmitted by the switch.
TX	**Request ID**	dot1xAuthEapolReqIdFramesTx	The number of EAPOL request identification frames transmitted by the switch.
TX	**Request count**	dot1xAuthEapolReqFramesTx	The number of valid EAPOL request frames sent by the switch (except request identification frames).

Count of back-end servers
The back-end server count can be used in the following management states:
• Port-based 802.1X
• Single user 802.1X
• Multi-user 802.1X
• MAC-based authentication

Backend server count			
Direction	**Name**	**IEEE name**	**Description**
RX	**Access Challege**	dot1xAuthBackendAccessChallenges	**Based on 802.1X:** Count the number of times the switch receives the first request from the backend server after the first response from the requester. Indicates that the back-end server communicates with the switch. **Based on MAC:** Calculate all access challenges received from the back-end server for this port (the leftmost table) or the client (the rightmost table).
RX	**Other Request**	dot1xAuthBackendOtherRequestsToSupplicant	**Based on 802.1X:** Count the number of times the switch sends EAP request packets to the requester after the first one. Indicates that the back-end server has selected the EAP method. **Based on MAC:** not applicable.
RX	**AuthenticateSuccess**	dot1xAuthBackendAuthSuccesses	**Based on 802.1X and MAC:** Count the number of successful indications received by the switch. Indicates that the requester/client has successfully passed the authentication
RX	**Authenticate fails**	dot1xAuthBackendAuthFails	**Based on 802.1X and MAC:** Count the number of failed messages received by the switch. This means that the requester/client has not yet authenticated to the back-end server.
TX	**Responses**	dot1xAuthBackendResponses	**Based on 802.1X:** Count the number of times the switch attempts to send the requester's first response packet to the back-end server. Indicates that the switch is trying to communicate with the back-end server. Possible retransmissions are not counted. **Based on MAC:** Calculate all back-end server data packets sent from the switch to the back-end server for a given port (leftmost table) or client (rightmost table). Possible retransmissions are not counted.

Last requester information (for 802.1X-based) or last customer information (for MAC-based authentication)

Information about the last requester/client that attempted to authenticate. This information applies to the following management states:

• Port-based 802.1X

• Single 802.1X

• Multiple 802.1X

• MAC-based authentication.

Last requester/customer information

Item	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last requester/client.
VLAN ID	-	The VLAN ID of the last frame that received the last requester/client
Version	dot1xAuthLastEapolFrameVersion	**Based on 802.1X:** The protocol version number carried in the recently received EAPOL frame. **Based on MAC:** not applicable.
ID	-	**Based on 802.1X:** The most recently received response identifies the username (requester ID) carried in the EAPOL frame. **Based on MAC:** not applicable.

Selected count

When the port is in one of the following management states, and the port status is not "unauthorized" (in "X authorized/Y unauthorized", you can see this table:

• Multi-user 802.1X

• MAC-based authentication

This table is the same as the port count table and is located next to it. If ID (for multi-user 802.1X) or MAC address (for MAC-based authentication) is not currently selected, the table will be empty. To fill in the form, select an ID or MAC address from the associated requestor/customer table.

Associate requester (multi-user 802.1X)/client (MAC-based authentication)

Item	Description
ID	Display the ID of the requester received in the response ID EAPOL frame. Clicking on the link will cause the requester's EAPOL and backend server counts to be displayed in the "Selected Counts" table. This column does not apply to MAC-based authentication.
MAC Address	For multi-user 802.1X, this column stores the MAC address of the associated requester. For MAC-based authentication, this column contains the MAC address of the connected client and forms a hyperlink. Clicking the link will cause the client's back-end server count to be displayed in the "Selected Count" table.
VLAN ID	This column contains the VLAN ID of the corresponding client currently protected by the port security module.
Status	The client can be "authorized" or "unauthorized". In the authorized state, the frame is allowed to be forwarded on the port, and in the unauthorized state, it will be blocked. As long as the back-end server does not successfully authenticate the client, it is unauthorized. If the authentication fails for some reason, the client will remain in an unauthorized state for several seconds (the specific time is determined by the "hold time" configured by the NAS system.
Last authentication	Shows the date and time (success and failure) of the last authentication.

Clear

Clear: This button is available in the following modes:

• Mandatory authorization

• Mandatory unauthorized
• Port-based 802.1X
• Single user 802.1X
Click to clear the count of the selected port.
Clear all: This button is available in the following modes:
• Multiple 802.1X
• MAC-based Auth.X
Click to clear the port counter and all connected client counters. However, "Last Request/Customer Information" will not be cleared.
Clear current: this button is available in the following modes:
• Multiple 802.1X
• MAC-based Auth.X
Click to clear only the currently selected requestor or client count, that is, "selected count".

5.2.2.4 CLI reference commands

Command	switch(config)# dot1x system-auth-control switch(config)# no dot1x system-auth-control switch(config)# dot1x re-authentication switch(config)# no dot1x re-authentication
Description	Turn on the NAS function; Turn off the NAS function; Enable NAS re-authentication; Turn off NAS re-authentication;

Command	switch(config)# dot1x authentication timer re-authenticate 3600 switch(config)# dot1x timeout tx-period 30 switch(config)# dot1x authentication timer inactivity 300 switch(config)# dot1x timeout quiet-period 11
Description	Configure the NAS re-authentication period; Configure NAS EAPOL timeout time; Configure the NAS aging cycle; Configure NAS EAPOL timeout retention time;

Command	switch(config)# dot1x feature radius-qos switch(config)# no dot1x feature radius-qos switch(config)# dot1x feature radius-vlan switch(config)# no dot1x feature radius-vlan
Description	Enable NAS RADIUS to specify QoS enable; Disable NAS RADIUS designated QoS enable; Enable NAS RADIUS designated VLAN enable; Disable NAS RADIUS designated VLAN enable;

Command	switch(config)# dot1x feature guest-vlan

	switch(config)# no dot1x feature guest-vlan switch(config)# dot1x guest-vlan 2 switch(config)# dot1x max-reauth-req 3 switch(config)# dot1x guest-vlan supplicant switch(config)# no dot1x guest-vlan supplicant
Description	Enable NAS Guest VLAN enable; Disable NAS Guest VLAN enable; Configure NAS Guest VLAN ID; Configure the maximum number of NAS request identification frames; Turn on the NAS and receive EAPOL permission to enter the Guest VLAN; Turn off the NAS and receive EAPOL to allow entry into the Guest VLAN;

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# dot1x port-control force-authorized switch(config-if)# dot1x port-control force-unauthorized switch(config-if)# dot1x port-control auto switch(config-if)# dot1x port-control single switch(config-if)# dot1x port-control multi switch(config-if)# dot1x port-control mac-based switch(config-if)# dot1x radius-qos switch(config-if)# dot1x radius-vlan switch(config-if)# dot1x guest-vlan
Description	Configure mandatory port authorization; Configure the port to force unauthorized; Configure the port based on port 802.1X; The configuration port is based on single-user 802.1X; The configuration port is based on multi-user 802.1X; Configure port MAC-based authentication; Configure port RADIUS to specify QoS enable; Configure port RADIUS to specify VLAN enable; Configure port Guest VLAN enable;

Command	switch# show dot1x status switch# show dot1x statistics all
Description	Print NAS status; Print NAS port statistics;

5.2.3 ACL

ACLs (Access Control Lists), also known as access lists (Access Lists), are commonly known as firewalls. It controls the data packets on the network device interface by defining some rules.

The device supports port-based ACL and flow-based ACL. Port-based ACLs are effective for all inbound packets on the port; flow-based ACLs are only effective for packets that match user configuration rules. For hit packets, the following action strategies are supported.

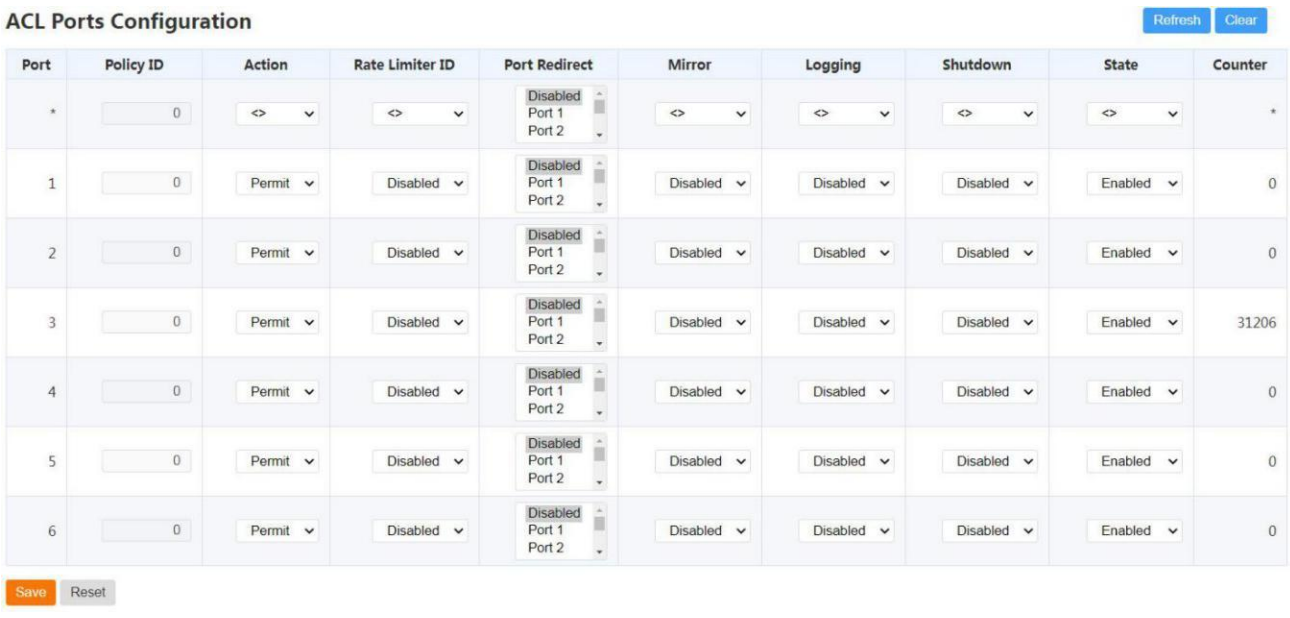
- Permit/deny: select release or discard
- Speed limit: The device supports the global configuration of 16 speed limit policies, and the port or flow-based ACL associates the policy ID to achieve speed limit
- Mirroring: send the hit message to the CPU
- Log: When the port receives a message, the system log is generated. The log generation itself is rate-limited, so it may not generate a log for every hit message
- Disable: shut down the port, close the port MAC address learning, discard all ingress packets
- Redirection: redirect the ingress message directly to a specific port for output

5.2.3.1 Configure ACL

- Port

In the [Navigation Bar] drop-down menu, select: Configuration->Security->Network->ACL->Port to enter the configuration interface.

Chart Figure 5-48 ACL port configuration



Item	Description
Port	Panel port number
Strategy ID	Maintain
Behavior	Choose release and discard. This behavior is equivalent to the default behavior of the specified port, and is generally used in conjunction with an access control list.
Speed limit ID	Disable or 1-16 rate limit ID, valid when the behavior is permit, the default is Disabled
Port redirection	Packets are redirected to other ports, valid when the behavior is permit, and the default is Disabled
Mirror image	Enable switch, closed by default
Log	
Disable	
status	When the port shutdown occurs when the ACL is disabled and enabled, configure Enabled to restore the port. You can also manually specify its shutdown, that is, configure it as Disable.
Statistics	Statistics on the number of hit packets on the port

■ Speed limit

In the [Navigation Bar] drop-down menu, select: Configuration->Security->Network->ACL->Speed Limit to enter the configuration interface.

Chart Figure 5-49 ACL rate limit configuration

Item	Description

Speed limit ID	Range 1-16, support 16 speed limit strategies
Speed rate	Range: 0-3276700 pps or 0, 100, 200, …, 1000000 kbps
Unit	Support two units of pps and kbps

- Access control list

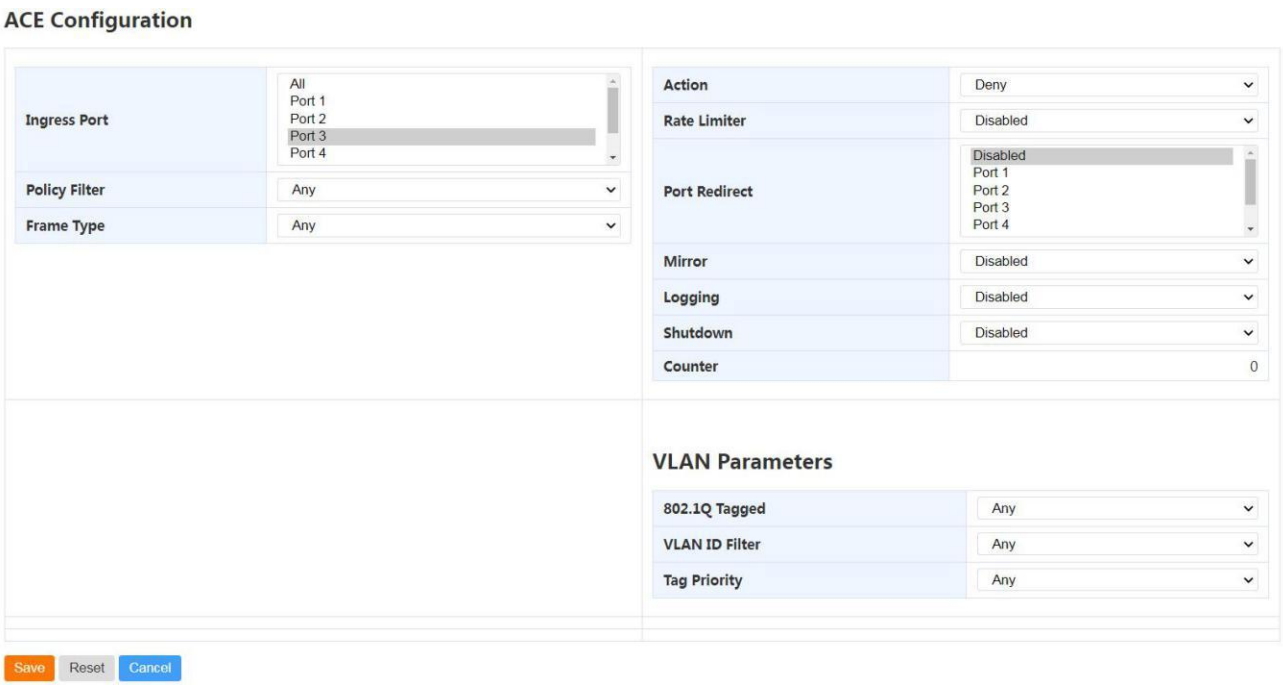
In the [Navigation Bar] drop-down menu, select: Configuration->Security->Network->ACL->Access Control List to enter the configuration interface.

Chart Figure 5-50 Access Control List Configuration

Display brief information of ACE, support ACE table entry up and down movement, add before, add after, delete, edit operations.

Click the Add button to enter the ACE creation interface.

Chart Figure 5-51 ACE entry information



Item	Subtopic	Details of Subtopic	Description
Access port	-	-	Support to match all ports or only a single panel port
Policy filtering	-	-	Keep
Policy filtering Frame type	Any	-	Hit all messages
	Ethernet Type	SMAC	Any: Hit all SMACs Specific: Hit a specific SMAC
		DMAC	Any: Hit all DMACs BC: Hit all broadcast packets

			MC: Hit all multicast packets UC: Hit all unicast packets Specific: Hit a specific DMAC
		Etype	Any: Hit all Etypes Specific: Hit a specific Etype
	ARP	SMAC	Any: Hit all SMACs Specific: Hit a specific SMAC
		DMAC	Any: Hit all DMACs BC: Hit all broadcast packets MC: Hit all multicast packets UC: Hit all unicast packets
		ARP/ARPA	Any: Hit all op codes ARP: op code that hits ARP RARP: the op code that hits RARP Other: hit non-ARP/RARP op code
		Request/response	Any: Hit all op codes Request: the op code that hits the ARP/RARP request Reply: hit the op code of ARP/RARP reply
		Send IP filtering	Any: Hit all IP addresses Host: Hit a specific IP address Network: Specific IP network segment after hit
		Target IP filtering	Any: Hit all IP addresses Host: Hit a specific IP address Network: Specific IP network segment after hit
		ARP send MAC hit	Any: hit all 0: The sender's hardware address is not equal to SMAC 1: The sender's hardware address is equal to SMAC
		RARP target MAC hit	Any: hit all 0: The target hardware address is not equal to the DMAC 1: The target hardware address is equal to the DMAC
		IP/Ethernet length	Any: hit all 0: The length of the hardware address is not equal to 6 or the length of the protocol address is not equal to 4 1: Hardware address length etc. 6 and protocol address length etc. 4
		IP	Any: hit all 0: The hardware type is not 1

			1: The hardware type is 1
		Ethernet	Any: hit all 0: Protocol types are not equal 0x0800 1: Protocol type, etc. 0x0800
	IPv4	DMAC	Any: Hit all DMACs BC: Hit all broadcast packets MC: Hit all multicast packets UC: Hit all unicast packets
		IP Protocol filtering	Any: hit all ICMP: ICMP protocol message UDP: UCP protocol packet TCP: TCP protocol message Other: other protocol packets
		IP TTL	Any: hit all None-Zero: TTL is not equal to 0 Zero: TTL etc. 0
		IP fragmentation	Any: hit all Yes: Fragmented packets are hit No: hits a non-fragmented packet
		IP Option	Any: hit all Yes: Hit the packet with the option flag bit set No: hits a packet with no option flag set
		SIP filtering	Any: Hit all IP addresses Host: Hit a specific IP address Network: Specific IP network segment after hit
		DIP filtering	Any: Hit all IP addresses Host: Hit a specific IP address Network: Specific IP network segment after hit
	IPv6	DMAC	Any: Hit all DMACs BC: Hit all broadcast packets MC: Hit all multicast packets UC: Hit all unicast packets
		Next head filter	Any: hit all ICMP: ICMP protocol message UDP: UCP protocol packet TCP: TCP protocol message Other: other protocol packets
		SIP filtering	Any: hit all Specific: Hit a specific SIP message
		Hop limit	Any: hit all 0: packets with hop as 0 are hit 1: The packet that hits hop is non-zero
VLAN	802.1Q Tagged	-	Any: matches all packets

parameters			Disabled: matching Untagged packets Enabled: matching tagged packets
	VLAN ID filtering	-	Any: all vlan Specific: Specific VLAN ID
	Tag priority	-	Any: all priority values Other: a specific value or range
Behavior/speed limit/mirror/log/disable/count	-	-	The specific actions are the same as port-based ACL

5.2.3.2 View ACL status

In the [Navigation Bar] drop-down menu, select: Monitoring->Security->Network->ACL Status to enter the view interface.

Chart Figure 5-52 ACL status information

Display brief information of ACE, including brief information configuration information of matching items, behaviors, and status information such as current packet hits and conflicts.

5.2.3.3 Typical ACL configuration examples

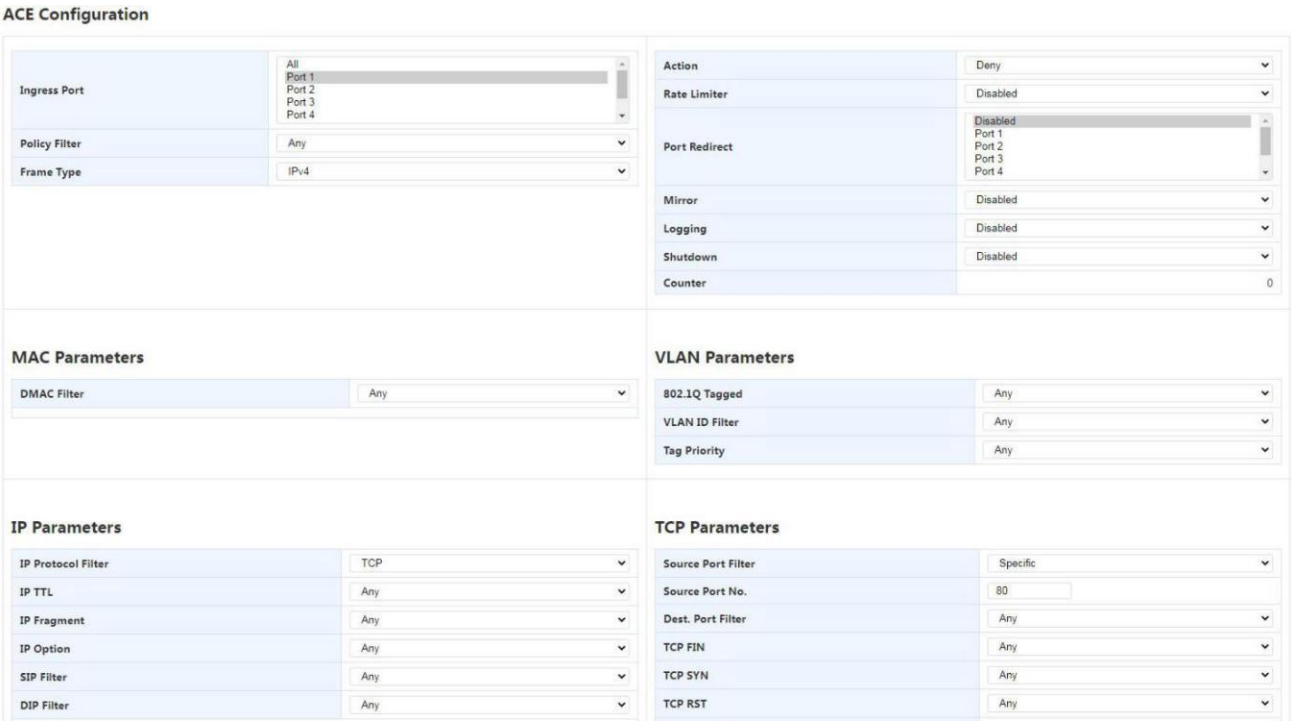
- Case requirements

Apply the ACL function to port 8 to prohibit TCP packets with the port source port number of 80 from passing.

- Operation Step

Create ACE in the access control list configuration interface, select 1 for access port; select IPv4 for frame type; select TCP for IP protocol filtering; select Specific for source port filtering, source port number 80; select Deny for behavior.

Chart Figure 5-53 ACL case configuration



After the configuration is complete, you can see the ACL status on the viewing interface:
Chart Figure 5-54 ACL case status

5.2.3.4 CLI reference commands

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# access-list action permit switch(config-if)# access-list action deny switch(config-if)# access-list rate-limiter 1 switch(config-if)# no access-list rate-limiter switch(config-if)# access-list redirect interface GigabitEthernet 1/2 switch(config-if)# access-list mirror switch(config-if)# no access-list mirror switch(config-if)# access-list logging switch(config-if)# no access-list logging switch(config-if)# access-list shutdown switch(config-if)# no access-list shutdown switch(config-if)# access-list port-state switch(config-if)# no access-list port-state

Description	Configure port ACL behavior as permit; Configure port ACL behavior to deny; Configure port ACL association limit ID; Configure port ACL to disable rate limit; Configure port ACL redirection port; Configure port ACL mirroring enable; Configure port ACL mirroring off; Configure port ACL log enable; Configure port ACL log to close; Configure port ACL to disable port enable; Configure port ACL to disable port closure; Configure port ACL port status enable; Configure port ACL port status is closed;

Command	switch(config)# access-list rate-limiter 1 pps 20 switch(config)# access-list rate-limiter 1 100kbps 100 switch(config)# no access-list rate-limiter 1
Description	Configure ACL to limit the rate based on the number of packets, in pps; Configure ACL to limit the rate based on traffic, the unit is 100kbps; Restore the ACL default rate limit;

Command	switch(config)# access-list ace 1 ingress interface GigabitEthernet 1/1-3 frame-type ipv4 sip 1.1.1.0/24 action deny switch(config)# access-list ace 2 next 1 ingress interface GigabitEthernet 1/1 frame-type ipv4 sip 1.1.1.1/24 switch(config)# no access-list ace 1
Description	Configure ACL access control list configuration 1, which acts on ports 1-3 ingress and filters packets whose source IP is 1.1.1.0/24 network; Configure ACL access control list configuration 2, which acts on the entrance of port 1 and allows packets with the source IP of 1.1.1.1 to be released. Its priority is higher than access control list configuration 1; Delete ACL access control list configuration 1;

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# dot1x port-control force-authorized switch(config-if)# dot1x port-control force-unauthorized switch(config-if)# dot1x port-control auto switch(config-if)# dot1x port-control single switch(config-if)# dot1x port-control multi switch(config-if)# dot1x port-control mac-based switch(config-if)# dot1x radius-qos switch(config-if)# dot1x radius-vlan switch(config-if)# dot1x guest-vlan

Description	Configure mandatory port authorization; Configure the port to force unauthorized; Configure the port based on port 802.1X; The configuration port is based on single-user 802.1X; The configuration port is based on multi-user 802.1X; Configure port MAC-based authentication; Configure port RADIUS to specify QoS enable; Configure port RADIUS to specify VLAN enable; Configure port Guest VLAN enable;

Command	switch# show access-list interface * switch# show access-list rate-limiter switch# show access-list ace statistics
Description	Print ACL port configuration and hit packet count; Print ACL rate limit configuration; Print ACL access control list configuration and hit packet count;

5.2.4 IP Source Guard

The IP Source Guard function is used to control the access of IP packets, and verify the input IP packets through the port + VLAN ID + MAC + IP quadruple. If there is no corresponding entry in the IP Source Guard table, The message is discarded. The entries in the IP Source Guard table can be dynamic entries, derived from the DHCP Snooping table; it can also be statically configured.

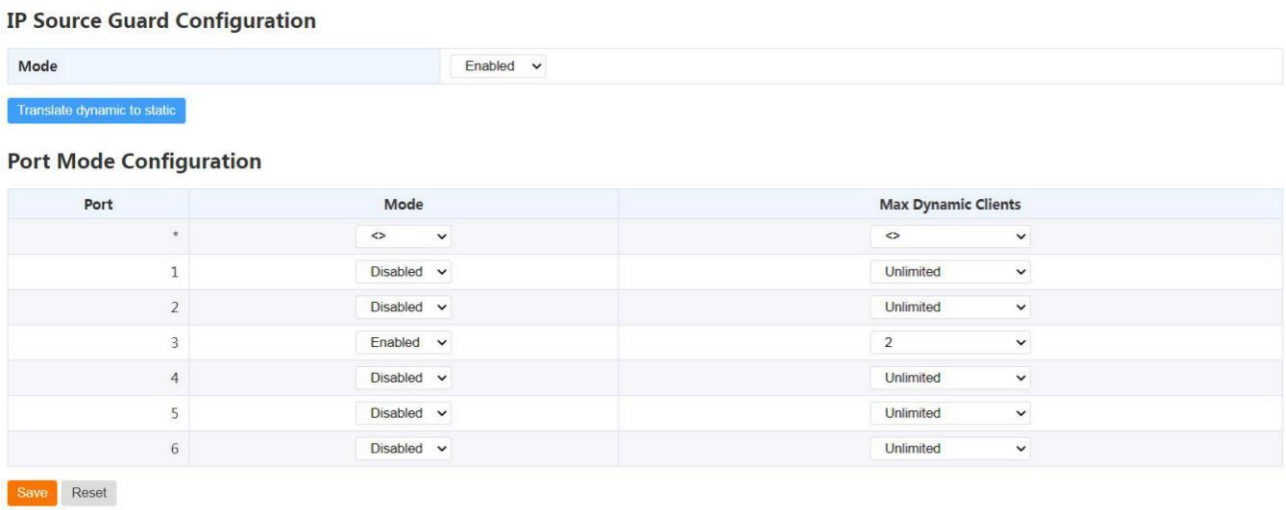
Quadruple extraction of the message:

- Port: refers to the source port (panel port) of the switch input.
- VLAN ID: VLAN ID assigned after the packet enters the switch.
- MAC: The source MAC address of the message.
- IP: The source IP address of the message.

5.2.4.1 Configure IP Source Guard

In the [Navigation Bar] drop-down menu, select: Configuration->Security->Network->IP Source Guard->Configuration to enter the configuration page.

Chart Figure 5-55 IP Source Guard configuration



- Global mode

  The global mode is disabled by default. As long as the mode is disabled, the IP Source Guard function is available.
- Dynamic to static

  As long as you click this button, the existing IP Source Guard dynamic entries will be converted to static entries. The source of the dynamic entries is the DHCP snooping table. If the entries in the DHCP Snooping table are deleted (such as lease expiration, power-off aging, etc.), the dynamic entries of IP Source Guard will also be deleted, but the static entries will remain unchanged. Exist, unless deleted manually.
- Port mode
  - Mode: Specify which ports IP Source Guard is enabled on. IP Source Guard will be enabled on this given port only when both the global mode and the corresponding port mode are enabled.
  - Maximum number of dynamic clients: Specify the maximum number of dynamic clients that can be learned on the corresponding port. The value can be 0, 1, 2, or unlimited. If the port mode is enabled and the value is 0, it means that only IP packets that match in the static entry on the corresponding port are allowed to be forwarded.

• Since the dynamic entries of the IP Source Guard function come from the DHCP Snooping table, it is necessary to ensure that the DHCP Snooping configuration is enabled and the correct DHCP Snooping trusted port is set.

5.2.4.2 Configure static table

In the [Navigation Bar] drop-down menu, select: Configuration->Security->Network->IP Source Guard->Static Table to enter the configuration page.

Chart Figure 5-56 Static IP Source Guard table configuration

Configure the four-tuple of IP Source Guard static entries. The IP address uses dotted decimal notation (A.B.C.D), and the MAC address supports two formats. XX-XX-XX-XX-XX-XX or XX:XX:XX:XX:XX:XX.

- Delete: After checking, delete the corresponding entry in the next save.
- Add new entry: Click to add a new entry.

5.2.4.3 Show dynamic table

In the [Navigation Bar] drop-down menu, select: Monitoring -> Security -> Network -> IP Source Guard, enter the display page.

Chart Figure 5-57 Dynamic IP Source Guard table display

Displays the four-tuple of IP Source Guard dynamic entries. If a dynamic entry is converted to a static entry, the corresponding entry will no longer be displayed on this page.

5.2.4.4 CLI Reference command

Command	switch(config)# ip verify source switch(config)# no ip verify source
Description	Configure IP Source Guard to be turned on globally; Configure IP Source Guard to close globally;

Command	switch(config)# ip verify source translate
Description	Configure IP Source Guard to convert all dynamic addresses to static addresses;

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# ip verify source switch(config-if)# no ip verify source switch(config-if)# ip verify source limit 2
Description	Configure the IP Source Guard port to open; Configure the IP Source Guard port to close; Configure the maximum number of dynamic clients on the IP Source Guard

	port;

Command	switch(config)# ip source binding interface GigabitEthernet 1/6 6 192.168.6.34 f4-93-9f-f3-4f-ef switch(config)# no ip source binding interface GigabitEthernet 1/6 6 192.168.6.34 f4-93-9f-f3-4f-ef
Description	Add IP Source Guard static table entries; Delete IP Source Guard static entries;

Command	switch# show ip verify source switch# show ip source binding static switch# show ip source binding dhcp-snooping
Description	Print IP Source Guard global configuration and port configuration; Print IP Source Guard static entries; Print IP Source Guard dynamic entries;

5.2.5 ARP Inspection

The ARP Inspection function is used to control the access of ARP packets, and verify the input ARP packets through the port+VLAN ID+MAC+IP quadruple. If there is no corresponding entry in the ARP Inspection table, the report The text is discarded. The entries in the ARP Inspection table can be dynamic entries, derived from the DHCP Snooping table; it can also be statically configured.

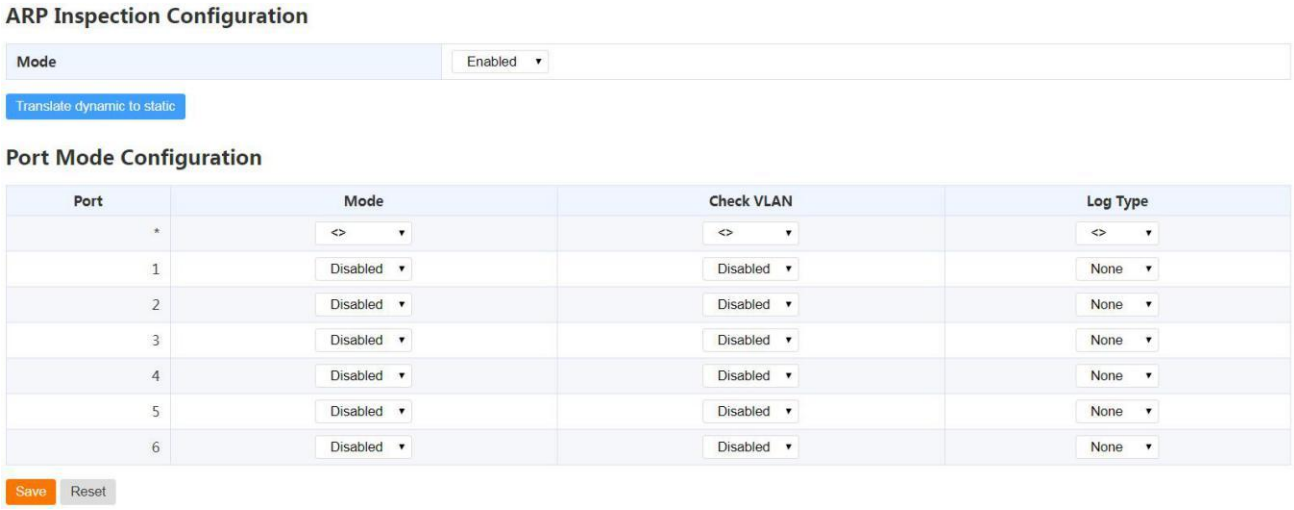
Quadruple extraction of the message:

- Port: refers to the source port (panel port) when ARP packets are input to the switch.
- VLAN ID: refers to the VLAN ID assigned by the ARP packet entering the switch.
- MAC: Refers to the Sender MAC address of the ARP packet.
- IP: Refers to the Sender IP address of the ARP packet.

5.2.5.1 Configure the port

In the [Navigation Bar] drop-down menu, select: Configuration->Security->Network->ARP Inspection->Port Configuration to enter the configuration page.

Chart Figure 5-58 ARP Inspection configuration



- Global mode

  The global mode is disabled by default, as long as the mode is disabled, the ARP Inspection function is not enabled.
- Dynamic to static

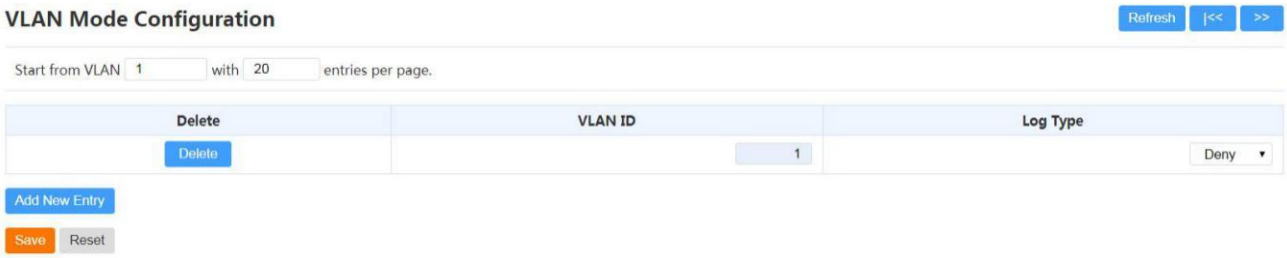
  As long as you click this button, the existing dynamic ARP Inspection entries will be converted into static entries. The source of dynamic entries is the DHCP snooping table. If the entries in the DHCP Snooping table are deleted (such as lease expiration, device power-off, etc.), the dynamic entries of ARP Inspection will also be deleted, but the static entries will always exist , Unless deleted manually.
- Port mode

  - Mode: Specify which ports IP Source Guard is enabled on. ARP Inspection will be enabled on this given port only when both the global mode and the corresponding port mode are enabled. The default port mode is disabled.
  - Check VLAN: If you want to check the VLAN configuration, you must enable the "Check VLAN" setting. By default, "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the Log type of ARP Inspection will refer to the port setting. After enabling the "Check VLAN" setting, the Log type of ARP Inspection will refer to the VLAN setting.
  - Log type: Only when the global mode is enabled, the corresponding port mode is also enabled, and the VLAN is disabled, the Log type will refer to the port settings. There are four types of Log, the possible types are:

    None: Nothing is recorded.
    Deny: Log is triggered by filtered ARP packets.
    Permit: Allowed ARP packets trigger Log.
    ALL: All ARP packets trigger Log.

5.2.5.2 Configure VLAN

In the [Navigation Bar] drop-down menu, select: Configuration->Security->Network->ARP Inspection->VLAN Configuration to enter the configuration page.
Chart Figure 5-59 ARP Inspection VLAN configuration



The Log type is the same as the Log type configured on the port. When the "Check VLAN" of the corresponding port is enabled in the port configuration, the corresponding Log type will refer to the VLAN setting.

- Delete: After checking, delete the corresponding entry in the next save.
- Add new entry: Click to add a new entry.

5.2.5.3 Configure static table

In the [Navigation Bar] drop-down menu, select: Configuration->Security->Network->ARP Inspection->Static Table to enter the configuration page.

Chart Figure 5-60 ARP Inspection static table configuration

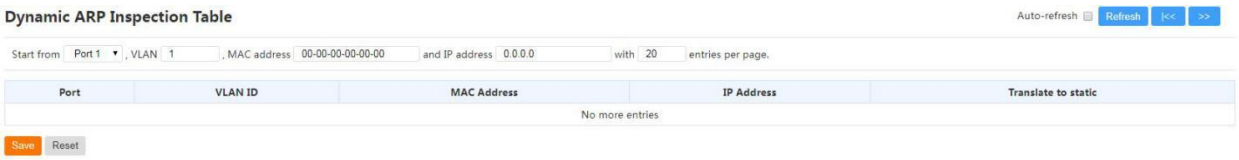
Configure the four-tuple of ARP Inspeciton static entries. The IP address uses dotted decimal notation (A.B.C.D), and the MAC address supports two formats. XX-XX-XX-XX-XX-XX or XX:XX:XX:XX:XX:XX.

- Delete: After checking, delete the corresponding entry in the next save.
- Add new entry: Click to add a new entry.

5.2.5.4 Configure dynamic table

In the [Navigation Bar] drop-down menu, select: Configuration->Security->Network->ARP Inspection->Dynamic Table to enter the configuration page.

Chart Figure 5-61 ARP Inspection dynamic table configuration



This page can only be configured with "Convert to static", which is used to convert a dynamic entry to static. If a dynamic entry is converted to a static entry, the corresponding entry will no longer be displayed on this page.

5.2.5.5 Display dynamic table

In the [Navigation Bar] drop-down menu, select: Monitoring->Security->Network->ARP Inspection->Dynamic Table to enter the display page.

Chart Figure 5-62 ARP Inspection dynamic table display

Display the four-tuple information of ARP Inspection dynamic entries. If a dynamic entry is converted to a static entry, the corresponding entry will no longer be displayed on this page.

5.2.5.6 CLI Reference command

Command	switch(config)# ip arp inspection switch(config)# no ip arp inspection
Description	Configure ARP Inspeciton to be turned on globally; Configure ARP Inspeciton to close globally;

Command	switch(config)# ip arp inspection translate switch(config)# ip arp inspection translate interface GigabitEthernet 1/6 6 00-00-00-11-22-33 1.2.3.4
Description	Configure all dynamic addresses of ARP Inspeciton to convert to static addresses; Configure the dynamic address to static address specified by ARP Inspeciton;

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# ip arp inspection switch(config-if)# no ip arp inspection switch(config-if)# ip arp inspection check-vlan switch(config-if)# no ip arp inspection check-vlan switch(config-if)# ip arp inspection logging deny
Description	Configure the ARP Inspeciton port to open; Configure the ARP Inspeciton port to close; Configure the ARP Inspeciton port to check the VLAN is enabled; Configure the ARP Inspeciton port to check that the VLAN is closed; Configure the LOG type of the ARP Inspeciton port;

Command	switch(config)# ip arp inspection vlan 10 switch(config)# ip arp inspection vlan 10 logging all switch(config)# no ip arp inspection vlan 10
Description	Add ARP Inspeciton VLAN mode configuration; Configure the LOG type of ARP Inspeciton VLAN mode; Delete the ARP Inspeciton VLAN mode configuration;

Command	switch(config)# ip arp inspection entry interface GigabitEthernet 1/6 6 00-00-00-

	11-22-33 1.2.3.4 switch(config)# no ip arp inspection entry interface GigabitEthernet 1/6 6 00-00-00-11-22-33 1.2.3.4
Description	Add ARP Inspeciton static table entry; Delete the ARP Inspeciton static table entry;

Command	switch# show ip arp inspection switch# show ip arp inspection entry static switch# show ip arp inspection entry dhcp-snooping switch# show ip arp inspection vlan 10
Description	Print ARP Inspeciton global configuration and port configuration; Print ARP Inspeciton static entries; Print ARP Inspeciton dynamic table entries; Print ARP Inspeciton VLAN mode configuration;

5.3 AAA

5.3.1 RADIUS

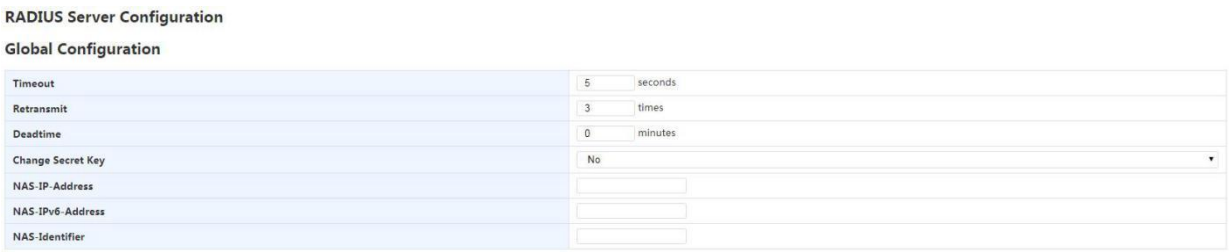
5.3.1.1 RADIUS Configuration

In the [Navigation Bar] drop-down menu, select: Configuration->Security->AAA->RADIUS to enter the configuration interface.

- Global configuration

Global configuration items are common to all RADIUS servers.

Chart Figure 5-63 RADIUS Global Configuration



Item	Description
Overtime time	The number of seconds to wait for a reply from the RADIUS server before resending the request. The range is 1 to 1000.
Number of retransmissions	The number of times to resend a RADIUS request to a server that did not respond. The range is 1 to 1000. If the server did not respond after the last retransmission, it is considered dead.
Dead time	It can be set to a number between 0 and 1440 minutes, during which time the switch will not send a new request to the server that fails to respond to the previous request. When multiple servers are configured, if the dead time is set to a value greater than 0, it can prevent the switch from constantly trying to contact the server that has been determined to be dead.

Modify key	Specify whether to change the key. If you select "Yes" for this option, you can change the key and share it between the RADIUS server and the switch.
Key	The specific key to be modified, up to 63 characters. After saving, the content of this field cannot be displayed.
NAS IP address	The IPv4 address used as attribute 4 in the RADIUS Access-Request packet. If this field is left blank, the IP address of the outgoing interface is used.
NAS logo	Identifier-up to 253 characters-is used as attribute 32 in the RADIUS Access-Request packet. If this field is left blank, the NAS-Identifier is not included in the data packet.

- Server configuration

You can add up to 5 servers.

Chart Figure 5-64 RADIUS server configuration

Item	Description
Delete	To delete the RADIUS server entry, check this box. The entry will be deleted during the next save.
Host name (IP address)	The IPv4 address of the RADIUS server.
Authentication port	The UDP port used for authentication on the RADIUS server. Set to 0 to disable authentication.
Accounting port	The UDP port used for accounting on the RADIUS server. Set to 0 to disable accounting.
Overtime time	This optional setting will override the timeout period set globally. Leave it blank to use the globally set timeout period.
Number of retransmissions	This optional setting will override the global setting of the number of restarts. Leave it blank to use the globally set number of retransmissions.
Modify key	Specify whether to change the key. After selecting the check box, you can change the key to override the global setting. Leave it blank to use the global key.
Add new server button	To add a new RADIUS server. A blank line has been added to the table, and the RADIUS server can be configured as required. Supports up to 5 servers.
Delete button	After clicking the Add New Server button, it exists when it has not been saved, click to cancel the new server just added.

5.3.1.2 View RADIUS

In the [Navigation Bar] drop-down menu, select: Monitoring -> Security -> AAA, two display sub-menus will be expanded. They are "RADIUS Overview" and "RADIUS Details".

- RADIUS overview

Chart Figure 5-65 RADIUS status overview

Item	Description
#	RADIUS server number. Click to navigate to detailed statistics for this server.
IP address	The IP address of the server.
Authentication port	The UDP port number used by the server for authentication.
Certification status	The current status of the server's authentication function. This field takes one of the following values: Disabled: The server is disabled. Not ready: The server is enabled, but IP communication has not been started and is running. Ready: The server is enabled, IP communication is up and running, and RADIUS is ready to accept access attempts. Zombie (X seconds remaining): An attempt has been made to access this server, but no reply was made within the configured timeout period. The server has been temporarily disabled, but will be re-enabled after the "dead time" expires. The number of seconds remaining before this is shown in parentheses. This state can only be accessed when multiple servers are enabled.
Accounting port	The UDP port number used by the server for accounting.
Accounting status	The current status of the server's accounting function. This field takes one of the following values: Disabled: The server is disabled. Not ready: The server is enabled, but IP communication has not been started and is running. Ready: The server is enabled, IP communication is up and running, and RADIUS is ready to accept access attempts. Zombie (X seconds remaining): An attempt has been made to access this server, but no reply was made within the configured timeout period. The server has been temporarily disabled, but will be re-enabled after the "dead time" expires. The number of seconds remaining before this is shown in parentheses. This state can only be entered when multiple servers are enabled.

- RADIUS status details

Chart Figure 5-66 RADIUS status details

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

Use the following checkboxes to switch between different servers.

- RADIUS authentication statistics 0
  - Counter

Direction	Name	RFC4668 Name	Description
RX	**Access accepted**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
RX	**Access denied**	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
RX	**Visit Challenge**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
RX	**Malformed access response**	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS access response packets received from the server. Malformed data packets include data packets of invalid length. The wrong authenticator or Message Authenticator attribute or unknown type is not included in the malformed access response.
RX	**Illegal authenticator**	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticator or Message Authenticator attributes received from the server.
RX	**Unknown type**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets of unknown type received from the server on the authentication port and discarded.
RX	**Discard message**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets received from the server on the authentication port and discarded for some other reason.
TX	**Access**	radiusAuthClientExtAccessRequests	Number of RADIUS Access-Request

	request		packets sent to the server. This does not include retransmission.
TX	**Access retransmission**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets resent to the RADIUS authentication server.
TX	**Pending request**	radiusAuthClientExtPendingRequests	The number of RADIUS access request packets sent to the server has not timed out or received a response. This variable is incremented when the access request is sent and reduced due to receiving access acceptance, access-rejection, access-challenge, timeout or retransmission.
TX	**Time out**	radiusAuthClientExtTimeouts	The number of server authentication timeouts. After the timeout, the client may retry to the same server, send to another server or give up. Retries to the same server are counted as retransmissions and timeouts. The counts sent to other servers are considered requests and timed out.

✧ Other information

Name	RFC4668 Name	Description
IP address	-	The IP address and UDP port of the authentication server in question.
Status	-	Display the status of the server. It takes one of the following values: Disable: Disable the selected server. Not ready: The server is enabled, but IP communication has not been started and is running. Ready: The server is enabled, IP communication is up and running, and RADIUS is ready to accept access attempts. Zombie (X seconds remaining): An access attempt has been made to this server, but no reply was made within the configured timeout. The server has been temporarily disabled, but will be re-enabled after the dead time expires. The number of seconds remaining before this is shown in parentheses. This state can only be entered when multiple servers are enabled.
Round-Trip time	radiusAuthClientExtRoundTripTime	The time interval (in milliseconds) between the most recent Access-Reply / Access-Challenge and the matching Access-Request from the RADIUS authentication server. The granularity of this measurement is 100 milliseconds. If it is 0 milliseconds, it means that there is no round-trip communication with the server.

➢ RADIUS Accounting statistics

✧ Counter

Direction	Name	RFC4670 Name	Description
RX	**Answer**	radiusAccClientExtResponses	Number of RADIUS packets received from the server (valid or invalid)
RX	**Malformed response**	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed data packets include data packets of invalid length. The wrong authenticator or unknown type is not included in the malformed response.

RX	**Illegal authenticator**	radiusAcctClientExtBadAuthenticators	Contains the number of invalid authentication RADIUS packets received from the server.
RX	**Unknown type**	radiusAccClientExtUnknownTypes	The number of unknown RADIUS packets received from the server on the accounting port.
RX	**Discard message**	radiusAccClientExtPacketsDropped	The number of RADIUS packets received from the server on the accounting port, which were discarded for some other reason.
TX	**Request**	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmission.
TX	**Retransmission**	radiusAccClientExtRetransmissions	The number of RADIUS packets resent to the RADIUS accounting server.
TX	**Pending**	radiusAccClientExtPendingRequests	The number of RADIUS packets sent to the server has not timed out or a response has been received. This variable is incremented when a request is sent and decremented due to receiving a response, timeout, or retransmission.
TX	**Time out**	radiusAccClientExtTimeouts	The number of server accounting timeouts. After the timeout, the client may retry to the same server, send to another server or give up. Retries to the same server are counted as retransmissions and timeouts. The counts sent to other servers are considered requests and timed out.

✧ Other information

It is similar to other information of RADIUS authentication statistics and will not be described in detail.

➢ Clear: Clear the counter of the selected server. This operation does not clear the "pending request" counter.

5.3.1.3 CLI reference commands

Command	switch(config)# radius-server timeout 5 switch(config)# radius-server retransmit 3 switch(config)# radius-server deadtime 1 switch(config)# radius-server key password switch(config)# radius-server attribute 4 192.168.1.3 switch(config)# radius-server attribute 95 4ff1:3301 switch(config)# radius-server attribute 32 server
Description	Configure the RADIUS timeout period; Configure the number of RADIUS retransmissions; Configure RADIUS dead time; Configure the RADIUS secret key; Configure the RADIUS NAS IPv4 address; Configure the RADIUS NAS IPv6 address; Configure RADIUS NAS identity;

Command	switch(config)# radius-server host 192.168.1.10 auth-port 1812 acct-port 1813 timeout 10 retransmit 3 key password

	switch(config)# no radius-server host 192.168.1.10 auth-port 1812 acct-port 1813 timeout 10 retransmit 3 key password
Description	Add RADIUS server; Delete the RADIUS server;

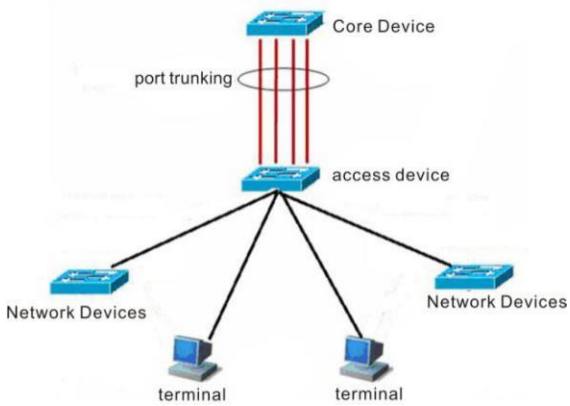
Command	switch# show radius-server switch# show radius-server statistics
Description	Print RADIUS configuration and server status; Print statistics of RADIUS authentication packets;

6 Port aggregation

6.1 Overview of the polymerization port

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

Chart Figure 6-1 Description of the aggregation port



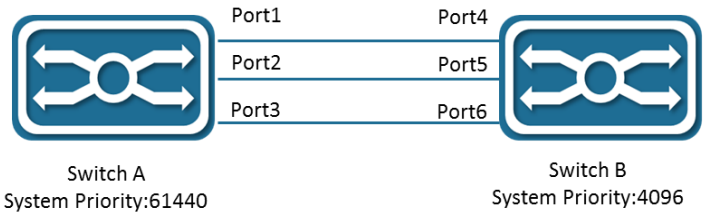
The aggregation port has the following characteristics: high bandwidth, the total bandwidth of the aggregation port is the sum of the bandwidth of the physical member ports; it supports a traffic balancing strategy, which can allocate traffic to each member link according to the strategy; supports link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

6.2 LACP overview

LACP (Link Aggregation Control Protocol) based on the IEEE802.3ad standard is a protocol for dynamic link aggregation. If the port is enabled with LACP protocol, the port will send LACPDU to announce its own system priority, system MAC, port priority, port number, operation key, etc. After the connected device receives the LACP packet from the opposite end, it compares the system priorities of both ends according to the system ID in the packet. At the end of the system ID with higher priority, the ports in the aggregation group will be set in the aggregation state according to the priority of the port ID from high to low, and updated LACP packets will be sent. After the peer device receives the packets, The corresponding port will also be set to the aggregation state, so that the two parties can reach the same when the port exits or joins the aggregation group. Only after the ports of both parties complete the dynamic aggregation and binding operation, the physical link can forward data packets.

After LACP member port links are bound, periodic LACP message interaction will be performed. When the LACP message is not received for a period of time, the packet is considered to be timed out, the member port link is unbound, and the port is not forwardable again. status. There are two modes of timeout here: long timeout mode (or called slow timeout mode) and short timeout mode (or fast timeout mode). In long timeout mode, the port sends a message every 30 seconds, if there is no time for 90 seconds When receiving a message from the opposite end, it is in a packet receiving timeout; in the short timeout mode, the port sends a message every 1 second, and if it does not receive a packet from the opposite end in 3 seconds, it is in a receiving packet timeout.

Chart Figure - 2 LACP description



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

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

6.3 General configuration

In the [Navigation Bar] drop-down menu, select: Configuration -> Link Aggregation -> General to enter the configuration page.

Chart Figure 6-3 General Configuration of Link Aggregation

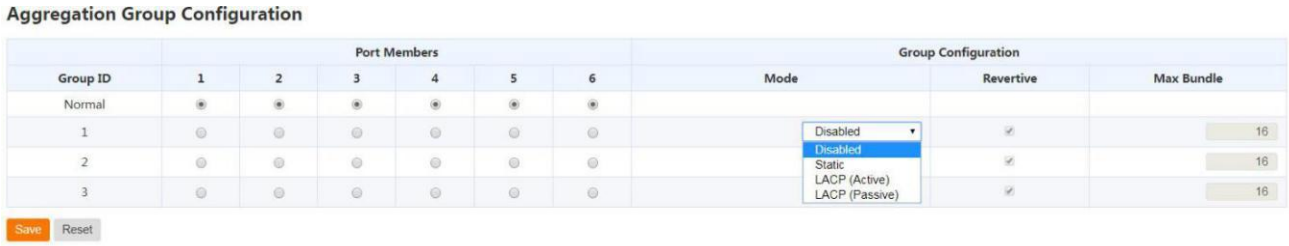
The Hash calculation of the aggregation port (ie balanced method) supports the hash combination of source MAC address, destination MAC address, IP address, and TCP/UDP port number.

6.4 Aggregation group configuration

6.4.1 Configure aggregation group

In the [Navigation Bar] drop-down menu, select: Configuration -> Link Aggregation -> Aggregation Group to enter the configuration page.

Chart Figure 6-4 Aggregation group configuration



Item	Description
Group ID	Aggregation group ID. The number of aggregation groups supported is the number of physical ports divided by 2. For example, 4*10/100/1000Base-T + 2*100/1000Base-X switch has 6 physical ports, and the number of aggregation groups supported is 3.
Port member	Select the port members of each aggregation group. By default, all ports do not belong to any aggregation group. A port can only belong to one aggregation group at most. A maximum of 16 member ports can be configured in an aggregation group. Only full-duplex ports can join the aggregation, and all ports in each aggregation group must have the same rate. If some physical ports have different configurations, they cannot be added to the aggregation group. For example, if one of the member ports is enabled with 802.1X, and the other member ports are not enabled, you cannot join the same aggregation group.
Mode	➢ Disable: The group has been disabled. ➢ static: The group runs in static aggregation mode. ➢ LACP (Active): This group runs in LACP active aggregation mode. ➢ LACP (Passive): This group runs in LACP passive aggregation mode.
Reconvergence	This parameter only applies to groups with LACP enabled. It determines whether the group will perform automatic link (re)calculation when a link with a higher priority is available.
Maximum number of members	This parameter only applies to groups with LACP enabled. It determines the maximum number of active bundled LACP ports allowed in the aggregation. The range is 1-16, and the default is 16.

6.4.2 View aggregation group

In the [Navigation Bar] drop-down menu, select: Monitoring -> Link Aggregation -> Status to enter the display page.

Chart Figure 6-5 Aggregation status display

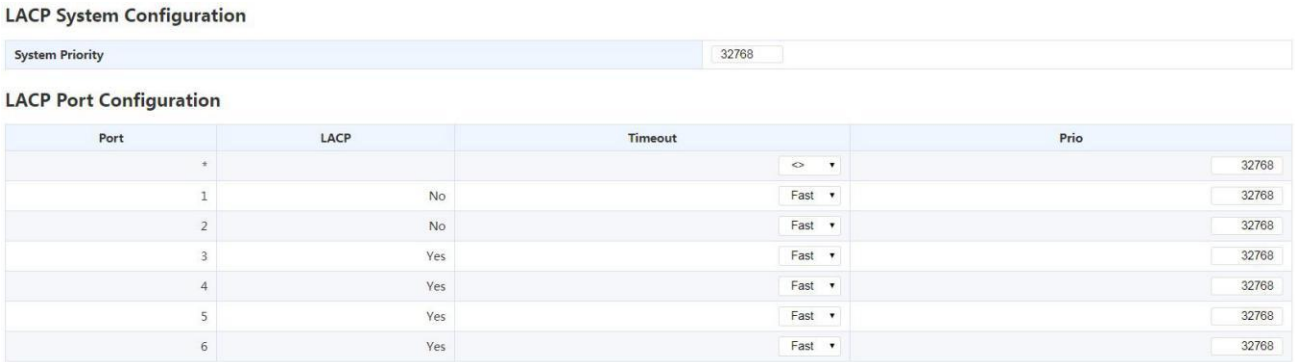
Item	Description
Aggregate ID	Aggregation group ID
Name	Aggregation group name
Types	Aggregation group type, static, LACP_ACTIVE or LACP_PASSIVE
Rate	The port rate of the aggregation group is determined based on the actual aggregation port member ports. If there is no actual aggregation member port, it will display Undefined.
Configure the port	User-configured aggregation group member port
Aggregate port	When the member ports of the aggregation group actually participate in the aggregation, the port is not linked (static group) or the LACP protocol is not joined (LACP group), the configured member ports are not displayed.

6.5 LACP

6.5.1 Configure LACP

In the [Navigation Bar] drop-down menu, select Configuration -> Link Aggregation -> LACP to enter the configuration page.

Chart Figure 6-6 LACP configuration



- LACP system configuration

  LACP system priority. When both devices running the LACP protocol are in ACTIVE mode, the one with the higher priority is the master. The smaller the number, the higher the priority, the range is 1-65535, and the default is 32768.

- LACP port configuration

Item	Description
Port	Panel port number.
LACP	Shows whether LACP is enabled on the port.

Time out	LACP packet timeout mode, Fast is 1 second, Slow is 30 seconds, and the default is Fast.
Priority	Ports are added to the aggregation port priority. The smaller the value, the higher the priority. It takes effect when the number of ports is greater than the maximum number of member ports of the aggregation port. Determine which ports are in the active state and which ports are in the backup state. The range is 1-65535, and the default is 32768.

6.5.2 View LACP information

- LACP system status

In the [Navigation Bar] drop-down menu, select: Monitoring->Link Aggregation->LACP->System Status to enter the viewing interface.

Chart Figure 6-7 LACP system status display

Item	Description
Priority	System priority of this device
MAC address	The MAC address of this device.
Aggregate ID	Aggregation group ID
Partner system ID	MAC address information of the peer device
Partner key	Peer device aggregation group ID
Partner priority	Priority of the peer device aggregation group
Last changed	The latest point in time when the aggregation group changed
Local port	Local port collection to join the aggregation group

- LACP internal state

In the [Navigation Bar] drop-down menu, select: Monitor->Link Aggregation->LACP->Internal Status, enter the view interface

Chart Figure 6-8 LACP internal status display

Item	Description
Port	Panel port number
Status	➢ Down: Port Link down. ➢ Active: The port is active. ➢ Standby: The port is in the backup state. When the active port is abnormal (such as link down or protocol failure), the port in the backup state can be changed to the active state.
Key	The key of the LACP group is generally the aggregation group ID. Only ports with the same key can be aggregated together.
Priority	Port priority
Activity	The working mode of the LACP group, Active or Passive.
Timeout	The timeout mode of the LACP group, Fast or Slow.
Aggregation	The system considers whether the port can be aggregated, that is, a potential aggregation candidate.
Synchronization	Shows whether the system considers this link to be "IN_SYNC"; that is, it has been assigned to the correct LACP group, the group has been associated with a compatible aggregation group, and the identifier is consistent with the sent system ID and operation key information.
Collecting	Shows whether the collection of incoming frames on this link is enabled.
Distributing	Shows whether outgoing frame distribution on this link is enabled.
Defaulted	Shows whether the Actor's receiving device is using the default partner information.
Expired	Shows whether the Actor's receiving device is in the Expired state.

■ LACP neighbor status

In the [Navigation Bar] drop-down menu, select: Monitor->Link Aggregation->LACP->Neighbor Status to enter the view interface.

Chart Figure 6-9 LACP neighbor status display

The information displayed in this table is similar to the internal status information, except that the information displayed is from neighbors. Among them, the partner Key, partner port, and partner port priority correspond to local information (the neighbor's partner is the local). Through these local information, you can observe the specific connection relationship with the neighbor.

■ LACP port statistics

In the [Navigation Bar] drop-down menu, select: Monitor->Link Aggregation->LACP->Port Statistics, enter the view interface.

Chart Figure 6-10 LACP port statistics

Item	Description
Port	Panel port number
LACP reception	Statistics of LACP packets received by the port
LACP send	Statistics of LACP packets sent by the port
Throw away	Statistics of unknown or illegal LACP packets received by the port

6.6 CLI reference commands

Command	switch(config)# aggregation mode smac dmac ip port switch(config)# lacp system-priority 32768
Description	Configure aggregation port hash code combination; Configure the LACP system priority of the aggregation port;

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# aggregation group 1 mode active switch(config-if)# no aggregation group 1
Description	Configure the port as an aggregation port; Configure the port to exit the aggregation port;

Command	switch(config-if)# lacp port-priority 32768 switch(config-if)# lacp timeout fast
Description	Configure the LACP priority of the port aggregation port; Configure port aggregation port LACP timeout mode;

Command	switch# show aggregation switch# show aggregation mode
Description	Print aggregation port configuration and status; Print the hash code combination status of the aggregation port;

Command	switch# show lacp system-id switch# show lacp internal

	switch# show lacp neighbor switch# show lacp statistics
Description	Print the priority of the LACP system of the aggregation port; Print the internal state of the LACP of the aggregation port; Print aggregation port LACP neighbors and port status; Print aggregation port LACP packet statistics;

7 Loop protection

With the increase in the application of ring network technology in the network, the network topology becomes more and more complex, and it often happens that a loop occurs in a local network due to a misconnection. The loop protection function of the equipment has the ability to detect loops, solve loop problems in real time, and provide log information to facilitate management personnel to solve loop faults.

The device port regularly sends private protocol messages and detects whether it has received the private protocol messages sent by the machine to determine whether a loop occurs in the topology. When a loop is detected, the offending port is selected and configuration actions are performed, such as shutting down the port and recording system logs.

Shutdown port: Clear the port MAC address, close the port MAC address learning ability, and prohibit the port forwarding function.

Log: Record the illegal port information in the device system log to facilitate the administrator to locate and troubleshoot the fault.

7.1 Configure loop protection

In the [Navigation Bar] drop-down menu, select: Configuration -> Loop Protection to enter the configuration interface.

- Global configuration

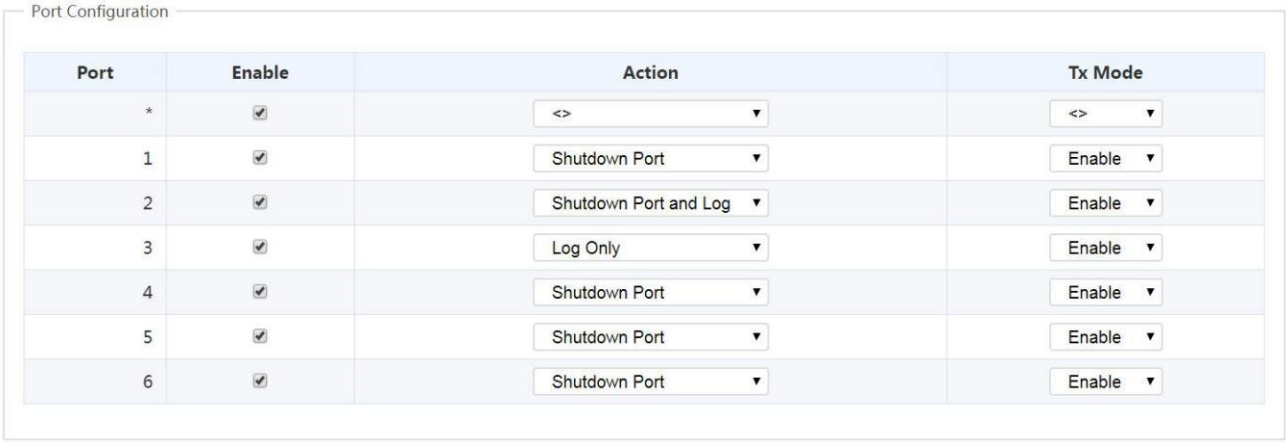
Chart Figure 7-1 Global configuration of loop protection

Item	Description
Enable loop protection	Globally enable loop protection
Transmission	The transmission interval of loop protection protocol packets on each port, the

time	range is 1-10 seconds, and the default is 5 seconds
Disable time	The recovery time of the protection port, the range is 0-604800 seconds, the default is 180 seconds, and the protection port will not recover when configured with 0 seconds.

■ Port configuration

Chart Figure 7-2 Loop protection port configuration

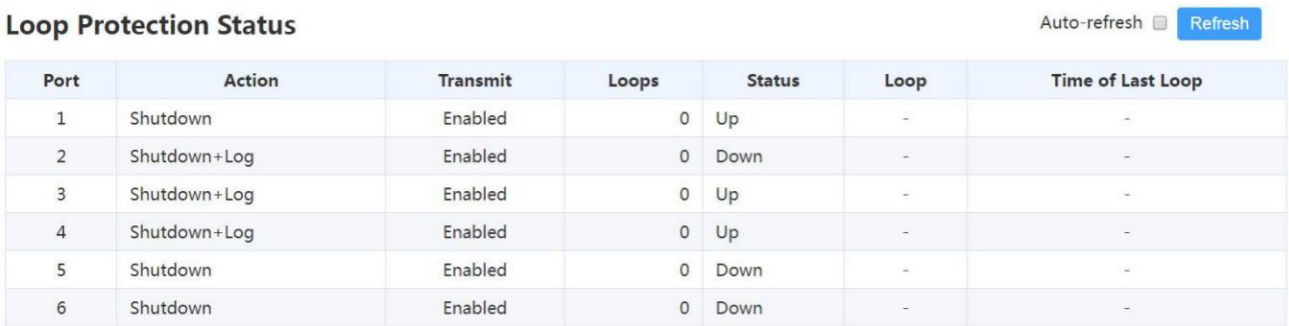


Item	Description
Port	Panel port number
Enable	Enable loop protection function on the port
Behavior	Action on the port when loop is found, supports three actions: Shutdown Port, Shutdown Port and Log, and Log Only
Tx mode	The port is enabled to send loop protection protocol packets, if it is disabled, it can only passively receive loop protection protocol packets

7.2 View loop protection status

In the [Navigation Bar] drop-down menu, select: Monitoring -> Loop Protection to enter the viewing interface.

Chart Figure 7-3 Loop protection status display



Item	Description
Port	Panel port number

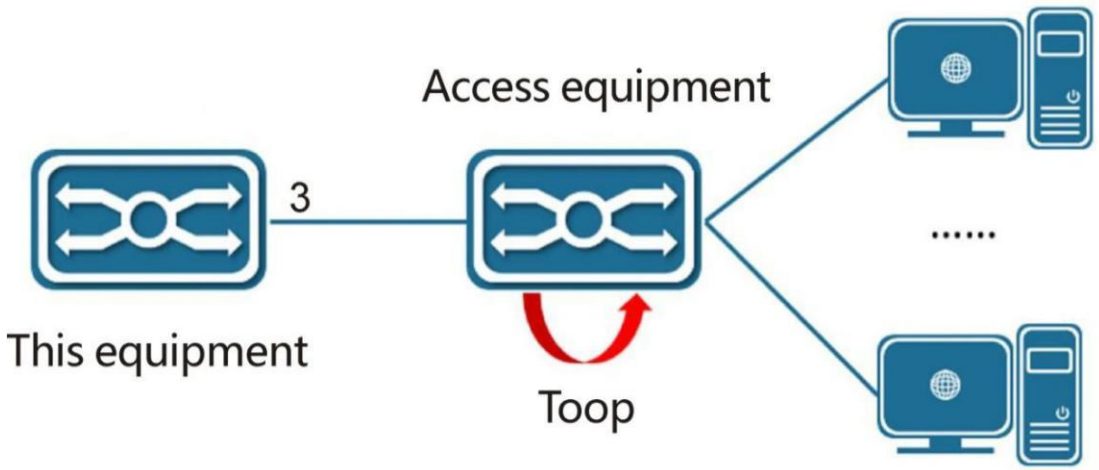
Behavior	Enable loop protection function on the port
Send	Whether the port is enabled in Tx mode
Number of cycles	Number of loops detected on the port
Status	The current port status, such as the behavior Shutdown, the port is in the Disabled state when a loop is detected
Ring	Whether the current port is in a loop state
Last ring time	The time when the port was last detected the loop

7.3 Typical configuration examples of loop protection

- Case requirements

In the system environment, port 9 is connected to the access device and extended terminal access. In order to prevent loops in the access device network, turn on the loop protection function on port 9, shut down port 9 and product logs in time when loops are detected, to avoid affecting the device network environment.

Chart Figure 7-4 Loop Protection Case

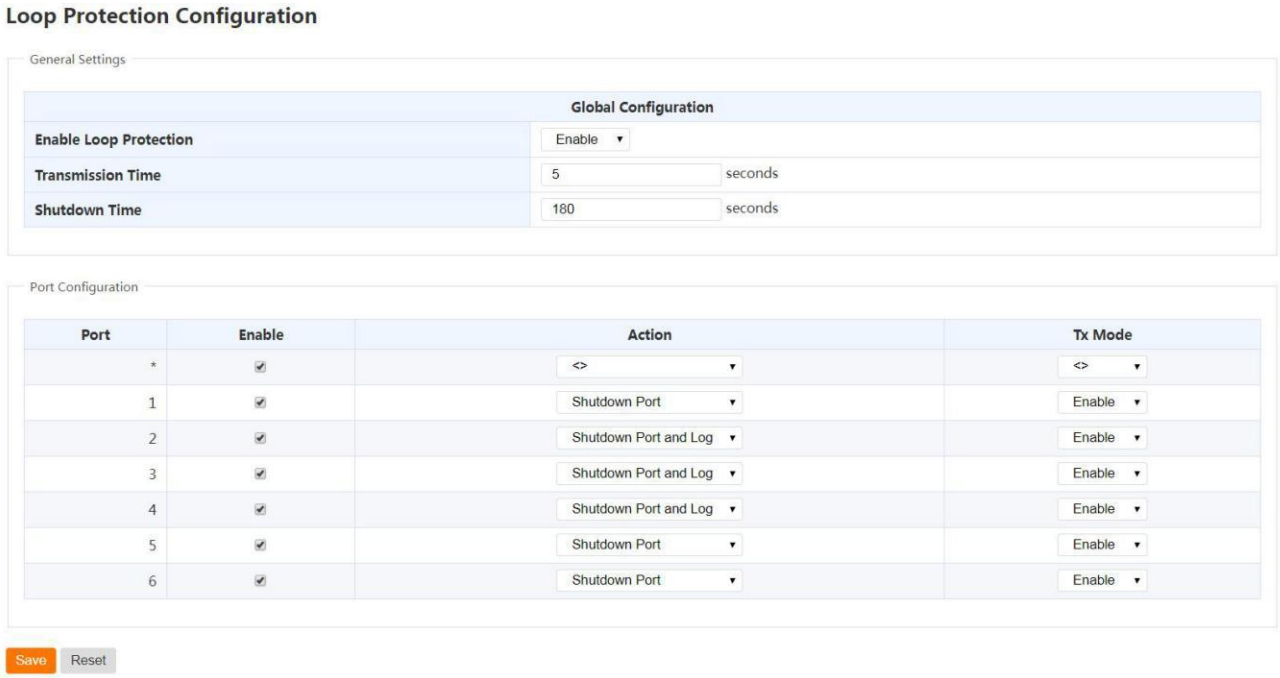


- Operation steps

The loop protection function is enabled globally, the loop protection function is enabled on port 3, and the behavior is Shutdown Port and Log.

Chart Figure 7-5 Loop Protection Case Configuration

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com



In the access equipment manufacturing loop, check the loop protection status information.

Chart Figure 7-6 Loop protection case status

Loop Protection Status

Auto-refresh Refresh

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	-	-
2	Shutdown+Log	Enabled	0	Down	-	-
3	Shutdown+Log	Enabled	0	Up	-	-
4	Shutdown+Log	Enabled	70	Down	-	1970-01-01T06:10:59+00:00
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-

7.4 CLI reference commands

Command	switch(config)# loop-protect switch(config)# no loop-protect switch(config)# loop-protect transmit-time 5 switch(config)# loop-protect shutdown-time 180
Description	Configure to open loop protection; Configure closed loop protection; Configure loop protection transmission time; Configure the loop protection recovery time;

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# loop-protect switch(config-if)# no loop-protect switch(config-if)# loop-protect action shutdown log switch(config-if)# loop-protect tx-mode switch(config-if)# no loop-protect tx-mode
Description	Configure the port to enable loop protection; Configure port to close loop protection; Configure port loop protection behavior; Configure the port to enable loop protection Tx mode; Configure the port to close the loop protection Tx mode;

Command	switch# show loop-protect
Description	Print loop protection configuration and status;

8 Spanning tree

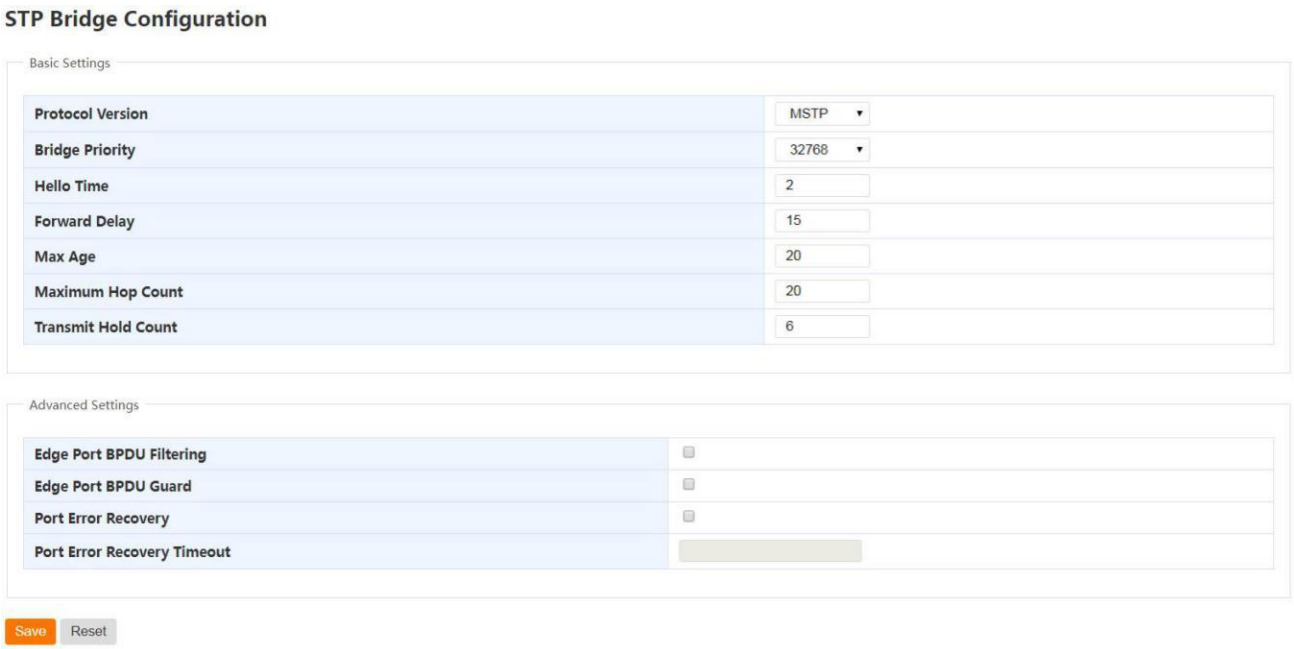
8.1 Overview

Spanning Tree Protocol is a two-layer management protocol. It eliminates two-layer loops by selectively blocking redundant links in the network. It also has the function of link backup. Like the development process of many protocols, the Spanning Tree Protocol is constantly updated with the development of the network, from the original STP (Spanning Tree Protocol) to RSTP (Rapid Spanning Tree Protocol), and then To the latest MSTP (Multiple SpanningTree Protocol).
For Layer 2 Ethernet, there can only be one active path between two LANs, otherwise a broadcast storm will occur. However, in order to enhance the reliability of a local area network, it is necessary to establish redundant links. Some of the paths must be in a backup state. If the network fails and another link fails, the redundant link must be upgraded to Active status. Manually controlling such a process is obviously a very hard work, and the STP protocol automatically completes this work. It enables the devices in a local area network to perform the following functions:
• Discover and start an optimal tree topology of the LAN.
• Find faults and recover accordingly, automatically update the network topology, so that the best possible tree structure is selected at any time.

8.2 Introduction to Spanning Tree Configuration

8.2.1 Bridge parameter configuration

Click on the navigation bar: Configuration -> Spanning Tree -> Bridge Settings to enter the bridge parameter configuration interface.
Chart Figure 8-1 Spanning Tree Bridge Configuration



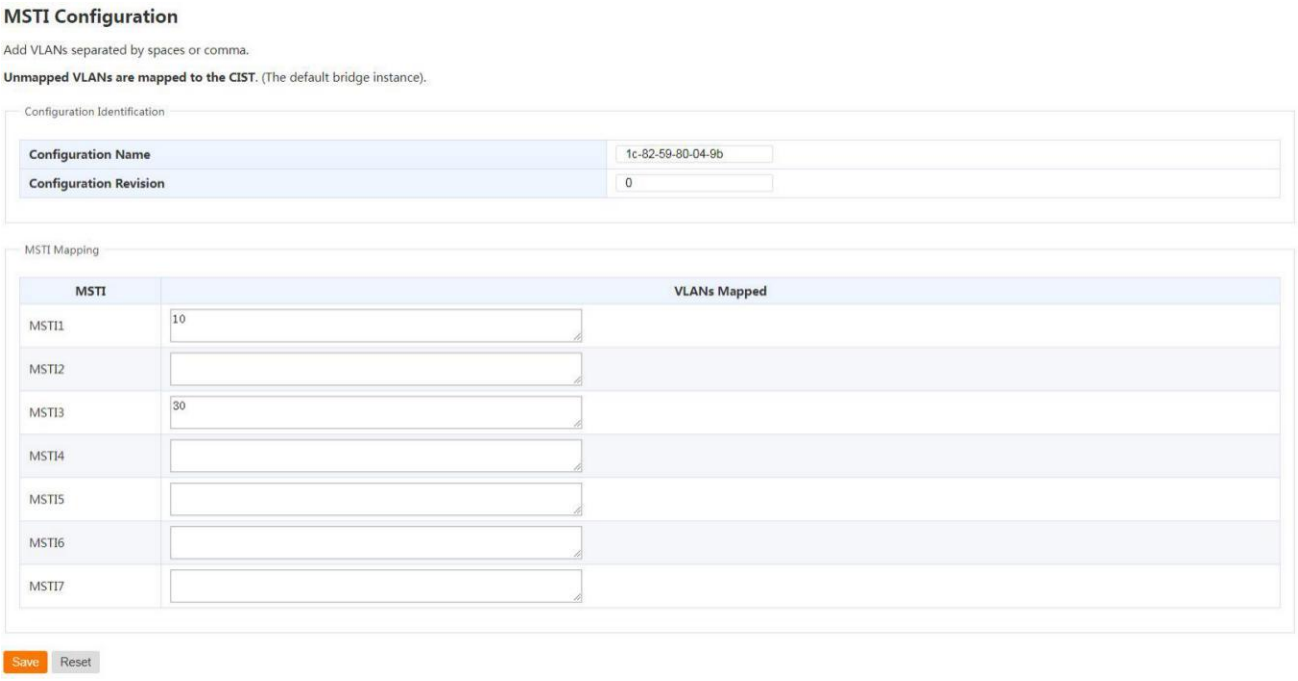
Item	Description
Protocol version	Set the version mode of STP, including STP, RSTP and MSTP STP: In STP mode, each port of the device will send out STP BPDU packets RSTP: In RSTP mode, each port of the device will send out RSTP BPDU packets. When it is found to be connected to a device running STP, the port will automatically migrate to work in STP mode MSTP: In MSTP mode, each port of the device will send out MSTP BPDU packets, when it is found to be connected to a device running STP, the port will automatically migrate to work in STP mode
Bridge priority	Spanning tree protocol parameters, used for optimal spanning tree calculation. The smaller the value, the higher the priority. For the MSTP protocol, this configuration is only valid for CIST.
Hello Time	Set the period for the device to send hello packets to detect link failures.
Forward Delay	Set the delay time for device state transition.
Max Age	Set the maximum length of time a message is stored in the device.
Maximum Hop Count	Set the maximum number of hops in the MST region. This parameter determines the size of the MST region Only the parameter configured on the domain root will take effect in the domain, and the configuration on the non-domain root is invalid.
Transmit Hold Count	The maximum number of BPDU packets sent by the bridge per second.
Edge port	Set whether to enable the BPDU filtering function.

BPDU filtering	After the BPDU filtering function is enabled, the edge port will enable BPDU message sending and receiving processing when receiving BPDU messages.
Edge port BPDU protection	Set whether to enable the BPDU protection function. After the BPDU protection function is enabled, the edge port will enter an error state when receiving BPDU packets, which can prevent man-made configuration messages from maliciously attacking the device and avoid network shocks.
Port error recovery	Set whether to enable the port error recovery function. When the port error recovery function is enabled, after the port enters the error state, the device will automatically restore the error port after the specified timeout period, allowing the port to participate in protocol calculation and forwarding again.
Port error recovery timeout	The timeout period to wait for recovery after a port error.

8.2.2 MSTI mapping configuration

Click on the navigation bar: Configuration -> Spanning Tree -> MSTI Mapping to enter the MSTI mapping configuration interface.

Chart Figure 8-2 MSTI mapping configuration



Item	Description
Configuration name	MSTI domain configuration name. The MSTI configuration names of switches in the same domain must be the same.
Configuration version number	MSTI version level. The MSTI version level of the switches in the same domain must be the same.
Mapped VLAN	Configure the mapping relationship between MSTI instances and VLANs.

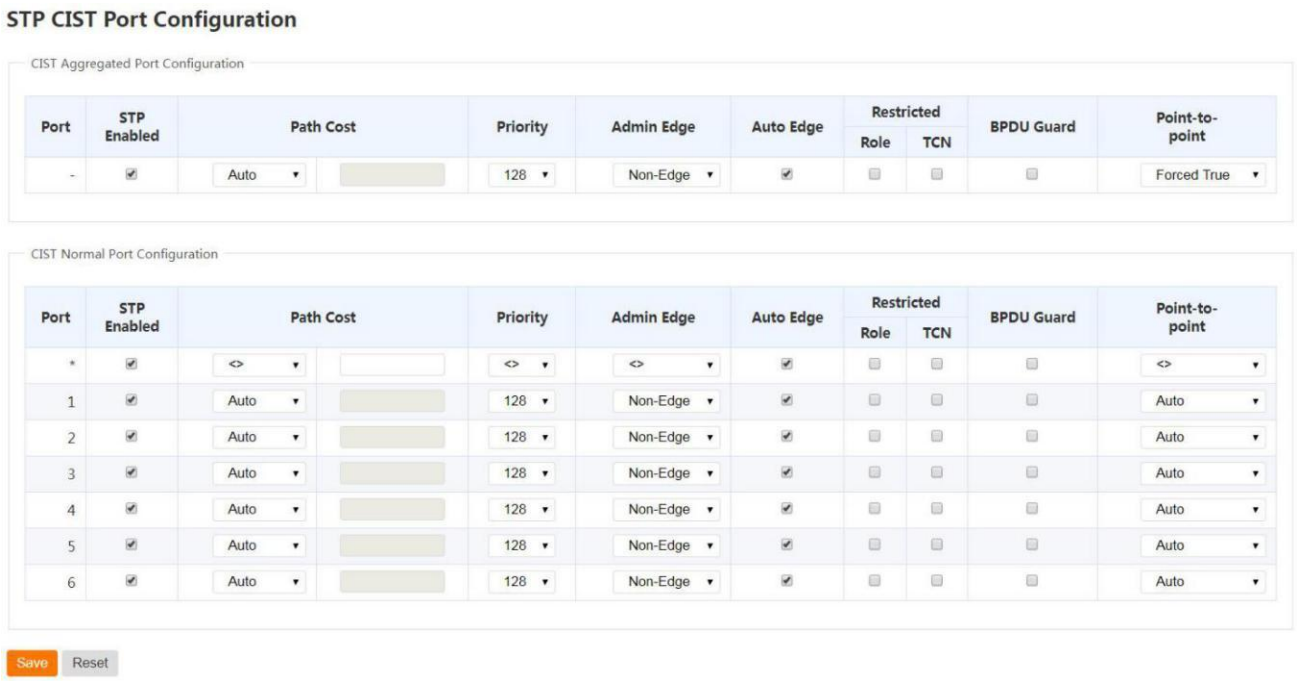
8.2.3 MSTI priority configuration

Click on the navigation bar: Configuration -> Spanning Tree -> MSTI Priority to enter the MSTI priority configuration interface.
Chart Figure 8-3 MSTI priority configuration

Item	Description
Priority	Spanning tree bridge priority. The CIST priority is the same as the bridge priority in the bridge parameter configuration, and the MSTI priority is the priority of the multiple spanning tree instance bridge, which is used to participate in the protocol calculation in each spanning tree.

8.2.4 CIST port configuration

Click on the navigation bar: Configuration -> Spanning Tree -> CIST Port to enter the CIST port configuration interface.
Chart Figure 8-4 CIST port configuration

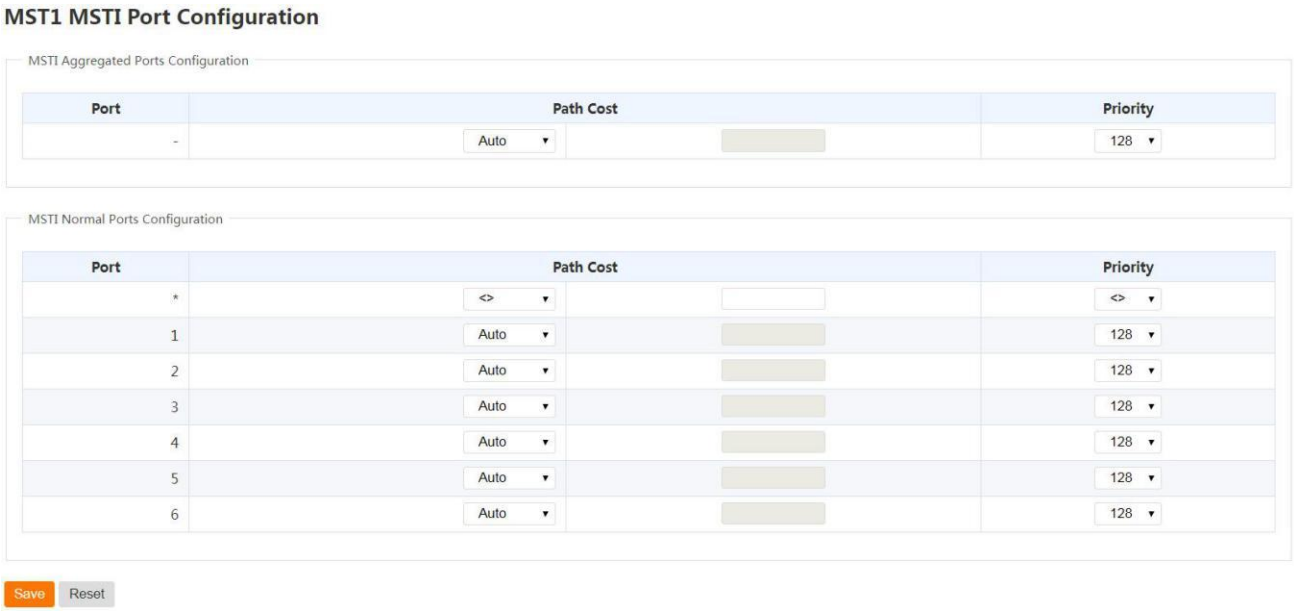


Item	Description
STP enabled	Spanning tree switch.
Path cost	Auto: Automatic calculation, the system will automatically calculate based on parameters such as port rate/type. Specific: Manually specify, the value is a number from 1-200000000.
Priority	Port priority, the smaller the value, the higher the priority.
Forced edge	Non-Edge: Non-edge mouth. Edge: Force recognition as an edge port. The edge port does not participate in STP protocol calculation by default.
Automatic edge	Set the automatic recognition port to be an edge port.
Restricted role	The protection port is not elected as the root port, and the effect is similar to the root protection function.
Restricted TCN	Restrict the port's ability to forward topology change notifications.
BPDU protection	After BPDU protection is enabled, the port will immediately enter an error state when receiving BPDU packets. The port can be restored through the error recovery function, or the port can be restored by resetting the port management status.
Point to Point	Auto: Automatically identify whether the port link mode is point-to-point mode. Force True: Force the port link mode to point-to-point mode. Force False: Force the port link mode to non-point-to-point mode. Links in point-to-point mode can quickly negotiate and converge without waiting for delays and timers to expire.

8.2.5 MSTI port configuration

Click on the navigation bar: Configuration -> Spanning Tree -> MSTI Port, select the MST instance that needs to be configured, and click the [Get] button to enter the MST port configuration interface.

Chart Figure 8-5 MSTI port configuration

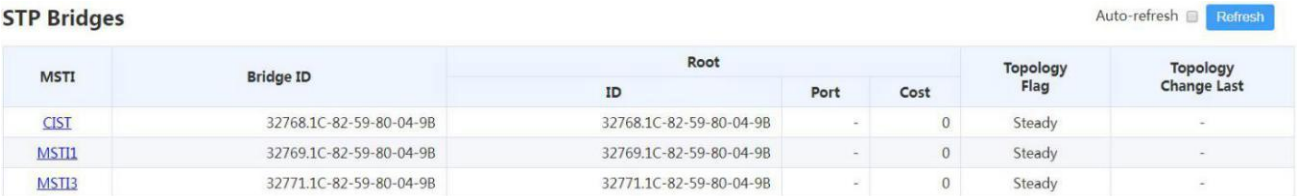


Item	Description
Path cost	Auto: Automatic calculation, the system will automatically calculate based on parameters such as port rate/type. Specific: Manually specify, the value is a number from 1-200000000.
Priority	Port priority, the smaller the value, the higher the priority.

8.2.6 View bridge status

Click on the navigation bar: Monitor -> Spanning Tree -> Bridge Status to enter the Spanning Tree Bridge Status interface.

Chart Figure 8-6 Spanning Tree Bridge Status

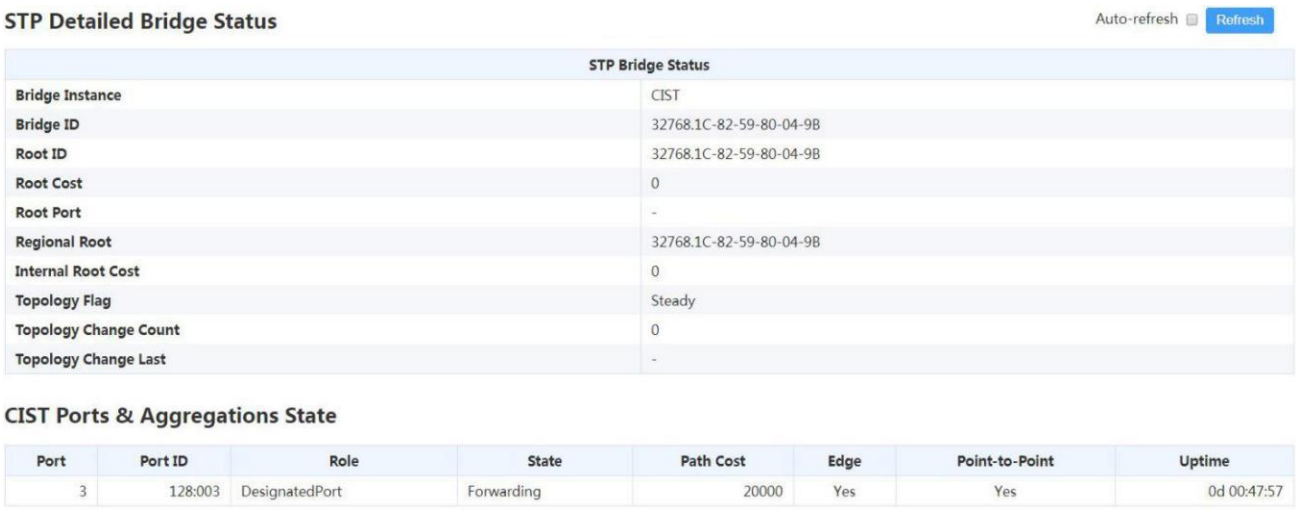


Item	Description
Bridge ID	Bridge ID of the MST region or CIST region.
Root ID	The ID of the root bridge elected in the MSTI or CIST spanning tree.

Root port	The role of the root port in the current spanning tree.
Root overhead	The total path cost from the current node to the root of the spanning tree.
Topology identification	The spanning tree topology change identifier of the current node.
Topology last changed	The time when the topology change was last detected.

Click the specific MSTI in the bridge status page, for example, click [CIST], you can view the detailed status information of the MST/CIST and the port information in the spanning tree.

Chart Figure 8-7 Bridge detailed status



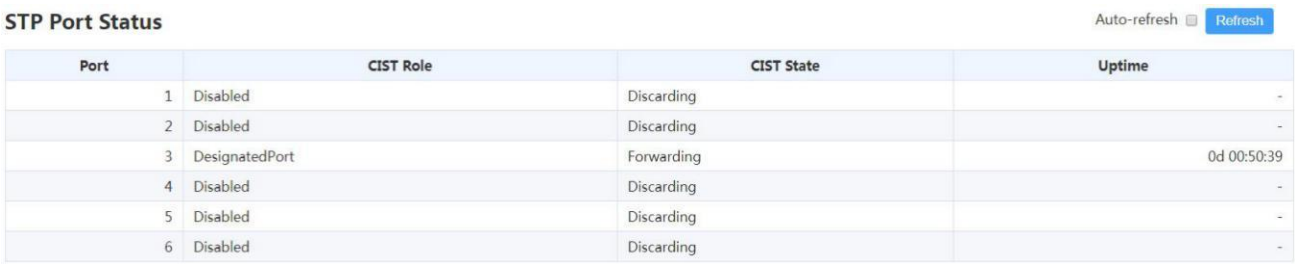
Item	Description
Bridge instance	The name of the bridge instance currently being viewed.
Bridge ID	The current bridge ID.
Root ID	The ID of the root bridge elected in the MSTI or CIST spanning tree.
Root overheat	The total path cost from the current node to the root of the spanning tree.
Root port	The role of the root port in the current spanning tree.
Domain root	Root ID of the MST region. The regional root of CIST is the root bridge of the entire network.
Internal root overhead	The total path cost from the current node to the regional root.
Topology identification	The spanning tree topology change identifier of the current node.
Topology change count	The number of detected topology changes.
Topology last changed	The time when the topology change was last detected.
Port	The port number of the bridge.
Port ID	Protocol port ID synthesized by port priority and port number.
Character	Port roles, including

	Root: Root port, the direction in which the interface is connected to the root bridge Designated: designated port, the port connected to the root port Alternate: alternate port, alternate root port Backup: Backup port Disable: The interface is Down or the port of the Spanning Tree Protocol is disabled
Status	Port roles, including Root: Root port, the direction in which the interface is connected to the root bridge Designated: designated port, the port connected to the root port Alternate: alternate port, alternate root port Backup: Backup port Disable: The interface is Down or the port of the Spanning Tree Protocol is disabled The current protocol status of the port, including: Forwarding: forwarding Discarding: Discarding Learning: Learning Listening: listening
Path cost	The path cost of the port.
Edge	Whether it is an edge port.
Point to point	Whether it is a point-to-point link.
Operation hours	Port protocol running time.

8.2.7 View port status

Click on the navigation bar: Monitoring -> Spanning Tree -> Port Status to enter the Spanning Tree Port Status interface.

Chart Figure 8-8 Spanning Tree Port Status



Item	Description
CIST role	CIST port roles, mainly including Root: Root port, the direction in which the interface is connected to the root

	bridge Designated: designated port, the port connected to the root port Alternate: alternate port, alternate root port Backup: Backup port Disable: The interface is Down or the port of the Spanning Tree Protocol is disabled
CIST status	The current protocol status of the CIST port, including: Forwarding: forwarding Discarding: Discarding Learning: Learning Listening: listening
Operation hours	Port protocol running time.

8.2.8 View port statistics

Click on the navigation bar: Monitoring -> Spanning Tree -> Port Statistics to enter the Spanning Tree Port Statistics interface.

Chart Figure 8-9 Spanning Tree Port Statistics

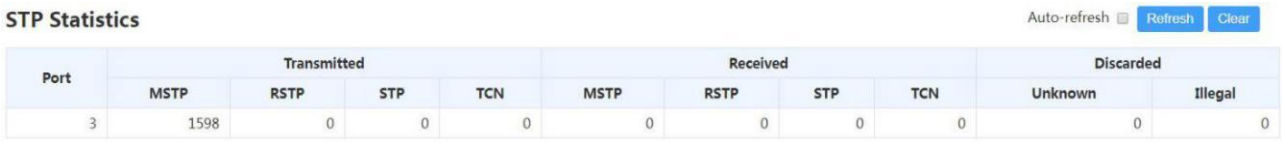


Table 8-1 Port statistics parameter description

Item	Description
Port	The port number
Send MSTP	Number of sent MSTP packets.
Send RSTP	Number of RSTP packets sent.
Send STP	Number of STP packets sent.
Send TCN	The number of TCN packets sent.
Receive MSTP	Number of received MSTP packets.
Receive RSTP	Number of RSTP packets received.
Receive STP	Number of received STP packets.
Receive TCN	Number of received TCN packets.
Discard unknown	The number of discarded unknown BPDU packets.
Discard illegal	Number of discarded illegal BPDU packets.

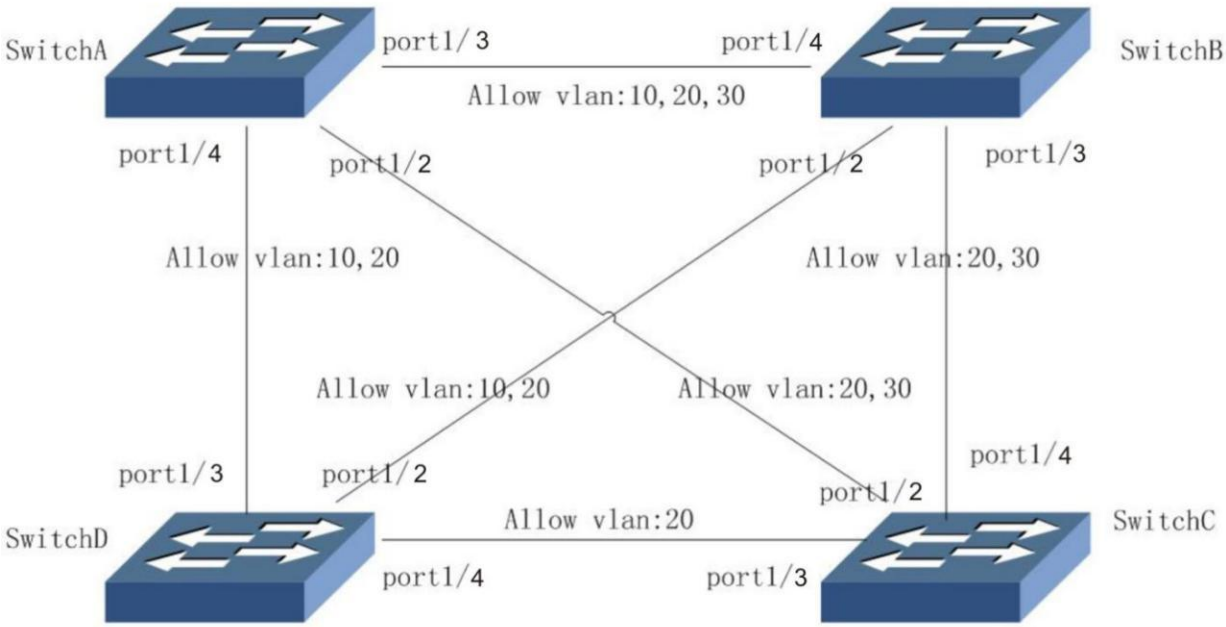
8.3 MSTP configuration examples

8.3.1 Networking requirements

Configure MSTP, as shown in the figure below, packets of different VLANs are forwarded according to different spanning tree instances. The specific configuration is:
• All devices in the network belong to the same MST domain, which is assumed to be the global domain;
• VLAN 20 is forwarded along instance 0 (that is, the default bridge instance CIST), VLAN 10 packets are forwarded along instance 1, and VLAN 30 is forwarded along instance 3.
The parameter configuration of each device is shown in the following table:

Device	VLAN	Instance	Port
Switch A	10	1	port1/3, port1/4
	20	0	port1/3, port1/4, port1/2
	30	3	port1/3, port1/2
Switch B	10	1	port1/4, port1/2
	20	0	port1/3, port1/4, port1/2
	30	3	port1/3, port1/4
Switch C	20	0	port1/3, port1/4, port1/2
	30	3	port1/4, port1/2
Switch D	10	1	port1/3, port1/2
	20	0	port1/3, port1/4, port1/2

Chart Figure 8-10 MSTP case



Note

- The description "Allow vlan" on the link in the figure indicates which VLAN packets are allowed to pass through the link.

8.3.2 Configure Switch A

Step 1: Configure VLAN and port.
In the navigation bar, select: Configuration -> VLAN, configure ports 2, 3, and 4 as trunk ports, configure the corresponding allow vlan, and click the [Save] button to save the configuration.
Chart Figure 8-11 MSTP case Switch A VLAN configuration

Global VLAN Configuration

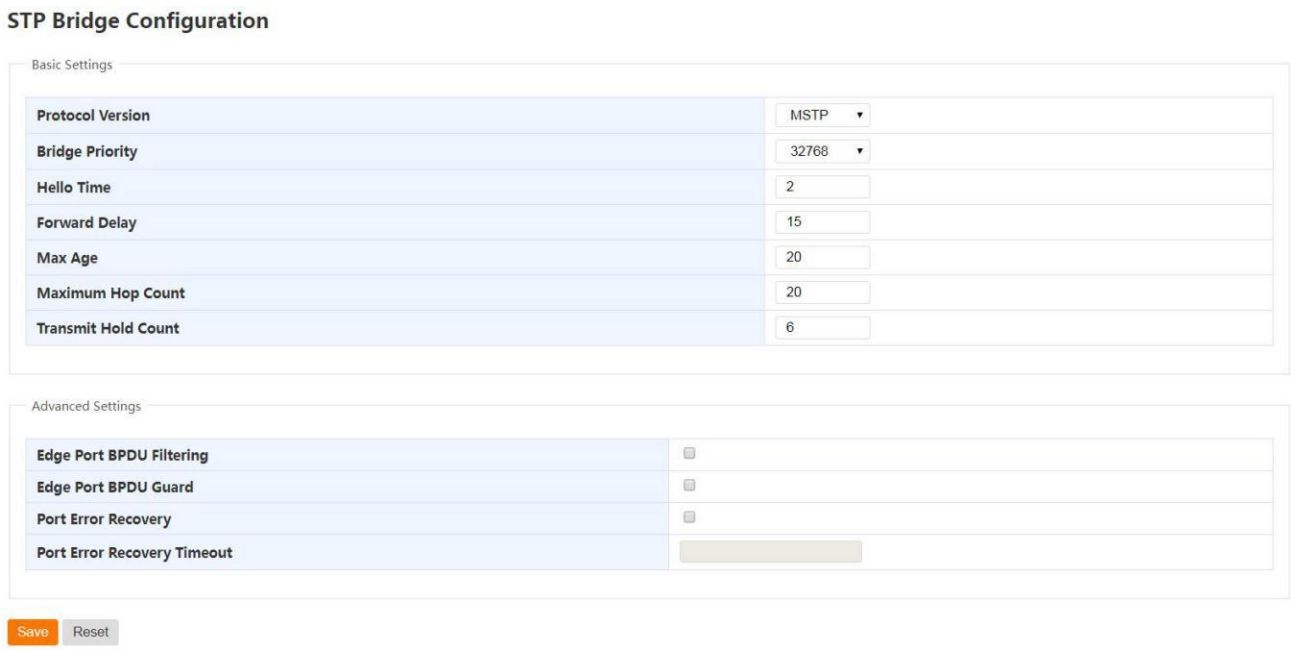
Allowed Access VLANs	1,10,20,30
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	20,30	
3	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	10,20,30	
4	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	10,20	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Save Reset

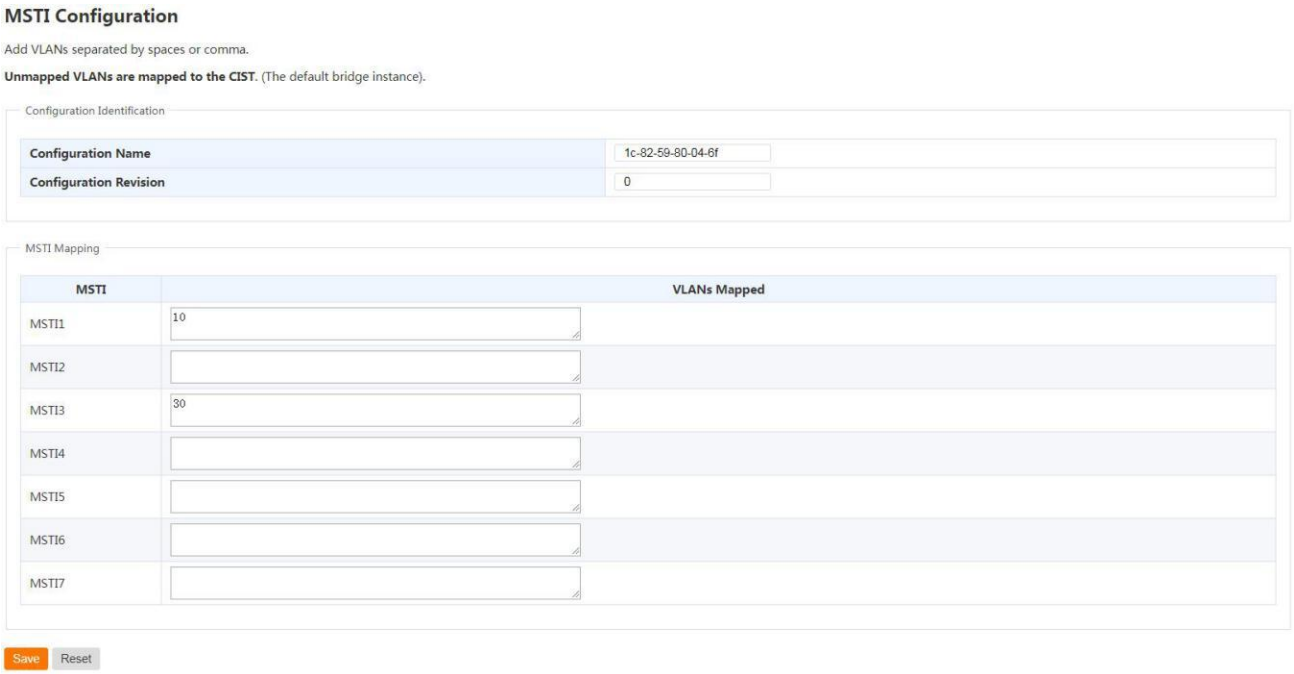
Step 2: Configure spanning tree bridge parameters.
In the navigation bar, select: Configuration -> Spanning Tree -> Bridge Settings, configure the protocol version as MSTP, and click the [Save] button to save the configuration.
Chart Figure 8-12 MSTP case Switch A bridge configuration



Step 3: Configure spanning tree MSTI mapping.

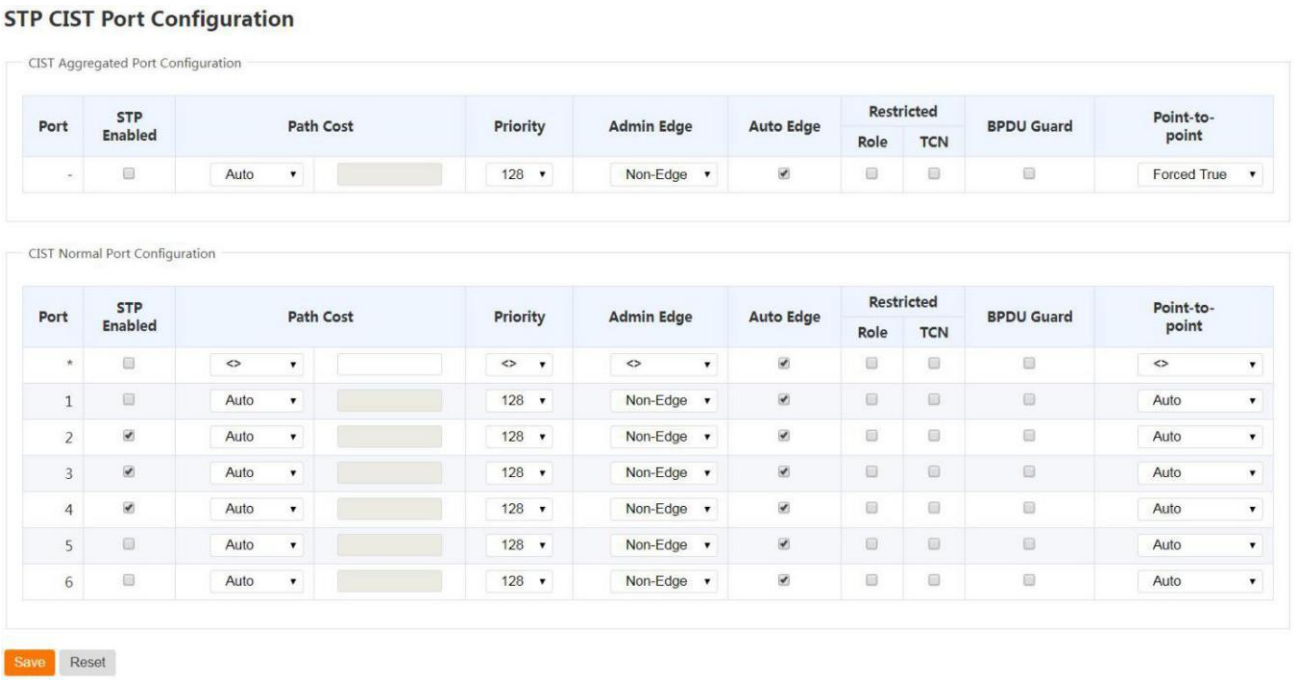
In the navigation bar, select: Configuration -> Spanning Tree -> MSTI Mapping, configure VLAN 10 to be mapped to MSTI 1, and VLAN 30 to MSTI 3, and click the [Save] button to save the configuration.

Chart Figure 8-13 MSTP case Switch A MSTI mapping configuration



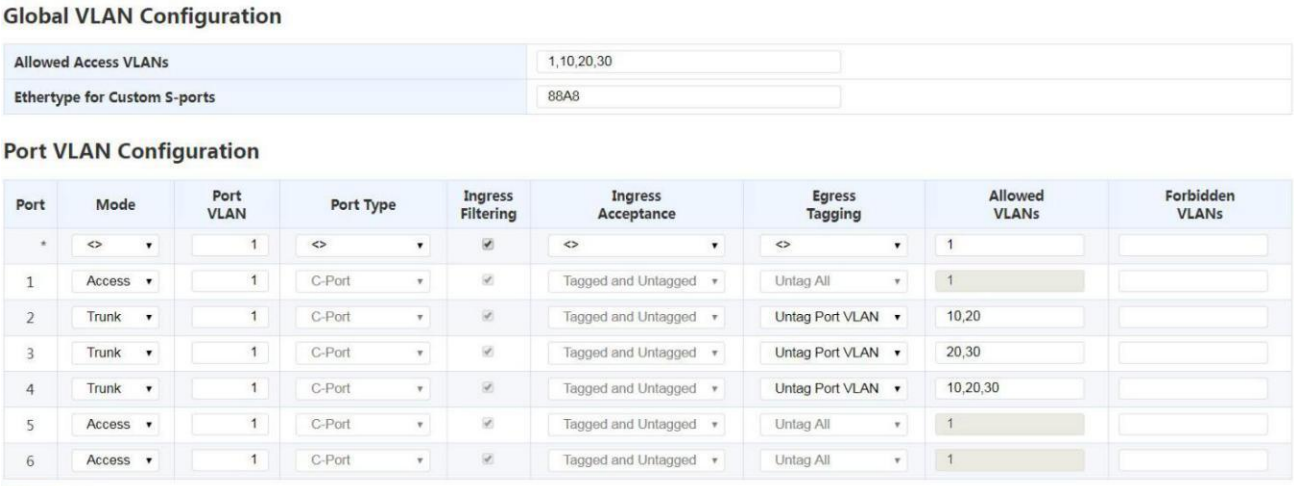
Step 3: Configure the port to enable Spanning Tree Protocol.

In the navigation bar, select: Configuration -> Spanning Tree -> CIST Port, configure ports 2, 3, and 4 as STP enabled state.
Chart Figure 8-14 MSTP case Switch A CIST port configuration

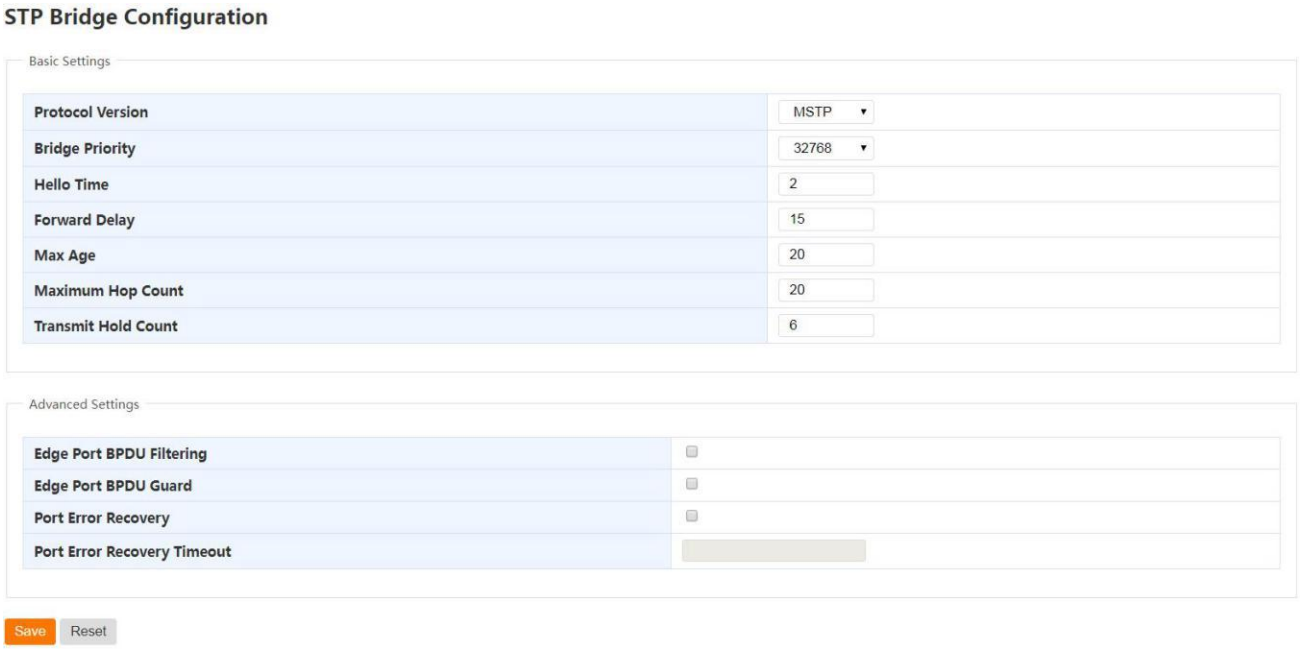


8.3.3 Configure Switch B

Step 1: Configure VLAN and port.
In the navigation bar, select: Configuration -> VLAN, configure ports 2, 3, and 4 as trunk ports, configure the corresponding allow vlan, and click the [Save] button to save the configuration.
Chart Figure 8-15 MSTP case Switch B VLAN configuration



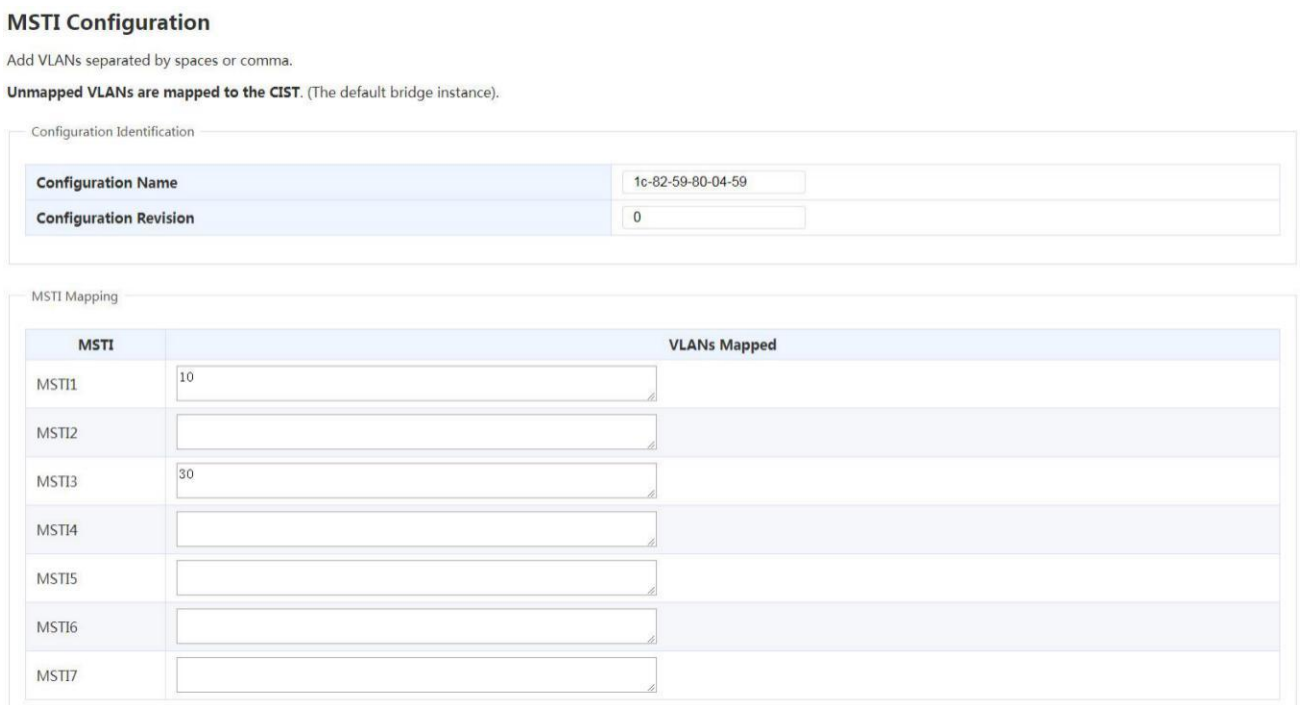
Step 2: Configure spanning tree bridge parameters.
In the navigation bar, select: Configuration -> Spanning Tree -> Bridge Settings, configure the protocol version as MSTP, and click the [Save] button to save the configuration.
Chart Figure 8-16 MSTP case Switch B bridge configuration



Step 3: Configure spanning tree MSTI mapping.

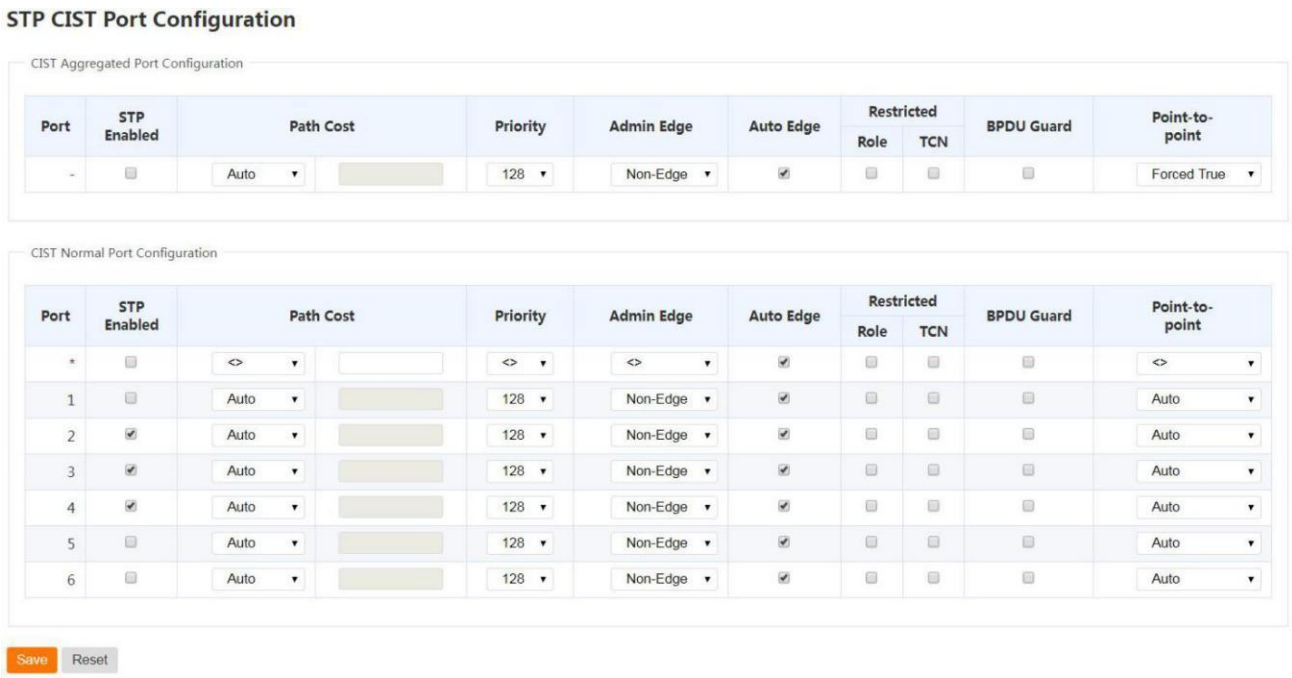
In the navigation bar, select: Configuration -> Spanning Tree -> MSTI Mapping, configure VLAN 10 to be mapped to MSTI 1, and VLAN 30 to MSTI 3, and click the [Save] button to save the configuration.

Chart Figure 8-17 MSTP case Switch B MSTI mapping configuration



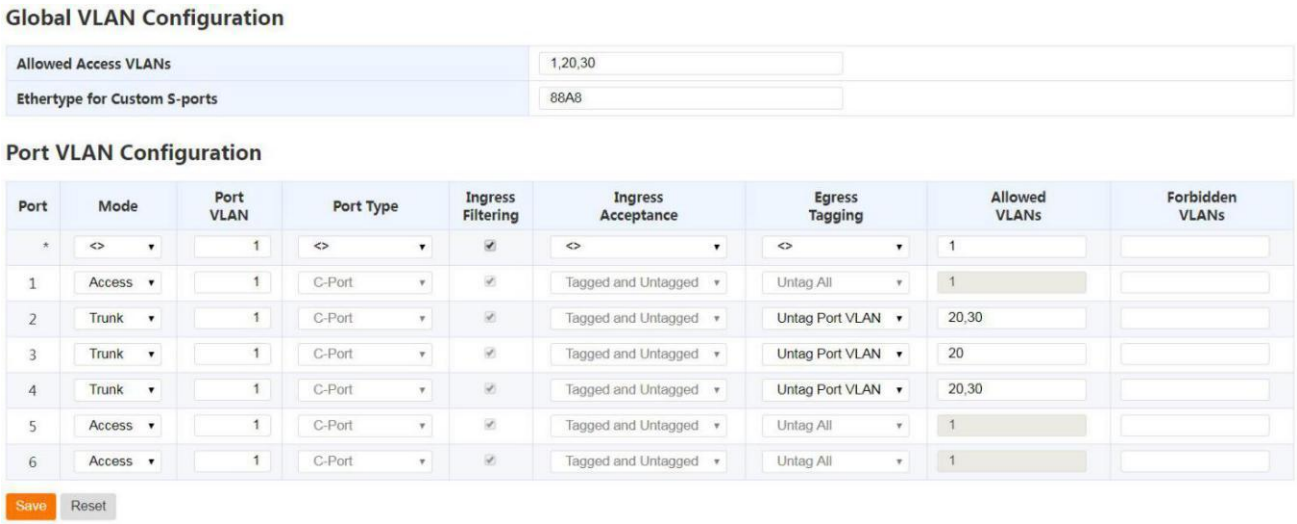
Step 3: Configure the port to enable Spanning Tree Protocol.
In the navigation bar, select: Configuration -> Spanning Tree -> CIST Port, configure ports 2, 3, and 4 as STP enabled state.

Chart Figure 8-18 MSTP case Switch B CIST port configuration

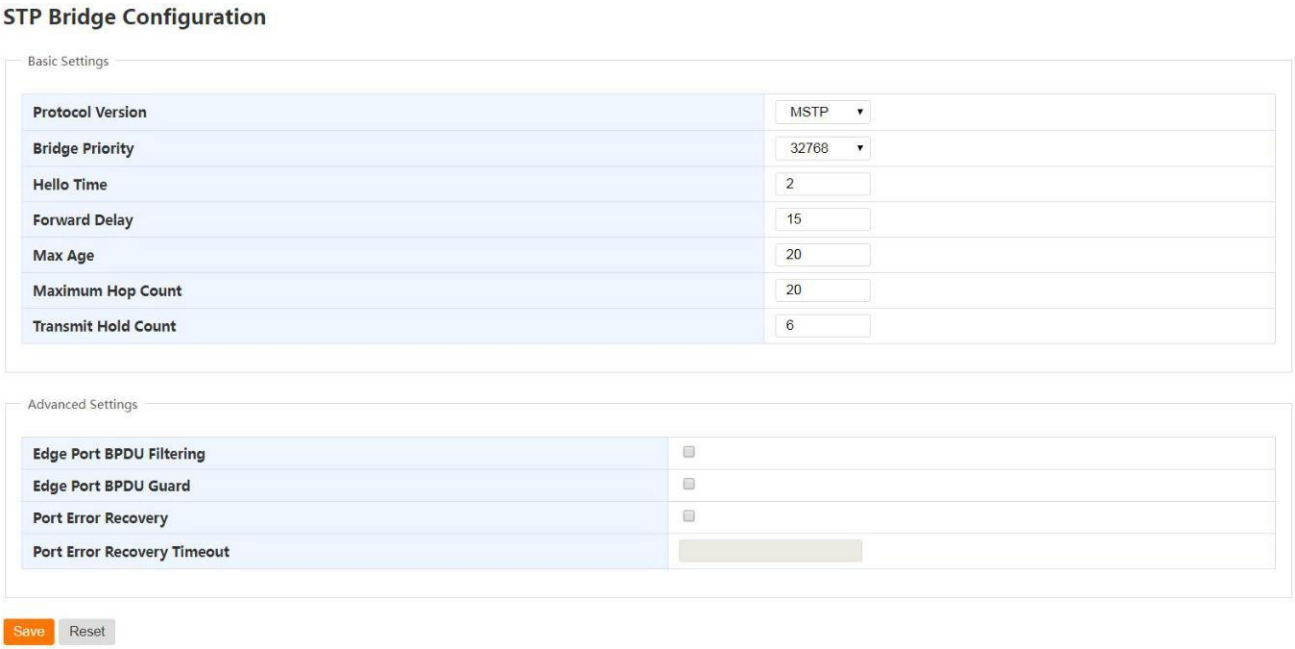


8.3.4 Configure Switch C

Step 1: Configure VLAN and port.
In the navigation bar, select: Configuration -> VLAN, configure ports 2, 3, and 4 as trunk ports, configure the corresponding allow vlan, and click the [Save] button to save the configuration.
Chart Figure 8-19 MSTP case Switch C VLAN configuration



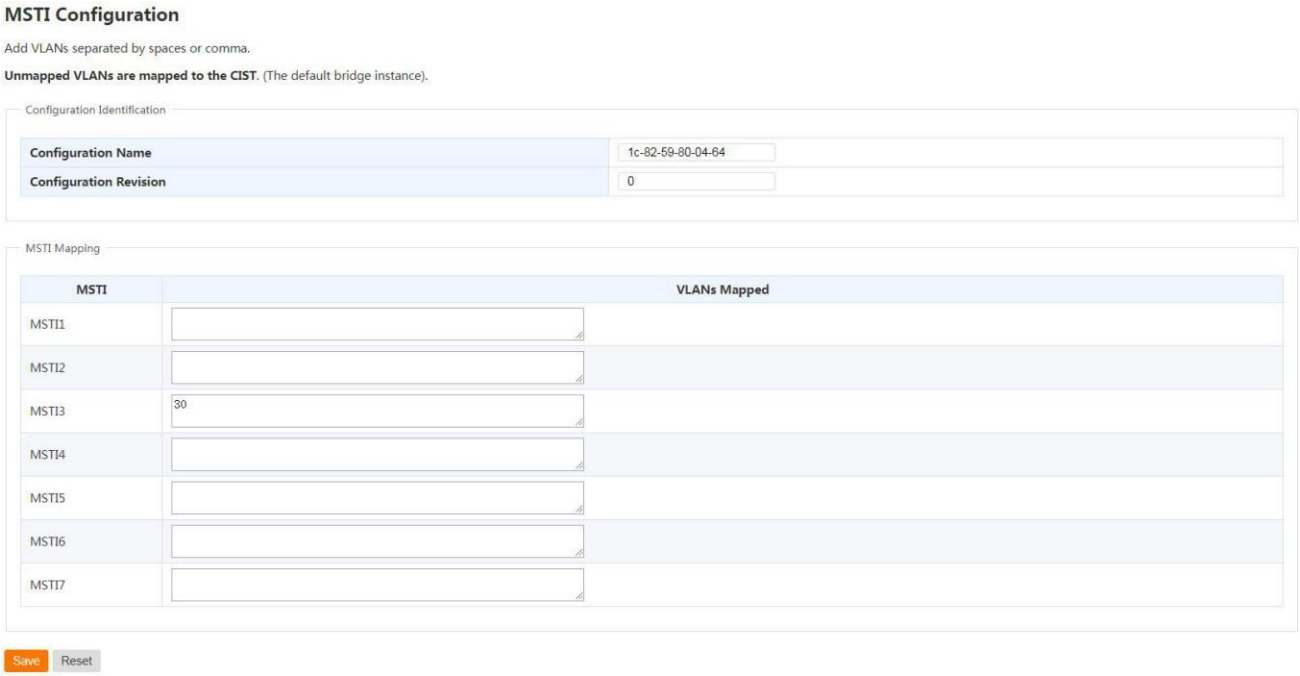
Step 2: Configure spanning tree bridge parameters.
In the navigation bar, select: Configuration -> Spanning Tree -> Bridge Settings, configure the protocol version as MSTP, and click the [Save] button to save the configuration.
Chart Figure 8-20 MSTP case Switch C bridge configuration



Step 3: Configure spanning tree MSTI mapping.

In the navigation bar, select: Configuration -> Spanning Tree -> MSTI Mapping, configure VLAN 30 to be mapped to MSTI 3, and click the [Save] button to save the configuration.

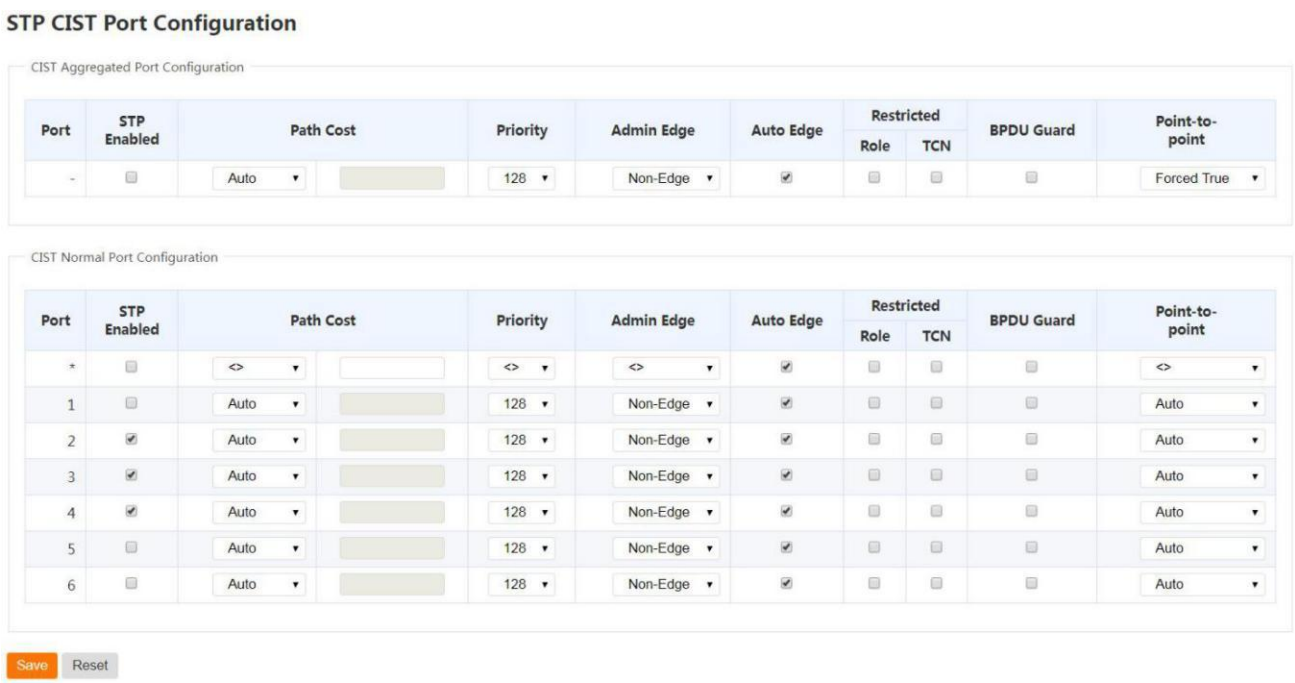
Chart Figure 8-21 MSTP case Switch C MSTI mapping configuration



Step 3: Configure the port to enable Spanning Tree Protocol.

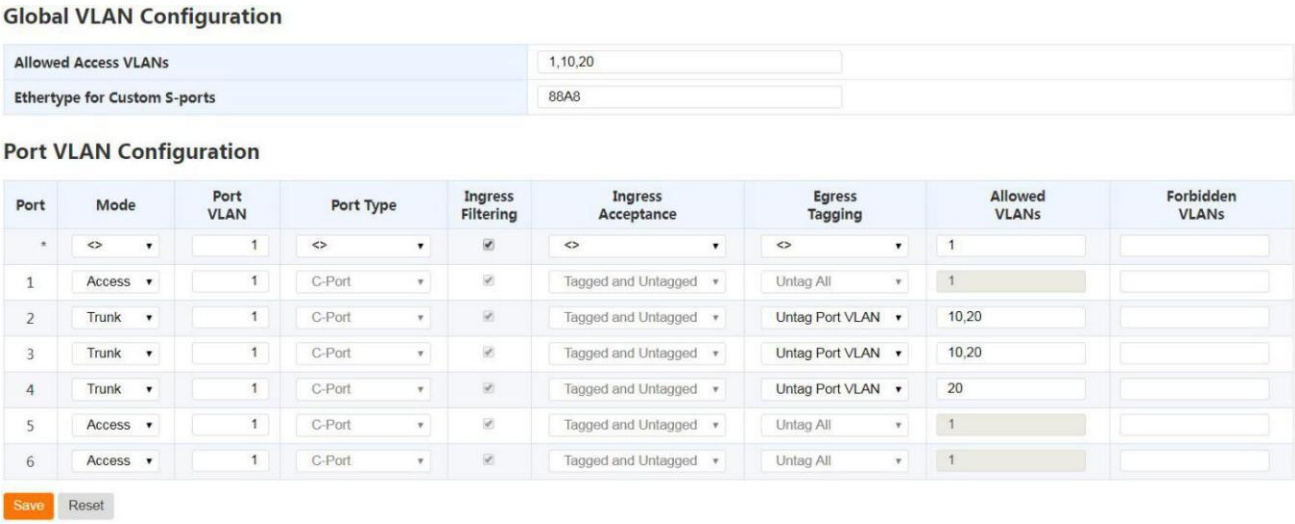
In the navigation bar, select: Configuration -> Spanning Tree -> CIST Port, configure ports 2, 3, and 4 as STP enabled state.

Chart Figure 8-22 MSTP case Switch C CIST port configuration

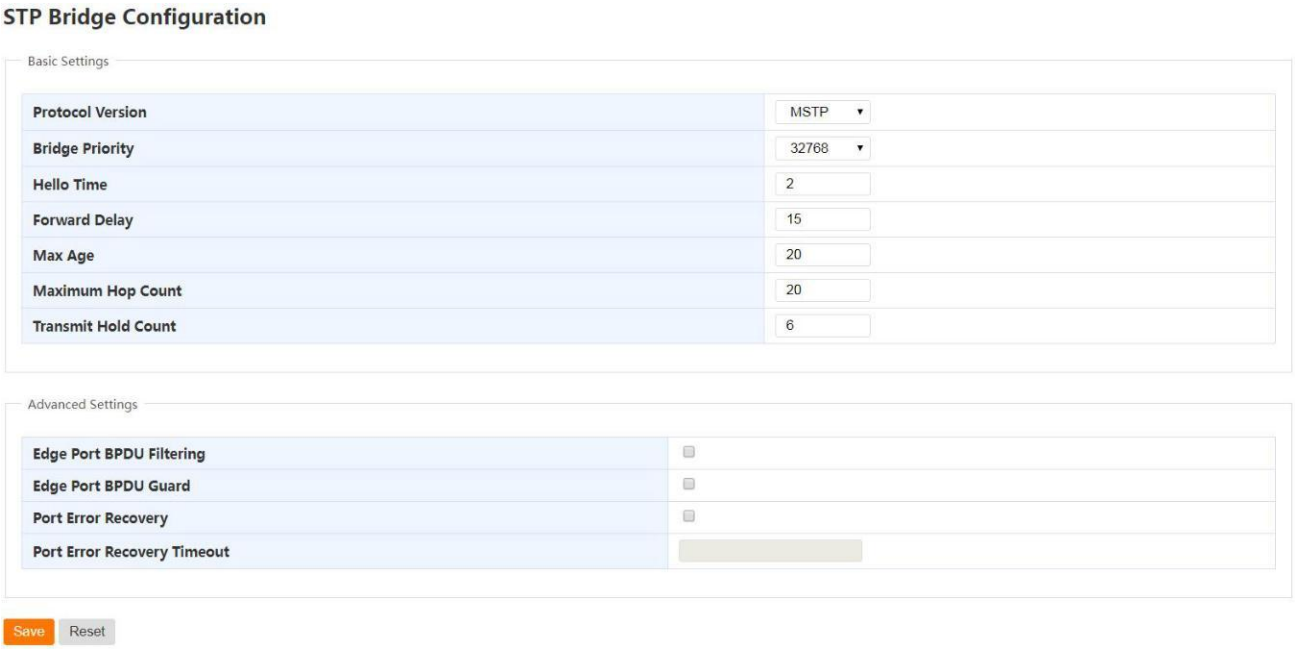


8.3.5 Configure Switch D

Step 1: Configure VLAN and port.
In the navigation bar, select: Configuration -> VLAN, configure ports 2, 3, and 4 as trunk ports, configure the corresponding allow vlan, and click the [Save] button to save the configuration.
Chart Figure 8-23 MSTP case Switch D VLAN configuration



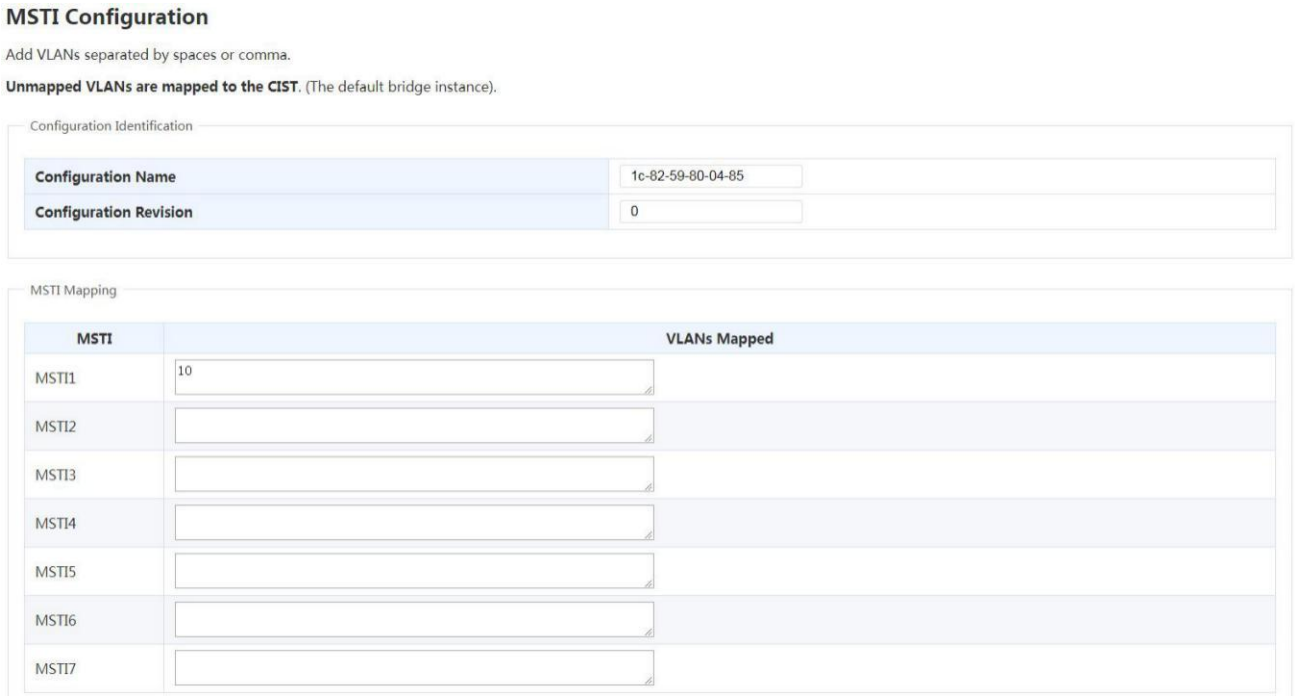
Step 2: Configure spanning tree bridge parameters.
In the navigation bar, select: Configuration -> Spanning Tree -> Bridge Settings, configure the protocol version as MSTP, and click the [Save] button to save the configuration.
Chart Figure 8-24 MSTP case Switch D bridge configuration



Step 3: Configure spanning tree MSTI mapping.

In the navigation bar, select: Configuration -> Spanning Tree -> MSTI Mapping, configure VLAN 10 to be mapped to MSTI 1, and click the [Save] button to save the configuration.

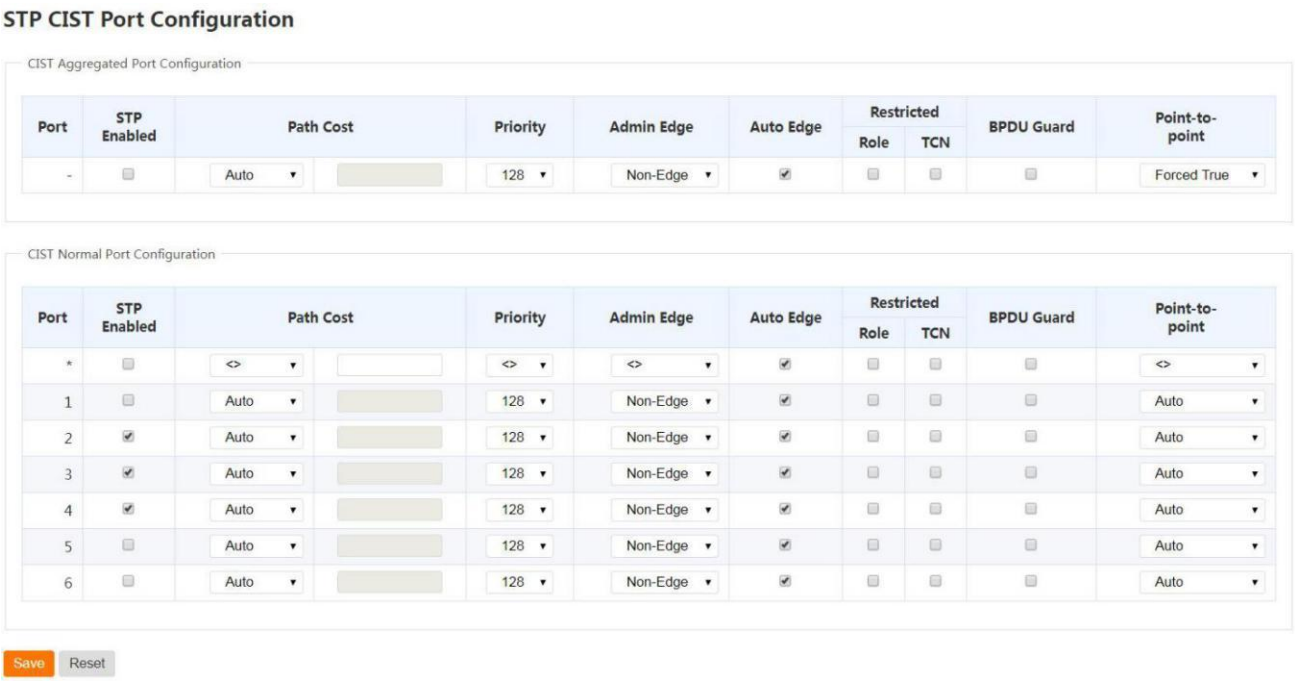
Chart Figure 8-25 MSTP case Switch D MSTI mapping configuration



Step 3: Configure the port to enable Spanning Tree Protocol.

In the navigation bar, select: Configuration -> Spanning Tree -> CIST Port, configure ports 2, 3, and 4 as STP enabled state.

Chart Figure 8-26 MSTP case Switch D CIST port configuration



8.4 CLI reference commands

Command	switch(config)# spanning-tree mode mstp switch(config)# spanning-tree mst 0 priority 32768 switch(config)# spanning-tree mst hello-time 2 switch(config)# spanning-tree mst max-age 20 forward-time 15 switch(config)# spanning-tree mst max-hops 20 switch(config)# spanning-tree transmit hold-count 6
Description	Configure the spanning tree protocol version; Configure the spanning tree CIST/MSTI priority; Configure the period of the spanning tree hello message; Configure the maximum duration and delay time of the spanning tree; Configure the maximum number of hops in the MST region of the spanning tree; Configure the maximum number of BPDU packets sent per second for spanning tree;

Command	switch(config)# spanning-tree edge bpdu-filter switch(config)# no spanning-tree edge bpdu-filter switch(config)# spanning-tree edge bpdu-guard switch(config)# no spanning-tree edge bpdu-guard switch(config)# spanning-tree recovery interval 33 switch(config)# no spanning-tree recovery interval
Description	Configure spanning tree to enable edge port BPDU filtering; Configure spanning tree to close edge port BPDU filtering; Configure spanning tree to enable edge port BPDU protection; Configure spanning tree to close the edge port BPDU protection; Configure spanning tree open port error recovery and recovery timeout time;

	Configure spanning tree shutdown port error recovery;

Command	switch(config)# spanning-tree mst name global revision 0 switch(config)# spanning-tree mst 3 vlan 1-10 switch(config)# spanning-tree edge bpdu-guard switch(config)# no spanning-tree edge bpdu-guard switch(config)# spanning-tree recovery interval 33 switch(config)# no spanning-tree recovery interval
Description	Configure the MSTI domain configuration name and version of the spanning tree; Configure spanning tree MSTI VLAN mapping;

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# spanning-tree switch(config-if)# no spanning-tree switch(config-if)# spanning-tree mst 0 cost auto switch(config-if)# spanning-tree mst 1 port-priority 32 switch(config-if)# spanning-tree edge switch(config-if)# no spanning-tree edge switch(config-if)# spanning-tree auto-edge switch(config-if)# no spanning-tree auto-edge switch(config-if)# spanning-tree restricted-role switch(config-if)# no spanning-tree restricted-role switch(config-if)# spanning-tree restricted-tcn switch(config-if)# no spanning-tree restricted-tcn switch(config-if)# spanning-tree bpdu-guard switch(config-if)# no spanning-tree bpdu-guard switch(config-if)# spanning-tree link-type point-to-point
Description	Configure the port to enable spanning tree; Configure the port to close the spanning tree; Configure port spanning tree CIST/MSTI path cost; Configure port spanning tree CIST/MSTI priority; Configure the port to open the spanning tree to force the edge; Configure the port to close the spanning tree to force the edge; Configure the port to enable the automatic edge of spanning tree; Configure the port to close the automatic edge of spanning tree; Configure the port to enable the restricted role of spanning tree; Configure the port to close the restricted role of spanning tree; Configure port to enable spanning tree restricted TCN; Configure the port to close the spanning tree restricted TCN; Configure the port to enable spanning tree BPDU protection; Configure the port to disable spanning tree BPDU protection;

	Configure the port to configure the spanning tree link mode;

Command	switch# show spanning-tree active switch# show spanning-tree interface GigabitEthernet 1/3 switch# show spanning-tree detail
Description	Print the status of the spanning tree bridge; Print the port status of the spanning tree; Print spanning tree port statistics;

9 IPMC

9.1 IPMC Profile

IPMC Profile is used to control access to IP multicast streams. Each configuration table is composed of several rules. The rules are stored in order. The rules complete the matching of IGMP Report messages by associating address table entries. Configure the association to the multicast configuration table based on the port. The IGMP Report message input to the port is searched for the rules of the associated multicast configuration table in turn, and the processing behavior is determined according to the first matching rule. If the corresponding behavior is "Deny", filtering is performed to achieve the purpose of access control to the downstream port of the IP multicast stream. The entire configuration process is as follows:

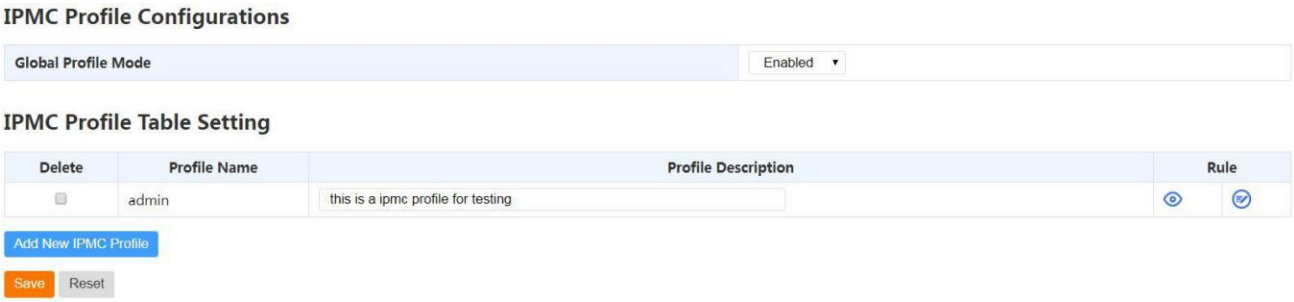
- Configure address table items: see the chapter "Address Table Items".
- Configuration configuration table: see "Configuration Table" chapter.
- Associated configuration table: Refer to the "Multicast->IGMP Snooping->Configuration->Port Filtering" chapter.

9.1.1 Configuration table

A maximum of 64 multicast configuration tables can be created, and a maximum of 128 rules can be set for each multicast configuration table.

9.1.1.1 Configuration table configuration

In the [Navigation Bar] drop-down menu, select: Configuration -> Multicast Configuration Table -> Configuration Table to enter the configuration table configuration page.
Chart Figure 9-1 Multicast configuration table configuration



- Global mode:

  Enable/disable the global IPMC configuration table. Only when the global configuration table is enabled, the system will start filtering based on the configuration table settings.
- Configuration table settings:

Item	Description
Delete	The specified configuration table will be deleted the next time it is saved.
Configuration table name	The name used to index the configuration table. Each entry has a unique name and can contain up to 16 alphanumeric characters. At least one letter
Configuration table description	Additional description about the configuration file, which can contain up to 64 characters.
Rule	After creating the configuration table, click the Edit button to enter the rule setting page of the specified configuration table. Clicking the View button will display a summary of the specified configuration table. View button: List the rules of the specified configuration table. Edit button: Edit and specify the rules of the configuration table..

Click the "Add New Configuration Table" button to create a new configuration table.

9.1.1.2 Rule configuration.

The configured rule entries are displayed in order of priority. The first rule entry has the highest priority in the search, and the last rule entry has the lowest priority in the search.
Click the Edit button on the configuration table page to enter the rule configuration page.
Chart Figure 9-2 Multicast configuration table rule settings.

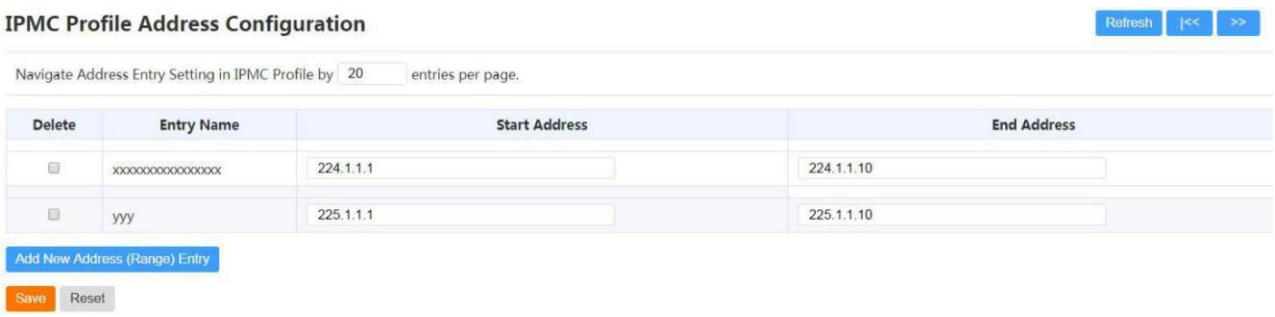
Item	Description
Configuration table name &	The name of the specified configuration table to be associated and the index corresponding to the rule. This field is not editable.

index	
Address table entry name	Used to specify the name of the address table entry used for this rule. Only select existing configuration table address entries in the selected box. When saving the rule, it is not allowed to select None ("-") in this field.
Address range	The address range corresponding to the selected configuration table address entry. This field is not editable and will be automatically adjusted according to the selected address table entry.
Behavior	Represents the learning operation of the IGMP Report frame where the received group address matches the address range of the rule. ➢ Permit: Allow learning. To ➢ Deny: It is forbidden to study.
Log	Indicates the logging preference of the IGMP Report frame where the received group address matches the address range of the rule. ➢ Enable: The corresponding information of the group address matching the range specified in the rule will be recorded. To ➢ DIsable: The corresponding information of the group address that matches the range specified in the rule will not be recorded.
Rule management button	You can use the following buttons to manage the rules and the corresponding priority order : Insert a new rule before the current rule. : Delete the current rule. : Move the current rule up in the list. : Move the current rule down in the list.

Click the "Add Rule (End)" button to add a new rule at the end of the list.

9.1.2 Address table entry

Up to 128 address table entries can be created, and each table entry can define a multicast address range, which is used to associate the rules of the multicast configuration table, and is used to match packets during rule search.
In the [Navigation Bar] drop-down menu, select: Configuration -> Multicast Configuration Table -> Address Table Item to enter the multicast configuration table address table item configuration page.
Chart Figure 9-3 Multicast configuration table address entry configuration



Item	Description
Delete	The specified address table entry will be deleted the next time it is saved.
Entry name	The name used to index the address table entry. Each entry has a unique name, which can contain up to 16 alphanumeric characters. At least one letter.
Start address	The IP multicast group address that will be used as the start of the address range.
End address	Will be used as the ending IP multicast group address of the address range.

Click the "Add new address table entry" button to add a new address table entry.

9.1.3 CLI Reference command

Command	switch(config)# ipmc profile switch(config)# no ipmc profile
Description	Configure the multicast configuration table to be globally enabled; Configure the multicast configuration table to be closed globally

Command	switch(config)# ipmc range config1 224.1.1.1 224.1.1.10 switch(config)# no ipmc range config2
Description	Configure the multicast add address table; Configure the multicast delete address table;

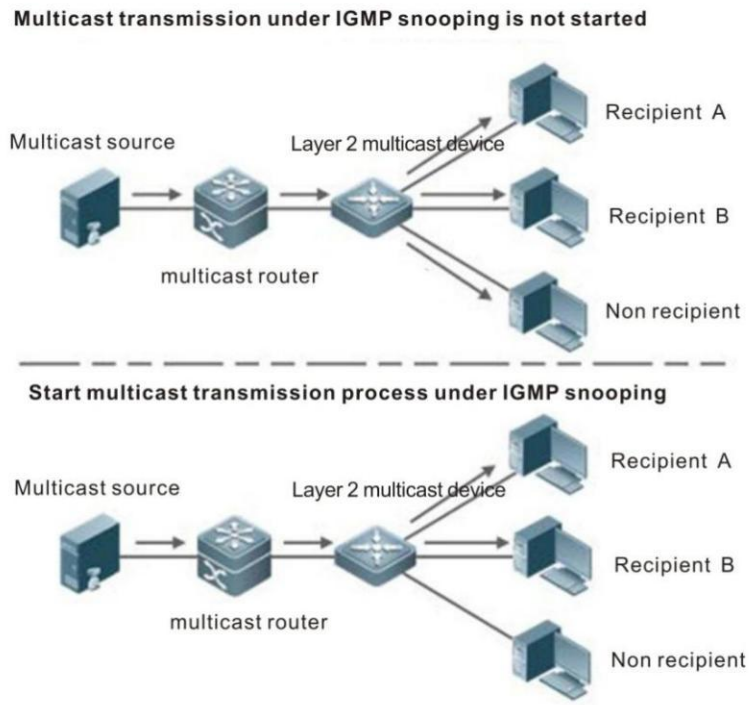
Command	switch(config)# ipmc profile table1 switch(config-ipmc-profile)#description description1 switch(config-ipmc-profile)#range config1 deny log switch(config-ipmc-profile)#range config2 permit next config1 switch(config-ipmc-profile)#no range config2
Description	Create/enter configuration table; Configure the multicast configuration table description; Configure the multicast configuration table to add the address table rule config1, the behavior is deny and logging is enabled; Configure the multicast configuration table to add the address table rule config2, the behavior is permit and the priority is after config1; Configure the multicast configuration table to delete the address table rules;

Command	switch# show ipmc profile switch# show ipmc range
Description	Print the status of the multicast configuration table; Print the status of the multicast address table;

9.2 IGMP Snooping

9.2.1 Overview

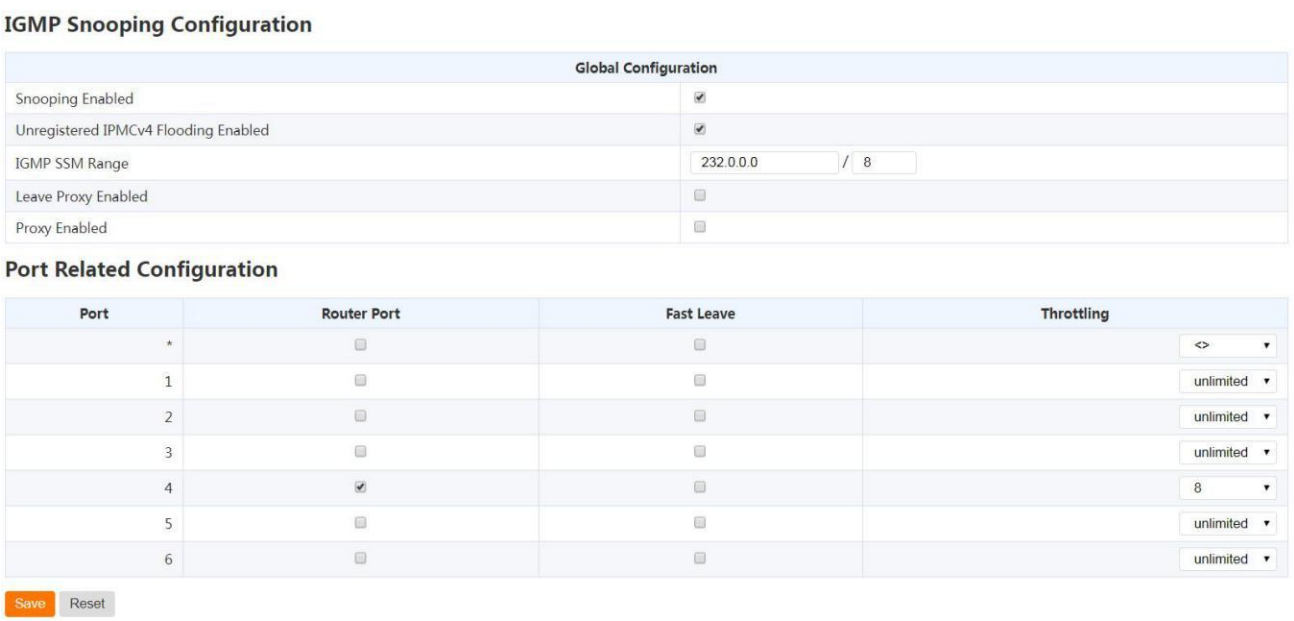
IGMP Snooping is the abbreviation of Internet Group Management Protocol Snooping (Internet Group Management Protocol Snooping). It is a multicast restriction mechanism running on Layer 2 devices and is used to manage and control multicast groups.
A Layer 2 device running IGMP Snooping analyzes the received IGMP messages, establishes a mapping relationship between ports and MAC multicast addresses, and forwards multicast data according to this mapping relationship. When the Layer 2 device is not running IGMP Snooping, the multicast data is broadcast at Layer 2. When the Layer 2 device is running IGMP Snooping, it is known that the multicast data of the multicast group will not be broadcast at Layer 2, but at Layer 2. It is multicast to the designated recipients.
As shown in the figure below, when the Layer 2 multicast device is not running IGMP Snooping, IP multicast packets are broadcast in the VLAN; when the Layer 2 multicast device is running IGMP Snooping, IP multicast packets are only sent to group members Receiver.
Chart Figure 9-4 IGMP Snooping multicast transmission process



9.2.2 Configuration

9.2.2.1 Basis

In the [Navigation Bar] drop-down menu, select: Configuration->Multicast->IGMP Snooping->Basics to enter the configuration page.
Chart Figure 9-5 IGMP Snooping basic configuration



- Global configuration

Item	Description
Snooping enable	Check the entry to enable IGMP Snooping globally.
Unregistered IPMCV4 packet flooding enable	Enable the flooding function of unregistered IPMCv4 packets. The flooding enable control only takes effect when IGMP Snooping is enabled. When IGMP Snooping is disabled, despite this setting, unregistered IPMCv4 messages can always be flooded.
IGMP SSM scope	The SSM (Source Specific Multicast) range allows SSM-aware hosts and routers to run the SSM service model for groups within the address range. Assign a valid IPv4 multicast address as a prefix, and specify the prefix length (from 4 to 32) for the range.
Leave agent enable	Enable IGMP leave agent. This function can be used to avoid forwarding unnecessary Leave messages to the router.
Proxy enable	Enable IGMP proxy. This function can be used to avoid forwarding unnecessary Join and Leave messages to the router.

- Port configuration

Item	Description
Port	Panel port number
Router port	Specify which ports act as router ports. The router port is a port on the Ethernet switch, leading to the Layer 3 multicast device or IGMP Querier (IGMP Querier). If the aggregation member port is selected as the router port, the entire aggregation port will act as the router port.
Leave quickly	Enable the port quick leave function. After this function is enabled, the system will delete the group record and stop forwarding data when receiving the IGMPv2 leave message, instead of sending the last member query message. It is recommended to enable this function only when a single IGMPv2 host is

	connected to a specific port.
Multicast number limit	Limit the number of multicast groups that a port can belong to. It can also be configured as unlimited.

9.2.2.2 VLAN

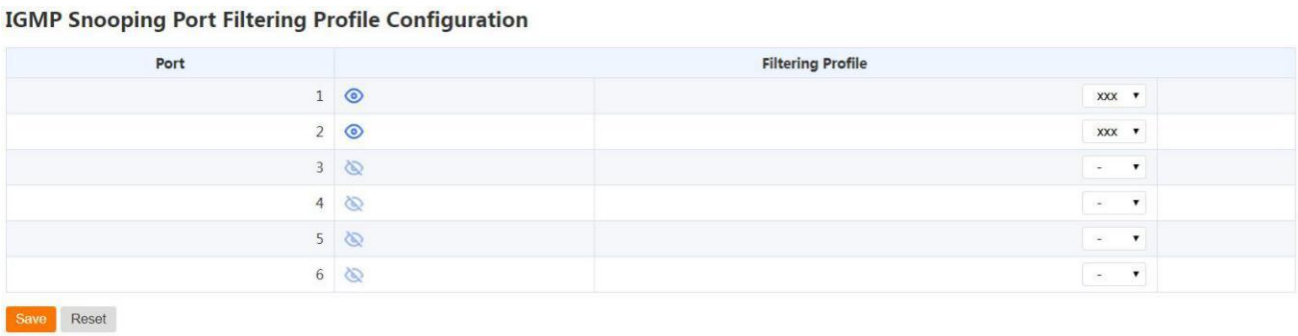
The VLAN shown in the figure below is the VLAN for which SVI has been created. For details, refer to the chapter "Configuring IP". If the corresponding SVI is deleted, the IGMP Snooping configuration on it will be deleted automatically.
In the [Navigation Bar] drop-down menu, select: Configuration->Multicast->IGMP Snooping->VLAN to enter the configuration page.
Chart Figure 9-6 IGMP Snooping VLAN configuration

Item	Description
VLAN ID	The VLAN ID of the IGMP VLAN interface (SVI port).
Snooping enable	Enable the Snooping function based on the SVI port, and open up to 8 SVI ports.
Querier campaign	Checking means that this VLAN allows this device to participate in the IGMP Querier election. If it is not checked, it can only be used as an IGMP Non-Querier device.
Querier address	Set the source address used in the IGMP Querier IP header. When the Querier address is not set, the system uses the IPv4 management address of the SVI interface. If the SVI does not set an IPv4 management address, the system uses the first available IPv4 management address. Otherwise, the system uses the predefined value. By default, this value is 192.168.1.234.
Compatibility	Hosts and routers take appropriate actions to maintain compatibility, depending on the version of IGMP running on the hosts and routers in the network. The allowed options are IGMP-Auto, mandatory IGMPv1, mandatory IGMPv2, and mandatory IGMPv3. The default compatibility value is IGMP-Auto.
Priority (PRI)	SVI interface priority. It represents the priority of IGMP control frames generated by the system. These values can be used to prioritize different types of traffic. The allowed range is 0-7, and the default interface priority value is 0.
Robustness Variable (RV)	Adjust the expected number of packet losses on the network. The allowed range is 1-255, and the default robustness variable value is 2.
Query interval (QI)	The query interval is the interval between regular queries sent by Querier. The unit is seconds, the allowed range is 1-31744, and the default query

	interval is 125, that is, 125 seconds
Query response interval（QRI）	The query response interval is used to calculate the maximum response time inserted into periodic regular queries. The unit is 0.1 seconds, the allowed range is 0-31744, and the default query response interval is 100, which is 10 seconds.
Last member query interval（LLQI）	The last member query time is the time value represented by the last member query interval, multiplied by the last member query count. The unit is 0.1 seconds, the allowed range is 0-31744, and the default interval for the last member query is 10, which is 1 second
Unsolicited reporting interval（URI）	The unsolicited report interval is the time between repeated reports when the host first became a member of the group. The unit is 1 second, the allowed range is 0-31744, and the default unsolicited report interval is 1, which is 1 second.

9.2.2.3 Port filtering

Port filtering is accomplished by associating the multicast configuration table on the port. The multicast configuration table is configured with a series of processing behaviors (Permit or Deny) for a range of multicast addresses through rules. If the corresponding behavior is Deny, then the entry from the port The corresponding Report message (as Join) will be discarded. For the configuration of the multicast configuration table, please refer to the "Multicast Configuration Table" chapter.
In the [Navigation Bar] drop-down menu, select: Configuration->Multicast->IGMP Snooping->Port Filtering to enter the configuration page.
Chart Figure 9-7 IGMP Snooping port filtering configuration



Item	Description
Port	Panel port number
Multicast configuration table	Select the IPMC configuration table as the filter condition for the corresponding port.
	Click to list the rules of the associated configuration table. No display when the configuration table is not associated.

9.2.3 Display

9.2.3.1 Status

In the [Navigation Bar] drop-down menu, select: Monitoring->Multicast->IGMP Snooping->Status to enter the display page.

Chart Figure 9-8 IGMP Snooping status display

- Statistics

Item	Description
VLAN ID	VLAN ID of the IGMP SVI interface.
Querier version	Corresponds to the version of the VLAN activity Querier.
Host version	Corresponding to the version of the VLAN working host.
Querier status	The status of the querier is displayed as "ACTIVE" or "IDLE". If it is "DISABLE", it means that the management status of the corresponding SVI port is Down.
Query message sending	The number of IGMP Query messages sent by the corresponding VLAN.
Query message reception	The number of IGMP Query messages received by the corresponding VLAN.
V1 request message reception	The number of IGMPV1 Report messages received by the corresponding VLAN.
V2 request message reception	The number of IGMPV2 Report messages received by the corresponding VLAN.
V3 request message reception	The number of IGMPV3 Report messages received by the corresponding VLAN.
V2 leave message reception	The number of IGMPV2 Leave messages received by the corresponding VLAN.

- Router port

Item	Description
Port	Panel port number

Status	Show which ports act as router ports. The router port is the port on the Ethernet switch that leads to the Layer 3 multicast device or IGMP Querier. ➢ Static indicates that the specific port is configured as a router port. ➢ Dynamic means that a specific port is learned as a router port. ➢ Both means that the specific port has been configured or learned as a router port.

9.2.3.2 Group information

In the [Navigation Bar] drop-down menu, select: Monitoring->Multicast->IGMP Snooping->Group Information to enter the display page.

Chart Figure 9-9 IGMP Snooping group information

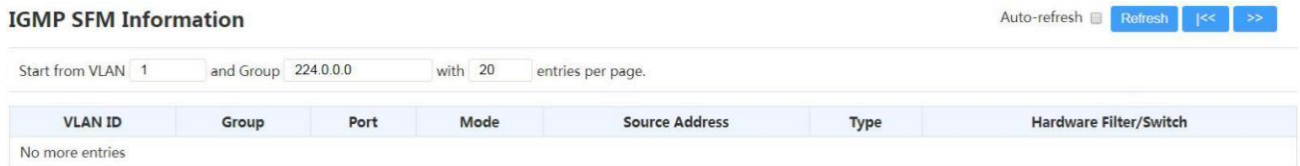
Item	Description
VLAN ID	VLAN VLAN to which the corresponding group belongs
Group	Multicast address of the corresponding group
Port member	Downstream port of the corresponding group

9.2.3.3 Source filtered multicast

The IGMP SFM (Source Filtered Multicast) information table also contains SSM (Source Specific Multicast) information. The table is sorted first by VLAN ID, then by group, and then by port. Different source addresses belonging to the same group are treated as a single entry.

In the [Navigation Bar] drop-down menu, select: Monitoring->Multicast->IGMP Snooping->Source Filtering Multicast to enter the display page.

Chart Figure 9-10 IGMP Snooping Source Filtering Multicast



Item	Description
VLAN ID	VLAN to which the corresponding group belongs
Group	Multicast address of the corresponding group
Port	Downstream port of the corresponding group
Mode	Filter mode based on (VLAN ID, group address, port).

	➢ Exclude: The multicast stream whose source IP belongs to the source address list is filtered. (If the source address is none, it means that all sources are allowed). ➢ Include: Multicast streams whose source IP belongs to the source address list are allowed, and those whose source IP does not belong to the source address list are filtered. (SSM is in this case)
Source address	Currently, the maximum number of IPv4 source addresses (per group) used for filtering is 8. When there is no source filtering address, the text "None" is displayed in the source address field.
Type	Indicates whether to filter or allow, which is strongly related to the mode value. When the mode is Exclude, the type is Deny, which means to filter the multicast streams whose source IP belongs to the source address list. When the mode is Include, the type is Allow, which means that multicast streams whose source IP belongs to the source address list are allowed to be forwarded.
Hardware filtering/forwarding	Indicates whether the hardware supports filtering or forwarding of multicast streams. Yes means support; No means that it is not supported and is completed by the software.

9.2.4 CLI Reference command

Command	switch(config)# ip igmp snooping switch(config)# no ip igmp snooping switch(config)# ip igmp unknown-flooding switch(config)# no ip igmp unknown-flooding switch(config)# ip igmp ssm-range 232.0.0.0 8 switch(config)# ip igmp host-proxy switch(config)# no ip igmp host-proxy switch(config)# ip igmp host-proxy leave-proxy switch(config)# no ip igmp host-proxy leave-proxy
Description	Configure IGMP Snooping to open; Configure IGMP Snooping to close; Configure IGMP unregistered IPMCV4 message flooding to start; Configure IGMP unregistered IPMCV4 message flooding to close; Configure IGMP SSM range; Configure IGMP proxy to open; Configure IGMP proxy to close; Configure IGMP leave agent to open; Configure the IGMP leave agent to close;

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# ip igmp snooping mrouter switch(config-if)# no ip igmp snooping mrouter switch(config-if)# ip igmp snooping immediate-leave switch(config-if)# no ip igmp snooping immediate-leave switch(config-if)# ip igmp snooping max-groups 4 switch(config-if)# ip igmp snooping filter table1
Description	Configure the port to enable the IGMP Snooping router port; Configure the port to close the IGMP Snooping router port; Configure the port to enable IGMP Snooping fast leave; Configure the port to close IGMP Snooping fast leave; Configure port IGMP Snooping multicast limit; Configure port IGMP Snooping port filtering function (associated with multicast configuration table);

Command	switch(config)# interface vlan 10
Description	Enter the IP interface of Vlan;

Command	switch(config-if)# ip igmp snooping switch(config-if)# no ip igmp snooping switch(config-if)# ip igmp snooping querier election switch(config-if)# no ip igmp snooping querier election switch(config-if)# ip igmp snooping querier address 192.168.1.1 switch(config-if)# ip igmp snooping compatibility auto switch(config-if)# ip igmp snooping priority 1 switch(config-if)# ip igmp snooping robustness-variable 2 switch(config-if)# ip igmp snooping query-interval 125 switch(config-if)# ip igmp snooping query-max-response-time 100 switch(config-if)# ip igmp snooping last-member-query-interval 10 switch(config-if)# ip igmp snooping unsolicited-report-interval 1
Description	Configure SVI to enable IGMP Snooping; Configure SVI to close IGMP Snooping; Configure SVI to start IGMP Snooping Querier election; Configure SVI to close the IGMP Snooping Querier election; Configure the SVI IGMP Snooping Querier address; Configure SVI IGMP Snooping compatible version; Configure SVI IGMP Snooping control frame priority; Configure SVI IGMP Snooping robustness variables; Configure SVI IGMP Snooping query interval; Configure SVI IGMP Snooping query response interval; Configure the last member query interval of SVI IGMP Snooping; Configure the unsolicited report interval of SVI IGMP Snooping;

Command	switch# show ip igmp snooping detail switch# show ip igmp snooping group-database detail switch# show ip igmp snooping group-database sfm-information

Description	Print IGMP Snooping status; Print IGMP Snooping group members; Print IGMP Snooping source to filter multicast;

10 LLDP

10.1 Overview

LLDP (Link Layer Discovery Protocol) is a link layer discovery protocol defined by IEEE 802.1AB. Through the LLDP protocol, it is possible to discover the topology and grasp the changes of the topology. LLDP organizes the local information of the device into TLV format (Type/Length/Value, type/length/value) and encapsulates it in LLDPDU (LLDP data unit, link layer discovery protocol data unit) and sends it to the neighboring device. At the same time, it sends it to the neighboring device. The LLDPDU sent by the device is stored in the form of MIB (Management Information Base) and provided to the network management system for access.

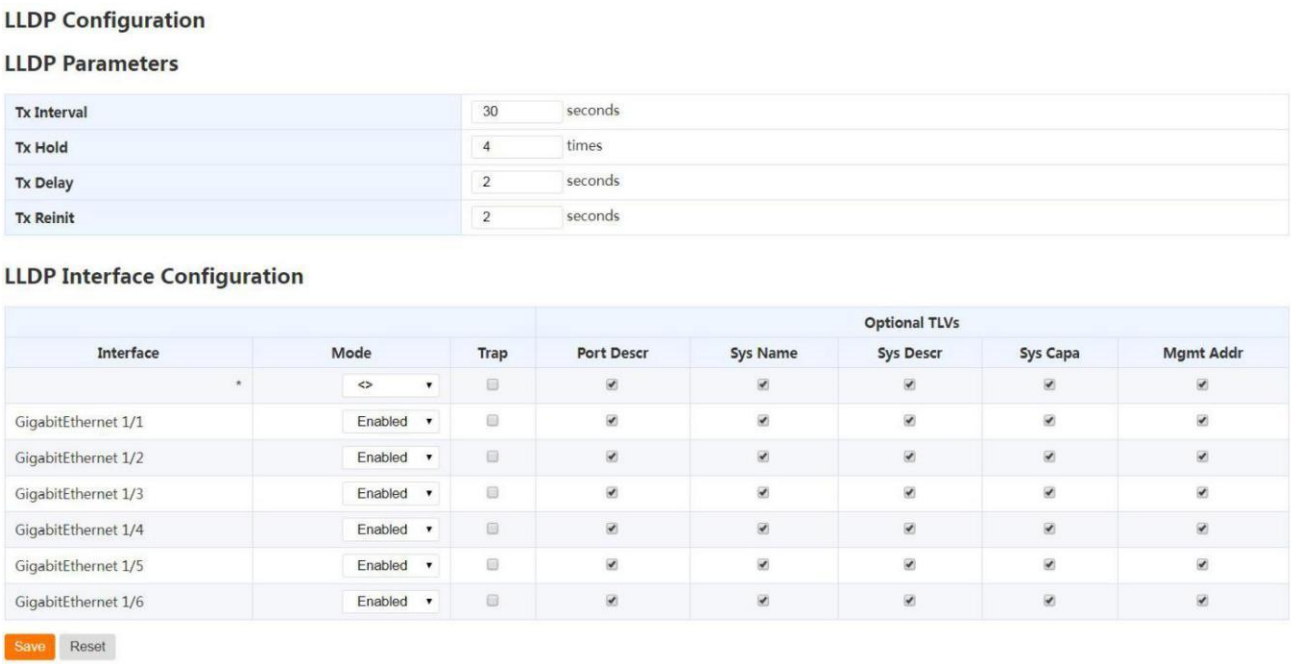
Through LLDP, the network management system can grasp the connection status of the topology, such as which ports of the device are connected to other devices, the speed of the ports at both ends of the link connection, and whether the duplex is matched, etc. The administrator can quickly locate and troubleshoot based on this information malfunction.

LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) is an extension of LLDP that works between endpoint devices (such as IP phones). It especially provides support for Voice over IP (Voice over IP) applications, and provides additional TLVs for capability discovery, network strategy, power over Ethernet, address information, etc. By default, all LLDP-MED TLVs are enabled.

10.2 Configuration

10.2.1 LLDP

In the [Navigation Bar] drop-down menu, select: Configuration->LLDP->LLDP to enter the configuration page.
Figure 10-1 LLDP configuration



- LLDP parameter

Item	Description
Tx interval	The exchange sends the LLDP message periodically so that the information received by the neighbor is updated. This configuration item is used to control the period of transmission. It ranges from 5 to 32768 in seconds. The default value is 30.
Tx keep	The information in the LLDP packet is considered valid for a period of time called hold time, where hold time = TX hold * TX interval. Tx keeps the range from 2 to 10 in degrees, and the default value is 4.
Tx delay	When the configuration changes, a new LLDP packet needs to be sent, but the new LLDP packet is not sent immediately and must wait at least as long as the "TX delay" time. The TX delay time cannot exceed 1/4 of the TX interval time. The range is 1-8192 in seconds, the default value is 2.
Tx reinitialize	When LLDP is disabled, an LLDP SHUTDOWN message is sent to notify neighbors that the LLDP message is no longer valid and that there must be an interval between the LLDP reinitialization and the LLDP SHUTDOWN message. This is the configuration item. The range is 1-10 in seconds, and the default value is 2.

- Interface configuration

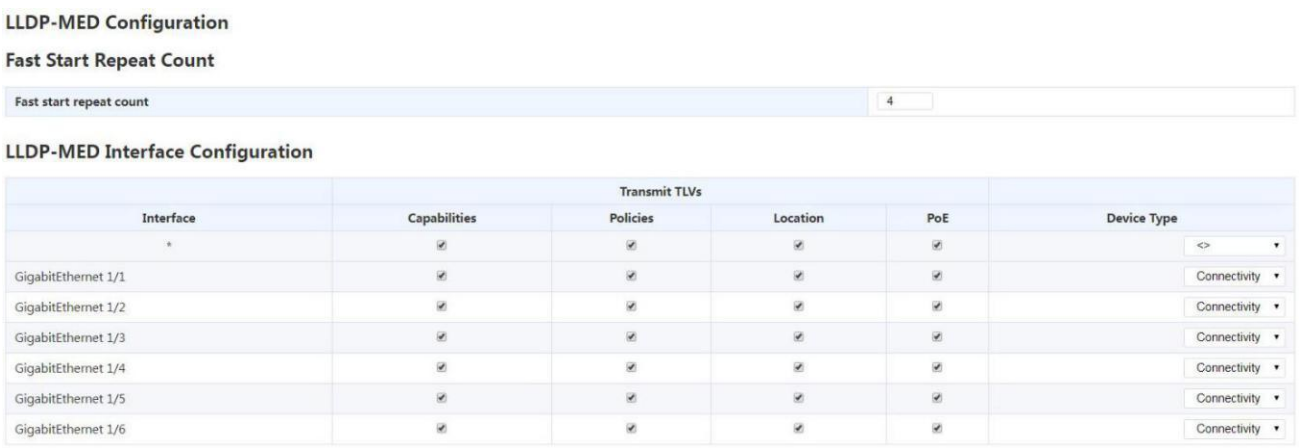
Item	Description
Interface	The interface name of a switch
model	➢ Rx only: the switch does not send LLDP information, but analyzes the LLDP information from the neighbor cell. ➢ TX only: The switch will discard the LLDP message received from the

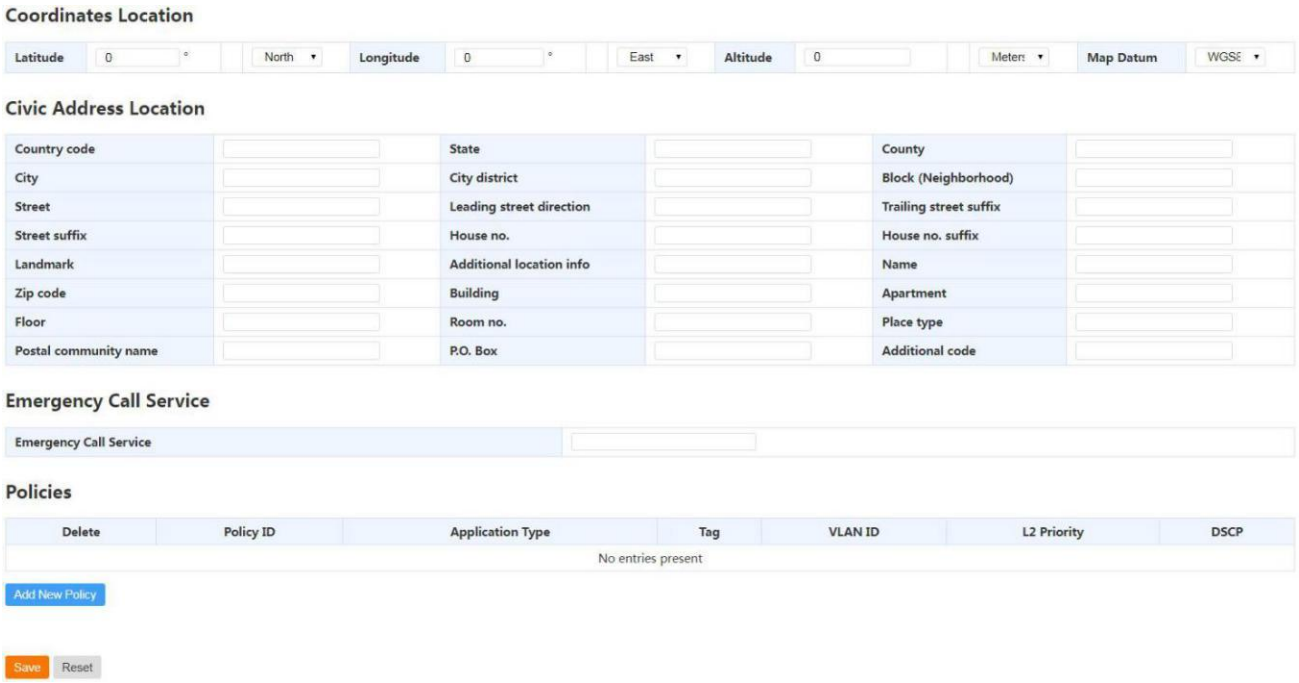
	neighbor, but will issue the LLDP message. ➢ Disabled: The switch will not send LLDP messages and will discard LLDP messages received from neighbors. ➢ Enable: The switch will issue LLDP messages and will analyze the LLDP messages received from neighbors.
Tracking	Whether LLDP-Trap function is enabled or not, this function is turned off by default. By configurable Trap function, LLDP information of the local device (such as the discovery of new neighbors, the detection of communication link failure with neighbors, etc.) can be sent to the network management server, according to which the administrator can monitor the running condition of the network.
Optional the TLV	The 5 types of TLV in the table are optional, and they are all enabled by default. Some TLV can be turned off by deselecting. The enabled TLV will be included in the transmitted LLDP packet.

10.2.2 LLDP-MED

In the [Navigation Bar] drop-down menu, select: Configuration->LLDP->LLDP-MED to enter the configuration page.

Chart Figure 10-2 LLDP-MED configuration





The emergency calling service and policy are related to Voice VLAN functionality and are not supported at this time. Therefore, the content is not described.

- Quick start repetition times

Network-connected devices will only transmit LLDP TLVs in LLDPDU.

Only after the LLDP-MED endpoint device is detected will network connected devices with LLDP-MED functionality begin to notify the LLDP-MED TLV in the LLDPPDU outgoing on the associated interface.

When a new LLDP-MED neighbor is detected, the LLDP-MED application will temporarily speed up the transmission of the LLDPDU, which will start in one second, so that LLDP-MED information can be shared with the new neighbor as soon as possible.

Since LLDP frames may be lost during transmission between neighbors, it is recommended that the transmission be started quickly and repeatedly to increase the likelihood that neighbors will receive LLDP frames.

Using the quick start repeat count, you can specify the number of times that the quick start transmission is repeated.

If an LLDP frame with new information is received, it is assumed that four LLDP frames are sent with an interval of one second, which is four times the recommended value.

It should be noted that the LLDP-MED and LLDP-MED quick start mechanisms are intended to operate only on links between LLDP-MED network connected devices and endpoint devices, and therefore do not apply to links between LAN infrastructure elements, including network connected devices or other types of links.

- Interface configuration

Item	Description
Interface	The interface name of the switch.
Transfer the	The four TLVs in the table are optional, and they are all enabled by default. A

TLV	TLV can be turned off by deselecting it. The enabled TLV will be included in the LLDP-MED message sent.
Device type	Any LLDP-MED device operates as a specific type of LLDP-MED device, either a Connectivity Device or an End-Point Device. ➢ The Network Connectivity Device is an LLDP-MED device that provides network access to LLDP-MED endpoint devices based on IEEE 802 LAN technology. ➢ Endpoint devices located at the edge of the network, based on IEEE802 LAN technology to provide IP communication services. The main difference between the networked and endpoint devices is that only the endpoint device can initiate the LLDP-MED information exchange. In general, a switch should always be a network connected device, but it can also be configured as a port device when connected to another switch and you want to initiate LLEP-MED information exchange.

■ Coordinate position

Item	Description
Dimension	Select "North" or "South", with values ranging from 0 to 90. Supports 4 decimal places.
Longitude	Select "East" or "West", with values ranging from 0 to 180. Supports 4 decimal places.
Sea level	Values range from -2097151.9 to 2097151.9, supporting 1 decimal place. Meters mean height above sea level. Floors denotes the height of the floor, or the altitude if it's outdoors, or inside, relative to the floor of the building.
Map data	WGS84: (Geographic 3D) - World Geodetic System 1984, CRS code 4327, Original Meridian Name: Greenwich. NAD83 / NAVD88: North American benchmark 1983, CRS code 4269, Meridian name: Greenwich; The relevant vertical datum is the North American vertical datum of 1988 (NAVD88). This reference pair will be used when referring to a position on land rather than near the tide (reference = NAD83 / MLLW will be used). NAD83 / MLLW: North American benchmark 1983, CRS code 4269, Meridian name: Greenwich; The associated vertical datum is the mean low water level (MLLW). This reference pair will be used when referring to water/sea/ocean locations.

■ Address Location

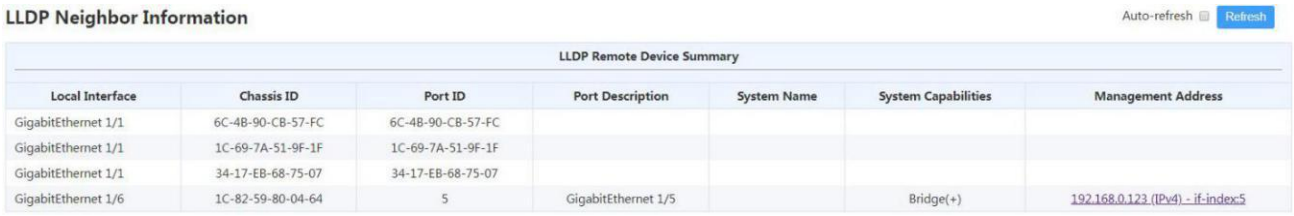
Location configuration information based on IETF citizen addresses.
The total number of characters in the combined public address information shall not exceed 250 characters.
Notes on the 250 character limit.

1) If more than one citizen address location is used, each citizen address location will add 2 extra characters to the citizen address location text.
2) A 2-letter country code does not fall under the 250-character limit.

10.3 Showing

10.3.1 LLDP neighbors

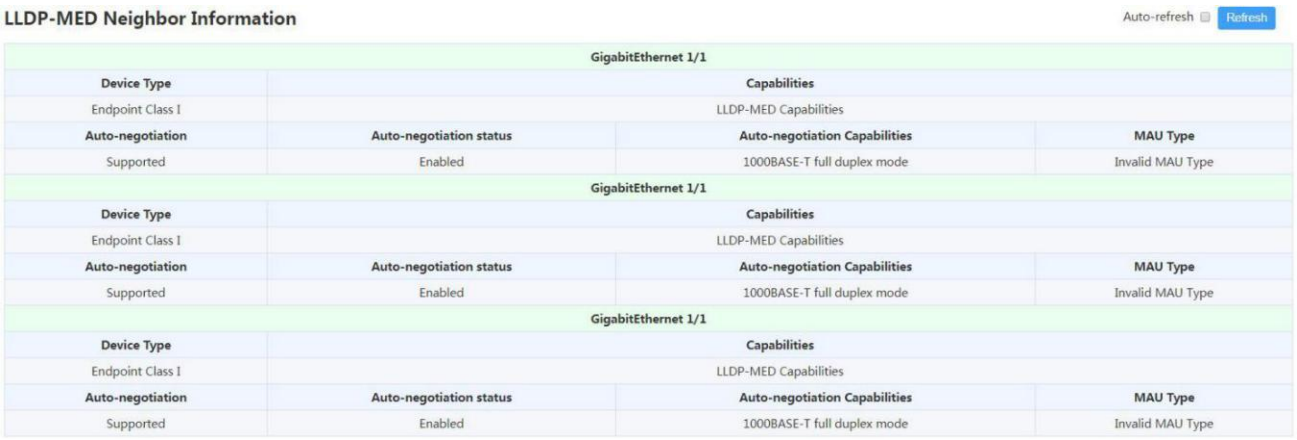
In the [Navigation Bar] drop-down menu, select: Monitor->LLDP->Neighbors to enter the display page.
Chart Figure 10-3 LLDP neighbor information



Item	Description
Local Interface	The name of the local interface that received the LLDP packet.
Device ID	The identity of the LLDP packet corresponding to the neighbor.
Port ID	The identity of the port information corresponding to the neighbor.
Port descriptor	Description of the port corresponding to the neighbor notification.
System name	The name of the system corresponding to the neighbor notification.
System capacity	Ability information corresponding to neighbor announcements.
Management address	The address of the corresponding neighbor unit is used for higher level entities to aid network management in discovery. For example, this can save a neighbor's IP address.

10.3.2 LLDP-MED neighbor

In the [Navigation Bar] drop-down menu, select: Monitor->LLDP->MED Neighbors to enter the display page.
Chart Figure 10-4 LLDP-MED neighbor information



LLDP-MED Neighbor Information

Auto-refresh Refresh

GigabitEthernet 1/1			
Device Type	**Capabilities**		
Endpoint Class I	LLDP-MED Capabilities		
Auto-negotiation	**Auto-negotiation status**	**Auto-negotiation Capabilities**	**MAU Type**
Supported	Enabled	1000BASE-T full duplex mode	Invalid MAU Type
GigabitEthernet 1/1			
Device Type	**Capabilities**		
Endpoint Class I	LLDP-MED Capabilities		
Auto-negotiation	**Auto-negotiation status**	**Auto-negotiation Capabilities**	**MAU Type**
Supported	Enabled	1000BASE-T full duplex mode	Invalid MAU Type
GigabitEthernet 1/1			
Device Type	**Capabilities**		
Endpoint Class I	LLDP-MED Capabilities		
Auto-negotiation	**Auto-negotiation status**	**Auto-negotiation Capabilities**	**MAU Type**
Supported	Enabled	1000BASE-T full duplex mode	Invalid MAU Type

Item	Description
Interface	The name of the local interface that received the LLDP packet
Device type	LLDP-MED devices consist of two main types of devices: network connected devices and endpoint devices. LLDP-MED Network Connectivity Devices: An LLDP-MED Network Connectivity Device as defined in TIA-1057 may be a LAN access device based on any of the following technologies: 1. LAN switches/routers 2. IEEE 802.1 Bridging 3. IEEE 802.3 transponders (included for historical reasons) 4. IEEE 802.11 wireless access point 5. Any device that supports IEEE 802.1AB and MED extensions as defined by TIA-1057 and can relay IEEE 802 frames by any means. LLDP-MED Endpoint Device: The LLDP-MED endpoint device as defined in TIA-1057 is located at the edge of an IEEE 802 LAN network and participates in IP communication services using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is divided into more endpoint device classes, as shown below. The definition of each LLDP-MED endpoint device class is based on the functionality defined for the previous endpoint device class. For example, any LLDP-MED endpoint device (Class II) that claims to comply with the Media Endpoint standard will also support all aspects of TIA-1057 for generic endpoints (Class I), and any LLDP-MED endpoint device that claims to comply as a communication device. (Class III) will also support all aspects of TIA-1057 for media endpoints (Class II) and generic endpoints (Class I). LLDP-MED Common Endpoints (Class I) The LLDP-MED Common Endpoint (Class I) definition applies to all endpoint products that require the basic LLDP discovery service defined in TIA-1057, but do not support IP media or act as an end-user communication device. Such devices may include (but are not limited to) IP communication controllers, other communications-related servers, or any devices that require the basic

	services defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management. LLDP-MED Media Endpoints (Class II) The LLDP-MED Media Endpoint (Class II) definition applies to all endpoint products with IP media capabilities, but may or may not be associated with a specific end user. The functionality includes all the functionality defined for the previous generic endpoint class (Class I) and has been extended to include aspects related to media streaming. Sample product categories that are expected to fit this category include (but are not limited to) voice/media gateways, conference Bridges, media servers, and more. Discovery services defined in this class include network layer policy discovery specific to media types. LLDP-MED Communication Endpoints (Class III) The LLDP-MED communication endpoints (Class III) definition applies to all endpoint products that act as end-user communication devices that support IP media. The functionality includes all the functionality defined previously for generic endpoints (Class I) and media endpoints (Class II), and has been extended to include aspects related to end-user devices. Sample product categories that are expected to fit into this category include, but are not limited to, end-user communications devices such as IP phones, PC-based softphones, or other communications devices that directly support end-users. Discovery services defined in this class include the provision of location identifiers (including ECS/E911 information), embedded L2 switch support, and inventory management.
Ability	Describes the LLDP-MED capabilities of neighbor units. Possible abilities are: 1. The LLDP - MED ability 2. Network strategy 3. Location recognition 4. Expand power supply through MDI-PSE 5. Expand the power supply through MDI-PD 6. Inventory 7. Keep
Self-negotiation	Automatic negotiation identifies whether a neighbor supports MAC/PHY auto negotiation.
Auto-negotiation status	Automatic negotiation status identifies whether automatic negotiation is currently enabled on a neighbor. If auto-negotiation support or auto-negotiation status is disabled, the operating mode of IEEE 802.3PMD will operate on the value of a field of type MAU rather than being determined by auto-negotiation.

Self-negotiation ability	The auto-negotiation feature shows the auto-negotiation capabilities of the neighbor's Mac/PHY.
MAU type	Shows the MAU type of the neighbor.

10.3.3 Ethernet power supply

This page is only available for switches that support Power over Ethernet.
In the [Navigation Bar] drop-down menu, select: Monitoring->LLDP->Power over Ethernet to enter the display page.
Chart Figure 10-5 LLDP Neighbor Power over Ethernet Information

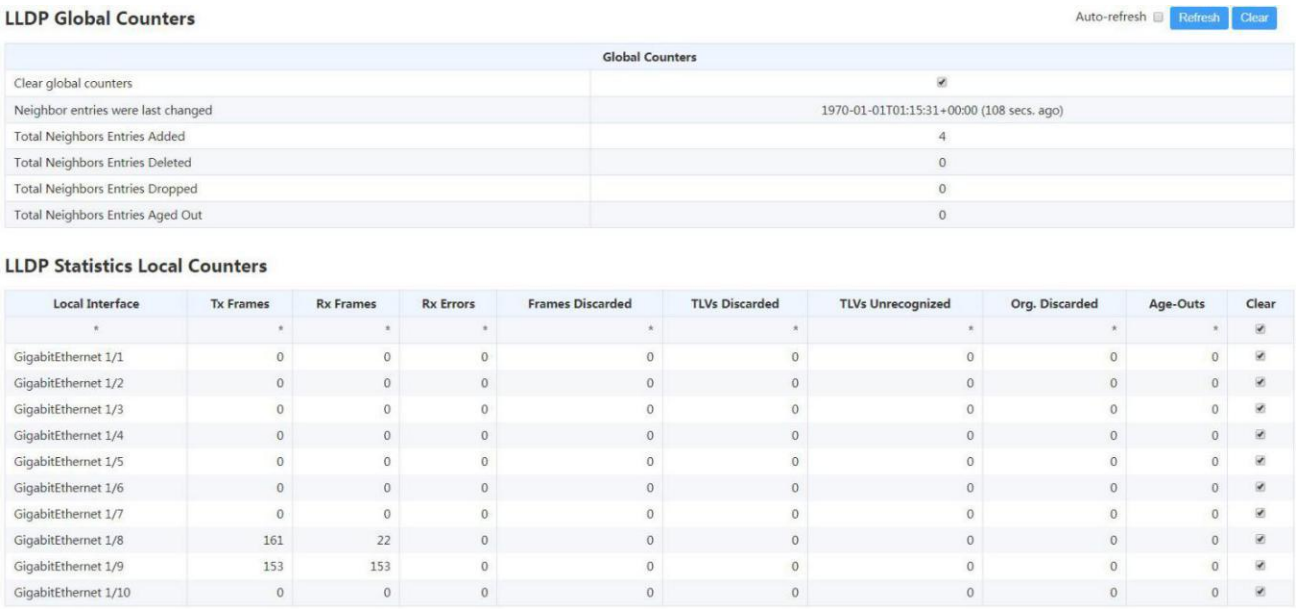
Item	Description
Local interface	The name of the local interface that received the LLDP packet.
Power source type	The power type indicates whether the device is a PSE device or a PD device, and if the power type is unknown, it is indicated as "reserved".
Source	In the case of a PSE device, the Power Source runs on its main or standby power supply. If it is not clear whether the PSE device is using its main or standby power supply, indicate it as "unknown". If the device is a PD device, it can be run using its local power supply, or it can use PSE as the power supply. It can also use both local power and PSE. If it is not clear which power source to use, indicate it as "unknown".
Power priority	Power Priority A power priority represents the priority of a PD device, or the power priority associated with the interface of a PSE-type device that is being powered. There are three levels of power priority. The three levels are: Critical, High, and Low. If the power priority is unknown, it is indicated as "unknown".
The most powerful	"Maximum power indicates the maximum power (in W) required by the PD device from the PSE device, or the minimum power that the PSE device can supply over the maximum length of cable based on its current configuration. The maximum allowable value is 102.3W.

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

10.3.4 Port statistics

In the [Navigation Bar] drop-down menu, select: Monitor->LLDP->Port Statistics to enter the display page.

Chart Figure 10-6 LLDP Statistics



- Global count

Item	Description
Clear global count	When selected, click the Clear button to clear the global count.
Last Update Time	Discounts when an entry was last deleted or added. It also shows how much time has elapsed since the last change was detected.
The number of added neighbors	Displays the number of entries added since the switch was restarted.
Number of neighbors deleted	Displays the number of entries that have been deleted since the switch was restarted.
Number of discarded neighbors	Displays the number of LLDP packets discarded because the entry table is full.
Number of aging neighbors	Discounts the number of entries that were deleted due to the expiration of the aging time.

- Local count

Item	Description
Local interface	The name of the local interface that receives or sends LLDP packets.
Send a message	Number of LLDP packets sent by the interface.

Receive a message	Number of LLDP packets received by the interface.
Receive error	Number of LLDP packets received by the interface that contained some kind of error.
Discarding the message	If an LLDP message is received on the interface and the internal table of the switch is full, the LLDP message is counted and discarded. This is called "too many neighbors" in the LLDP standard. If the table does not already contain a device ID or remote port ID, the LLDP message needs to add a new entry to the table. When a link for a given interface is broken, LLDP SHUTDOWN messages are received, or an entry is aged, the entry is removed from the table.
Discard the TLV	Each LLDP packet can contain multiple pieces of information, called TLV (TLV is short for "type length value"). If the TLV format is wrong, it is counted and discarded.
Unrecognized TLV	The number of properly formed TLVs with unknown type values.
Discarding the Org.	If the LLDP packet carries an Organizationally TLV, but the TLV is not supported, it is counted and discarded.
Number of aging	Each LLDP packet contains information about how long the LLDP message is valid (the timeout). If no new LLDP message is received within the valid time, the LLDP message is deleted and the number of aging increases.
Remove	When selected, click the "Clear" button to clear the local count of the corresponding interface.

10.4 CLI reference command

Command	switch(config)# lldp timer 20 switch(config)# lldp holdtime 5 switch(config)# lldp transmission-delay 3 switch(config)# lldp reinit 4 switch(config)# no lldp timer switch(config)# no lldp holdtime switch(config)# no lldp transmission-delay switch(config)# no lldp reinit
Description	Configure the LLDP send interval to be 20 seconds. Configure the LLDP send hold number to be 5. Configure the LLDP send delay to 3 seconds. Configure the LLDP send reinitialization time to be 4 seconds. Restore LLDP send interval to the default value of 30 seconds. Restore LLDP Send Hold to the default value of 4 times. Restores LLDP send delay to default value of 2 seconds. Restore LLDP send reinitialization time to the default value of 2 seconds.。

Command	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# lldp receive switch(config-if)# lldp transmit switch(config-if)# no lldp receive switch(config-if)# no lldp transmit
Description	Enables LLDP packet reception.(On by default) Enables LLDP message sending.(On by default) Turn off LLDP packet reception. Turn off LLDP message sending.

Command	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# lldp trap switch(config-if)# no lldp trap
Description	Open the LLDP Trap function. Turn off LLDP Trap.(Off by default)

Command	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# lldp tlv-select port-description switch(config-if)# lldp tlv-select system-name switch(config-if)# lldp tlv-select system-description switch(config-if)# lldp tlv-select system-capabilities switch(config-if)# lldp tlv-select management-address switch(config-if)# no lldp tlv-select port-description switch(config-if)# no lldp tlv-select system-name switch(config-if)# no lldp tlv-select system-description switch(config-if)# no lldp tlv-select system-capabilities switch(config-if)# no lldp tlv-select management-address
Description	Enable the LLDP optional TLV "Port Description".(On by default) Enable LLDP optional TLV "System Name".(On by default) Enable the LLDP optional TLV "System Description".(On by default) Enable the LLDP optional TLV "System Capabilities".(On by default) Enable the LLDP optional TLV "Manage Address".(On by default) Turn off the LLDP optional TLV "Port Description". Turn off the LLDP optional TLV "System Name". Turn off the LLDP optional TLV "System Description". Turn off the LLDP optional TLV "System Capability". Turn off the LLDP optional TLV "Admin Address".

Command	switch(config)# lldp med fast 5

	switch(config)# no lldp med fast
Description	The rapid start of LLDP-MED was repeated for 5 times. Restoring LLDP-MED quick start repeats to the default value of 4 times.

Command	switch(config)# lldp med location-tlv latitude north 33.2507 switch(config)# lldp med location-tlv longitude east 105.2371 switch(config)# lldp med location-tlv altitude meters 300.5 switch(config)# no lldp med location-tlv latitude switch(config)# no lldp med location-tlv longitude switch(config)# no lldp med location-tlv altitude
Description	LLDP-MED coordinate position - dimension: 33.2507 ° N LLDP-MED coordinate position - accuracy: 105.2371 degrees east longitude LLDP-MED coordinate position - Altitude: 330.5 m Value LLDP-MED coordinate position-dimension configuration.(Default: 0 ° N) Cancel the LLDP-MED coordinate position-precision configuration.(Default is 0 degrees east longitude) Cancel the LLDP-MED coordinate position-altitude configuration.(Default is 0 m)

Command	switch(config)# lldp med datum nad83-navd88 switch(config)# no lldp med datum
Description	The coordinate position data of LLDP-MED is configured as "NAD80-NAVD88". Cancel LLDP-MED coordinate location data configuration, default is "WGS84".

Command	switch(config)# lldp med location-tlv civic-addr *XXXX* switch(config)# no lldp med location-tlv civic-addr *XXXX*
Description	Configure the LLDP-MED address location.There are many parameters, not one list. Value LLDP-MED coordinate position-address location configuration.

Command	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# lldp med type end-point switch(config-if)# no lldp med type
Description	The LLDP-MED device type is configured as "end-point". Unconfigure the LLDP-MED device type.(Default "Connectivity")

Command	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# lldp med transmit-tlv capabilities switch(config-if)# lldp med transmit-tlv location switch(config-if)# lldp med transmit-tlv poe

	switch(config-if)# no lldp med transmit-tlv capabilities switch(config-if)# no lldp med transmit-tlv location switch(config-if)# no lldp med transmit-tlv poe
Description	Enable the LLDP-MED optional TLV "capability".(On by default) Turn on the LLDP-MED optional TLV "location".(On by default) Open LLDP-MED optional TLV "POE".(On by default) Turn off the LLDP-MED optional TLV "capability". Close the LLDP-MED optional TLV "location". Turn off the LLDP-MED optional TLV "POE".

Command	switch# show lldp neighbor interface GigabitEthernet 1/1 switch# show lldp neighbor interface * switch# show lldp neighbor
Description	Displays LLDP neighbor information for interface 1/1. Displays LLDP neighbor information for all interfaces. Displays all LLDP neighbor information.

Command	switch# show lldp med remote-device interface GigabitEthernet 1/1 switch# show lldp med remote-device interface * switch# show lldp med remote-device
Description	Displays lldp-med neighbor information for interface 1/1. Displays LLDP-MED neighbor information for all interfaces. Displays all LLDP-MED neighborhood information.

Command	switch# show lldp statistics interface GigabitEthernet 1/1 switch# show lldp statistics interface * switch# show lldp statistics
Description	Displays LLDP statistics for interface 1/1. Displays LLDP statistics for all interfaces. Displays all LLDP statistics.

11 Ethernet power supply

Only the switches of the IMS3214 series support Ethernet power supply. For switches that do not support Ethernet power supply, the Ethernet power supply page will not be visible in the Web management,

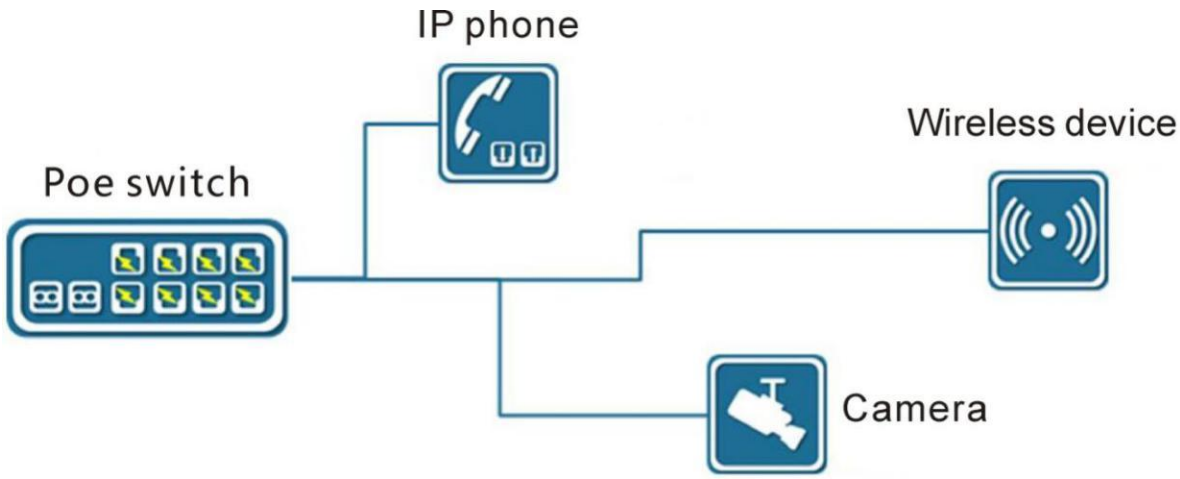
11.1 POE Overview

Power over Ethernet (POE) is a technology that provides direct current Power to a terminal in an Ethernet network through twisted-pair data exchange.

It is commonly used to power VoIP phones, WiFi AP, webcams, hubs, computers and other devices.

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

Chart Figure 11-1 POE power supply schematic



PSE (Power Sourcing Equipment), such as the POE switch in the figure above.

PSE searches for and detects PD on the line of POE port, classifies PD, and supplies power to it.

When PD is detected to pull out, PSE stops power supply.

PD is the device that receives power supply from PSE, such as IP phone, wireless device and camera in the figure above.

The development of POE has gone through two sets of standards:

IEEE 802.3AF (15.4W) is the first POE power supply standard, which defines the Ethernet power supply standard, and is the mainstream implementation standard for POE applications.

It specifies power detection and control in remote systems and how routers, switches, and hubs can supply power over Ethernet cables to devices such as IP phones, security systems, and wireless LAN access points.

IEEE802.3AT (30W) is born in response to the demand of high-power terminals. On the basis of compatibility with 802.3AF, it provides greater power supply demand and meets new demands.

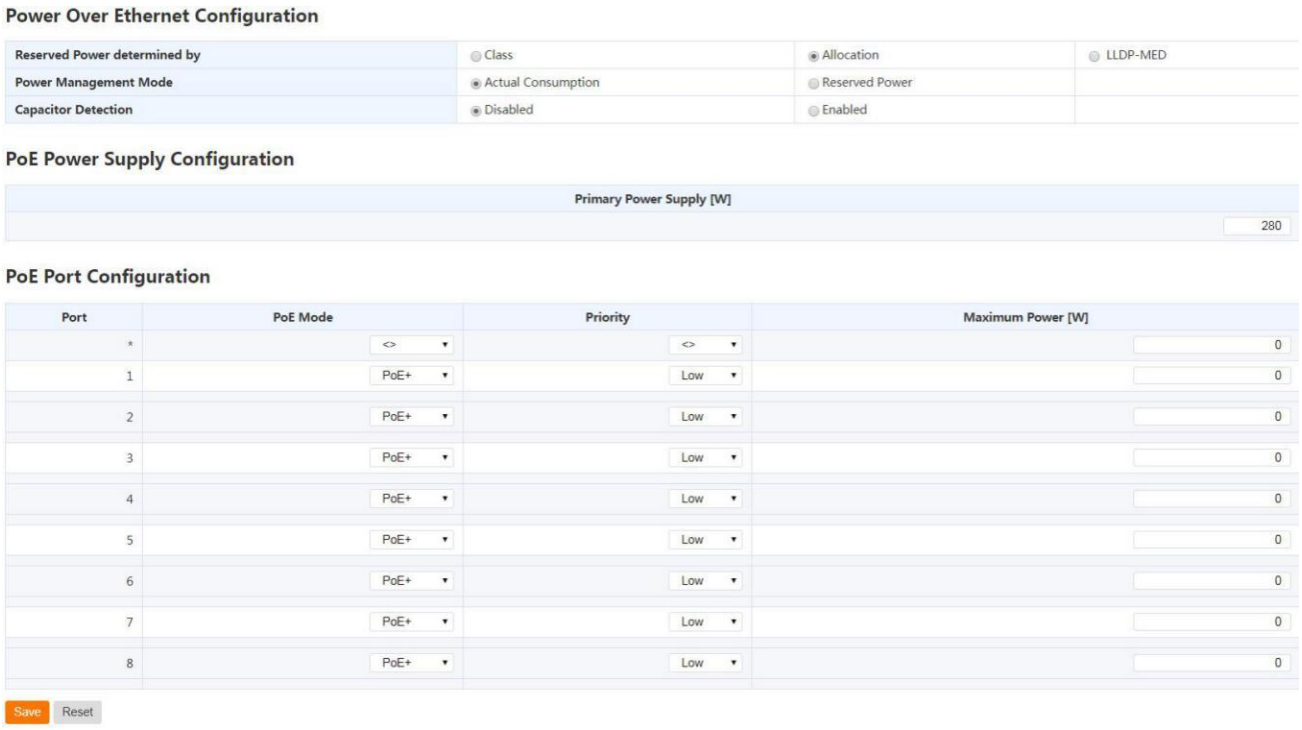
According to the IEEE 802.3AF specification, the power supply device (PSE) can provide no more than 15.4W on a single port.

IEEE 802.3AT, which defines as Class 4 devices requiring more than 15.4W (described in IEEE 802.3AF but reserved for future use), extends the power level to 30W.

11.2 Configuration

In the [Navigation Bar] drop-down menu, select: Configuration -> Power over Ethernet to enter the configuration page.

Chart Figure 11-2 POE configuration page



11.2.1 Reserved power mode

Reserved power: Reserved power is used to determine the maximum power reserved for the port, which sets a threshold for port power overload.

That is, when the output power of the port exceeds the reserved power, there will be overload and the power supply of the port POE will stop.

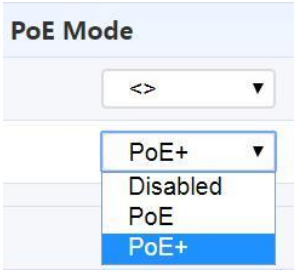
Chart Figure 11-3 POE reserved power mode configuration

- PD level: the reserved power is determined according to the Class of the PD device accessed by the port, as follows:
  - Class 0： 15.4W
  - Class 1： 4W
  - Class 2： 7W

- Class 3： 15.4W
- Class 4： 15.4W(for poe) 30W(for poe+)

It is important to note that the reserved power for Class4 is dependent on the POE mode selected for the port. For the POE mode (AF standard), class 4 corresponds to 15.4W, and for the POE + standard (AT standard), class 4 corresponds to 30W.
If the POE mode is Disable, the port is off and POE power is supplied.

Chart Figure 11-4 POE port mode configuration



- Static allocation, according to the set maximum power of the port to determine the reserved power. Therefore, when selecting static allocation mode, the maximum power of the port must be configured.

Chart Figure 11-5 POE port maximum power configuration

PoE Port Configuration

Port	PoE Mode	Priority	Maximum Power [W]
*	<>	<>	35
1	PoE+	Low	35
2	PoE+	Low	0
3	PoE+	Low	0
4	PoE+	Low	0
5	PoE+	Low	0
6	PoE+	Low	0
7	PoE+	Low	0
8	PoE+	Low	0

Save Reset

- Reserving power through LLDP-MED negotiation is more accurate than reserving power according to PD grade or static allocation, but PD equipment must support LLDP-MED.
- If the PD device does not support LLDP-MED, the LLDP-MED mode performs the same as the PD grade mode, that is, the reserved power is determined according to the Class of the PD device.
- Default configuration: Reserved power mode defaults to "PD level".

11.2.2 Power management mode

The purpose of power management is to coordinate the power supply relationship between ports.
The rated power of the power supply is a scarce resource. When the rated power is insufficient, it is necessary to decide which ports to power down, which is the purpose of power management.
Obviously, there are two key steps in power management:

- Port power calculation: The power management mode is used to determine how the port power is calculated. If the reserved power mode is used, the allocated power calculation is used, and if the actual consumption mode is used, the used power calculation is used.

Chart Figure 11-6 POE power management mode configuration

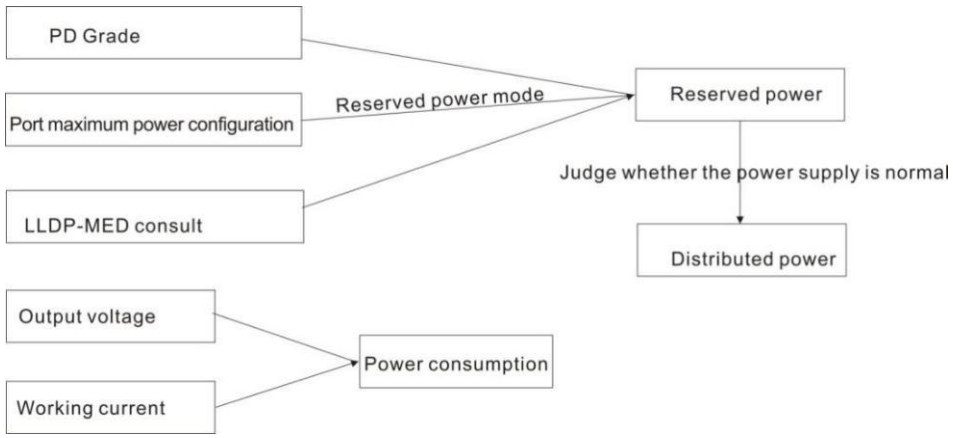
Power Over Ethernet Configuration

Reserved Power determined by	Class	Allocation	LLDP-MED
Power Management Mode	Actual Consumption	Reserved Power	
Capacitor Detection	Disabled	Enabled	

  - Actual consumption: Calculate whether the system power is sufficient according to the actual consumption (power used) of the port.
  - Reserved power: Calculate whether the system power is sufficient based on the allocated power of the port (allocated power is related to the reserved power mode).
  - Default configuration: Power management mode defaults to "actual consumption".

In the POE module, there are three kinds of power involved: demand power, distributed power and used power.
Combined with the above, the calculation of several kinds of power is as follows:
1. Demand power, namely reserved power.
2. Assigned power: if the port is not powered, the allocated power of the port is 0; if the port is powered, the allocated power is the reserved power of the port.
3. Power used: that is, power consumed, which is calculated according to the voltage and current used, indicating the actual power consumed by PD.

Chart Figure 11-7 POE various power calculations



- Judgment and decision:

Judging whether the system power is sufficient according to different power management modes (the actual consumption mode is calculated according to the used power, and the reserved power mode is calculated according to the allocated power), judging according to the following power configuration:

Chart Figure 11-8 Power Supply Rated Power Configuration

PoE Power Supply Configuration

Primary Power Supply [W]
280

If the system power is insufficient, power off certain ports. Which port(s) to choose depends on the port priority configuration.

Chart Figure 11-9 POE port priority configuration

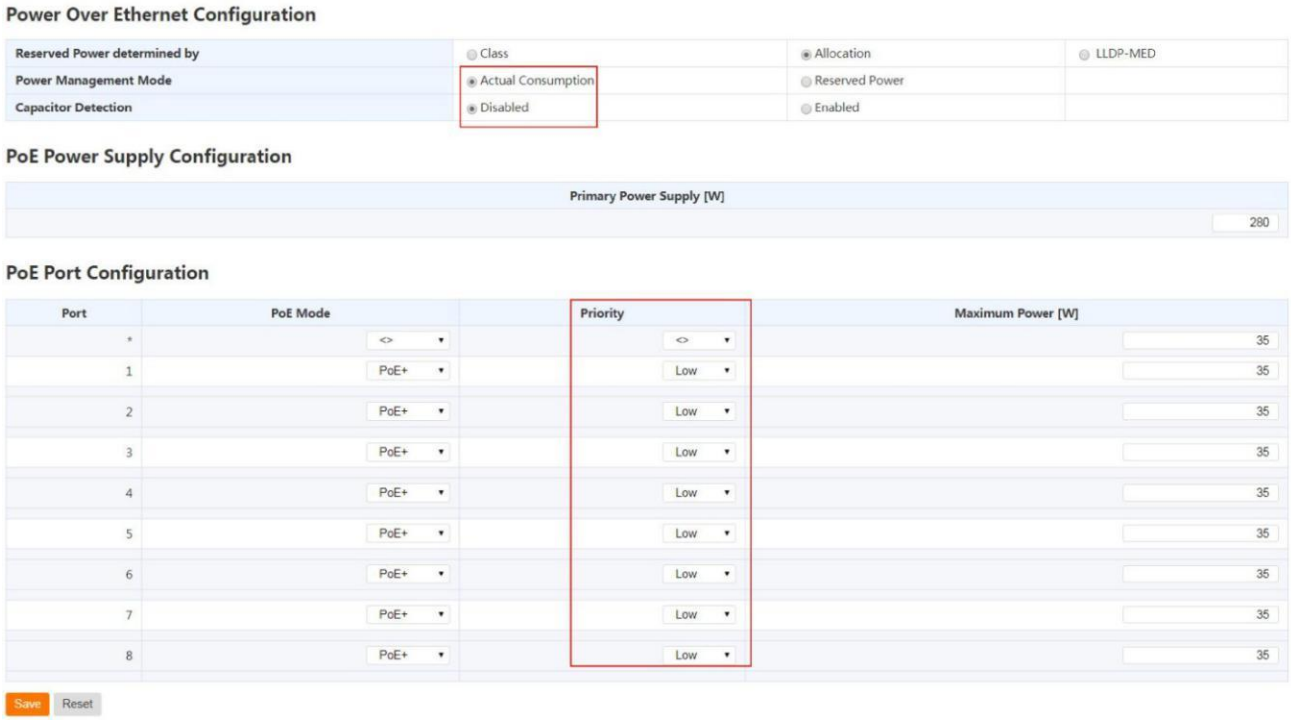
PoE Port Configuration

Port	PoE Mode	Priority	Maximum Power [W]
*	<>	<>	35
1	PoE+	Low	0
2	PoE+	Low / High / Critical	0
3	PoE+	Low	0
4	PoE+	Low	0
5	PoE+	Low	0
6	PoE+	Low	0
7	PoE+	Low	0
8	PoE+	Low	0

Save Reset

Note: When the reserved power mode selects static allocation and the power management mode selects reserved power, the priority cannot be configured, because in this case, the allocated power is equal to the maximum power of the port configuration, and the maximum power configuration will directly determine whether If the power supply exceeds the rated power, as long as the configuration is legal, there will be no power shortage. Therefore, there is actually no need to power off the power management.

Chart Figure 11-10 POE static mode description



11.2.3 Combination method

Model	Power management mode	Reserved power mode	Demand power /reserved power	Distribution of power
Automatic mode /Class mode	Reserve power	Level of PD.	Determine according to PD rating.	Equal to demand power
Static mode	Reserve power	Statically allocated	Determine according to the maximum power of port configuration.	Equal to demand power
LLDP mode	Reserve power	LLDP-MED	Negotiation according to LLDP-MED (negotiation failure, determined according to PD level)	Equal to demand power
Consumption patterns	Actual consumption	Level of PD.	Determine according to PD rating.	Equal to use power
		Statically allocated	Determine according to the maximum power of port configuration.	Equal to use power
		LLDP-MED	Determine according to the maximum power of port configuration.	Equal to use power

Note: in the consumption mode, the selection of reserved power mode has nothing to do with power management (because the allocated power is equal to the used power). The selection of reserved power mode is only used to determine the port power threshold and determine whether the port power overload occurs.
By default, consume mode is used.

11.3 Displaying

In the [Navigation Bar] drop-down menu, select: Monitoring -> Power over Ethernet to enter the display page.

Power Over Ethernet Status

Auto-refresh Refresh

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	3	15.4 [W]	15.4 [W]	3.2 [W]	61 [mA]	Low	PoE turned ON
2	3	15.4 [W]	15.4 [W]	3.2 [W]	62 [mA]	Low	PoE turned ON
3	3	15.4 [W]	15.4 [W]	3.2 [W]	62 [mA]	Low	PoE turned ON
4	-	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PD overload
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		61.6 [W]	46.2 [W]	9.6 [W]	185 [mA]		

The required power, allocated power and used power are described in the section of "Power Management Mode".

11.4 CLI reference commands

Command	switch(config)# poe supply 200 switch(config)# no poe supply
Description	PoE power rating configuration; Restore POE power rating to default value.

Command	switch(config)# poe management mode allocation-consumption switch(config)# poe management mode allocation-reserved-power switch(config)# poe management mode class-consumption switch(config)# poe management mode class-reserved-power switch(config)# poe management mode lldp-consumption switch(config)# poe management mode lldp-reserved-power switch(config)# no poe management
Description	Configuration POE reserved power mode and power management mode combination. Restors POE reserved power mode and power management mode to default (class-consumption).

Command	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# poe mode standard switch(config-if)# poe mode plus switch(config-if)# no poe mode
Description	The POE mode for configuring Interface 1/1 is POE (802.3af). The POE mode for configuring interface 1/1 is POE+(802.3AT). Turn off connector 1/1 of POE power supply. The default is POE+ mode.

Command	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# poe power limit 27.8 switch(config-if)# no poe power limit
Description	The maximum POE power for the 1/1 configuration is 27.8W. Remove interface 1/1 of the POE maximum power configuration. Default is 0W.

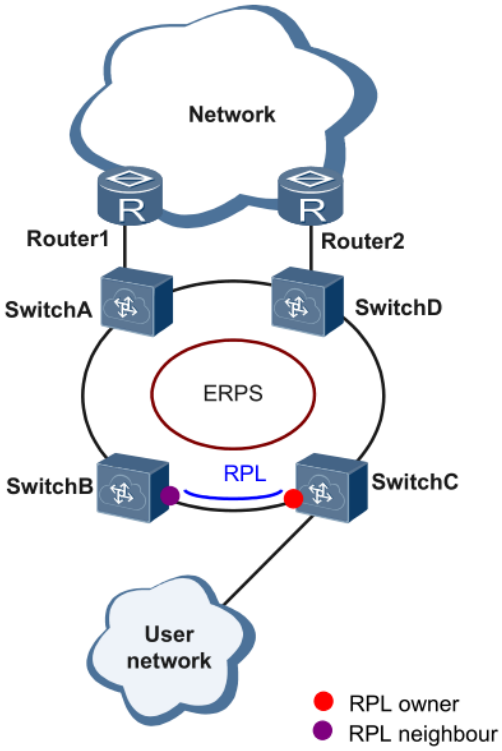
Command	switch(config)# interface GigabitEthernet 1/1 switch(config-if)# poe priority critical switch(config-if)# poe priority high switch(config-if)# poe priority low switch(config-if)# no poe priority
Description	Configure the POE priority of interface 1/1. The POE priority of the configuration interface 1/1 is the default value, which defaults to Low.

Command	switch# show poe interface GigabitEthernet 1/1 switch# show poe interface * switch# show poe
Description	Displays POE information of interface 1/1. Displays POE information for all interfaces. Display all POE information.

12 ERPS

12.1 Overview of ERPS functions

ERPS (Ethernet Ring Protection Switching) is a Ring Protection protocol developed by ITU, also known as G.8032.
It is a link layer protocol that is specifically applied to Ethernet ring networks.
It can prevent the broadcast storm caused by the data loop while the Ethernet loop is intact, and can quickly restore the communication between the nodes of the Ethernet loop when a link is disconnected.
At present, the technology to solve the problem of two layer network loop is STP.
The application of STP is relatively mature, but its convergence time is relatively long (second level).
ERPS is a link layer protocol specially applied to Ethernet ring network. The convergence performance of the second layer is less than 50ms, and it has faster convergence speed than STP.
Chart Figure 12-1 EPS Typical Networking

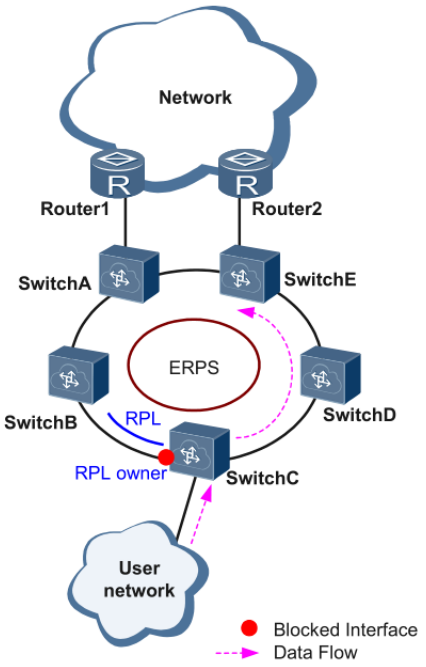


12.2 Brief introduction of ERPS principle

ERPS is a standard ring network protocol dedicated to Ethernet link layer, taking ERPS ring as the basic unit.
Only two ports can be added to the same ERPS ring on each Layer 2 switching device.
In the ERPS ring, in order to prevent the occurrence of a loop, you can activate the break loop mechanism to block the RPL Owner port and eliminate the loop.
When the link failure occurs in the ring network, the equipment running ERPS protocol can quickly release the blocking port, carry out the link protection reversal, and restore the link communication between the nodes in the ring network.
This section mainly introduces the implementation principle of ERPS under the basic single-loop networking in the form of examples according to the process of link normal-link failure-link recovery (including protection switching operation).

12.2.1 Link normal

All devices on the loop composed of Switch A ~ Switch E communicate normally.
Chart Figure 12-2 ERPS link normal scenario

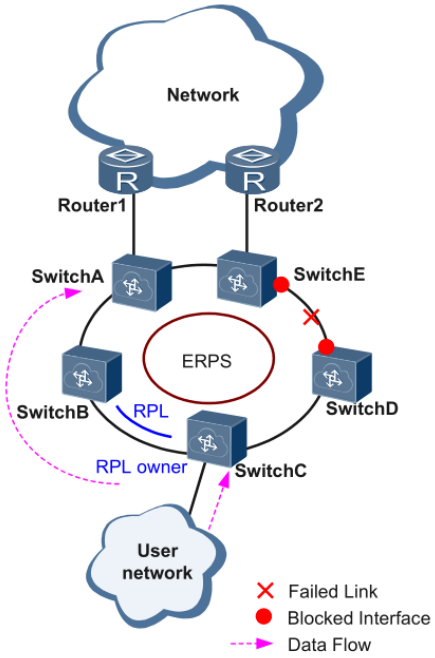


To prevent the creation of a loop, ERPS first blocks the RPL Owner port. If the RPL Neighbor port is configured, this port is blocked as well, allowing other ports to forward traffic normally.

12.2.2 Link failure

As shown in the figure below, when the link between Switch D and Switch E fails, the ERPS protocol initiates the protection reversal mechanism, blocking the ports at both ends of the failed link, and then opening the RPL Owner port. These ports resume the receiving and sending of user traffic, thus ensuring uninterrupted traffic.

Chart Figure 12-3 ERPS link failure scenario



12.2.3 Link recovery

When the link is restored, by default, the ERPS ring is configured in backcut mode, and the device hosting the RPL Owner port will re-block traffic on the RPL link, and the failed link will be re-used to complete the transfer of user traffic.

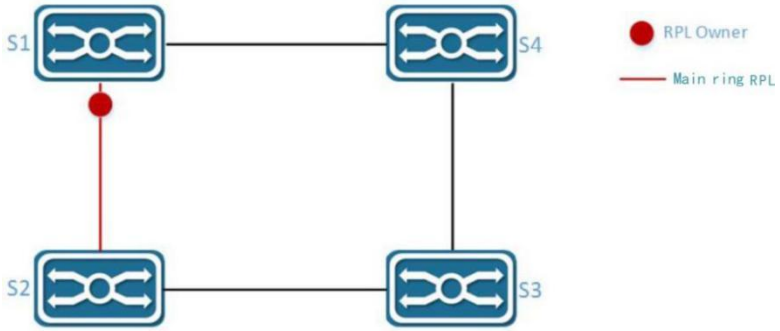
12.2.4 Types of ERPS rings

Single ring:

There is only one ring in the network topology; there is one and only one RPL Owner; there is one and only one RPL link; all nodes need to have the same RAPS management VLAN

- 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, without intermediate devices.

Chart Figure 12-4 ERPS single loop model

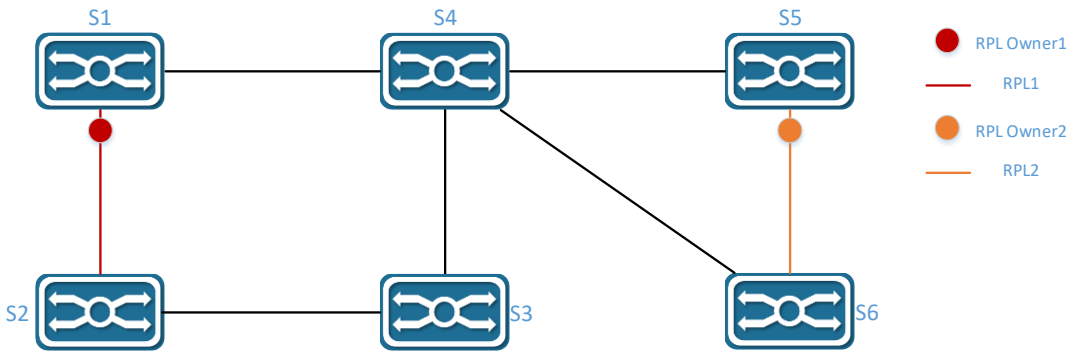


Tangent ring:

Application scenarios where two or more ring networks sharing one device in the network topology need to be protected. Take the following figure as an example. Two rings in the network topology share one device; each ring has and only one blocking point, and each ring has and only one RPL link; different rings need different RAPS management Vlan.

- All devices in the ring network need to support ERPS.
- The links between the devices in the ring network must be directly connected without intermediate devices.

Chart Figure 12-5 ERPS Tangent Ring Model



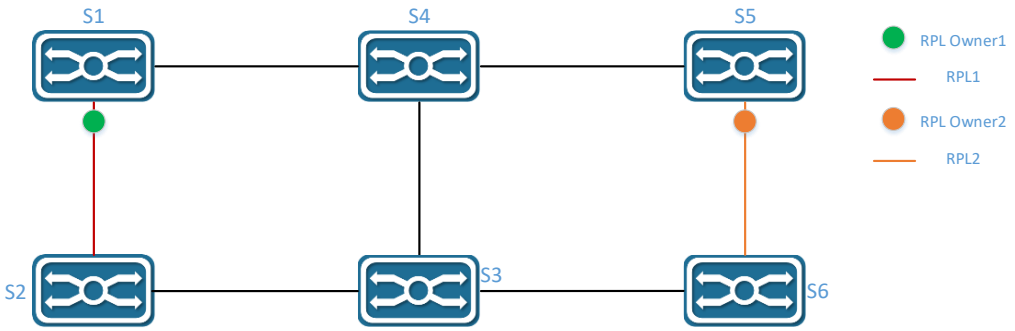
Intersecting rings:

In a network topology, two or more rings share a link (two nodes that intersect must be directly connected to each other without any other nodes).
For example, there are two 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 require different RAPS to manage the VLAN.

- □All devices in the ring network need to support ERPS.
- □The links between the devices in the ring network must be directly connected without intermediate devices.

Chart Figure 12-6 ERPS intersecting ring model

□□



12.3 Introduction to ERPS configuration

- The spanning tree protocol and ERPS protocol cannot be enabled at the same time.

12.3.1 MEP configuration interface

Click on the navigation bar: Configuration->MEP to enter the MEP configuration interface.

Chart Figure 12-7 MEP Configuration 1

12.3.2 Add MEP Node

Click the "Add MEP" button in the MEP configuration interface to add a MEP node, and click the "Save" button to add a MEP node after configuration.

Chart Figure 12-8 MEP Configuration 2

Item	Description
Instance	MEP instance number, numbers 1-100. The MEP node instance must be unique. For simple mapping, the port number can be used as the MEP instance directly.
Domain	Port: Based on Port. VLAN: VLAN-based. ERPS uses the Port field.
Model	MEP: Terminal mode. MIP: Intermediate mode. ERPS uses the MEP mode.
Direction	Down: handles traffic in the admittance direction. Up: handle the flow in the correct direction. ERPS uses the DOWN direction.
Port	Physical port number.
Level	Instance priority. The default for ERPS is 0.

Flow instance	Stream instance ID, valid only in the VLAN domain. ERPS does not require configuration.
Tagged VID	VLAN tag. ERPS uses RAPS to manage the VLAN of the packet.

12.3.3 Enabling the RAPS function of MEP

Click the configured MEP node instance to enter the instance configuration page, enable the APS protocol, and click Save to complete the configuration.

Chart Figure 12 9 MEP instance entry

Chart Figure 12-10 MEP instance configuration

Item	Description
Priority	RAPS priority, numbers 0-7. The default for ERPS is 0.
Mapping	Uni: unicast address, provided that the opposite MEP is known. Multi: Multicast address. ERPS uses standard multicast addresses.

Type	R-APS: ERPS message. L-APS: ELPS message. ERPS uses the R-APS type.
The last byte	The contents of the last byte of the MAC address. ERPS uses the ring ID as the last byte of MAC, and ring 1 is 1.

12.3.4 ERPS configuration interface

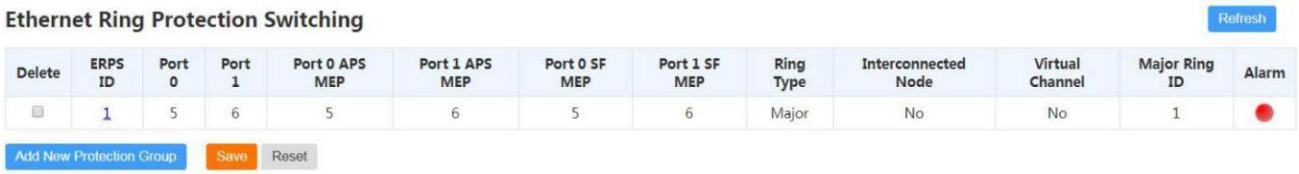
Click on the navigation bar: Configuration->ERPS to enter the ERPS management interface.

Chart Figure 12-11 ERPS configuration 1

12.3.5 Add ERPS protection group

Click the "Add Protection Group" button in the ERPS configuration page, enter the protection group information in the input box that appears, and click the "Save" button to complete the configuration.

Chart Figure 12-12 ERPS configuration 2



Item	Description
ERPS ID	Ring number. Different switches in the same ring need to be configured with the same ring number. The ring number should be the same as the last byte of the RAPS MAC address of the MEP node.
Port 0	Also known as Port0, left port, east port.
Port 1	Also known as Port1, right interface, west interface.
Port 0 APS MEP	The MEP node associated with the port 0 protocol packet.
Port 1 APS MEP	The MEP node associated with the port 1 protocol packet.
Port 0 SF MEP	Port 0 fault detection associated with the MEP node.
Port 1 SF MEP	Port 1 fault detection associated with the MEP node.
Ring type	Major: Main ring Sub: subring

Interconnected nodes	Whether the current node is an interconnected node, only the multi-ring intersecting node needs to be set.
Virtual channel	Virtual channel mode is not currently supported.
Main ring ID	Configurable only if the ring type is a subring.

12.3.6 ERPS protection group parameter configuration

Click the specific ERPS ID in the ERPS configuration page to enter the protection group parameter configuration page, modify the protection group parameters, and click the [Save] button to complete the configuration.

Chart Figure 12-13 ERPS protection group entry

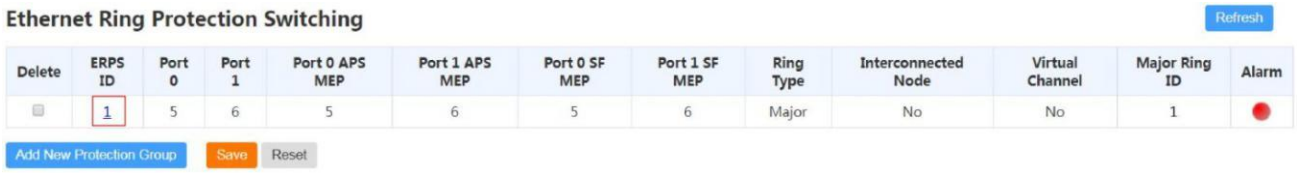
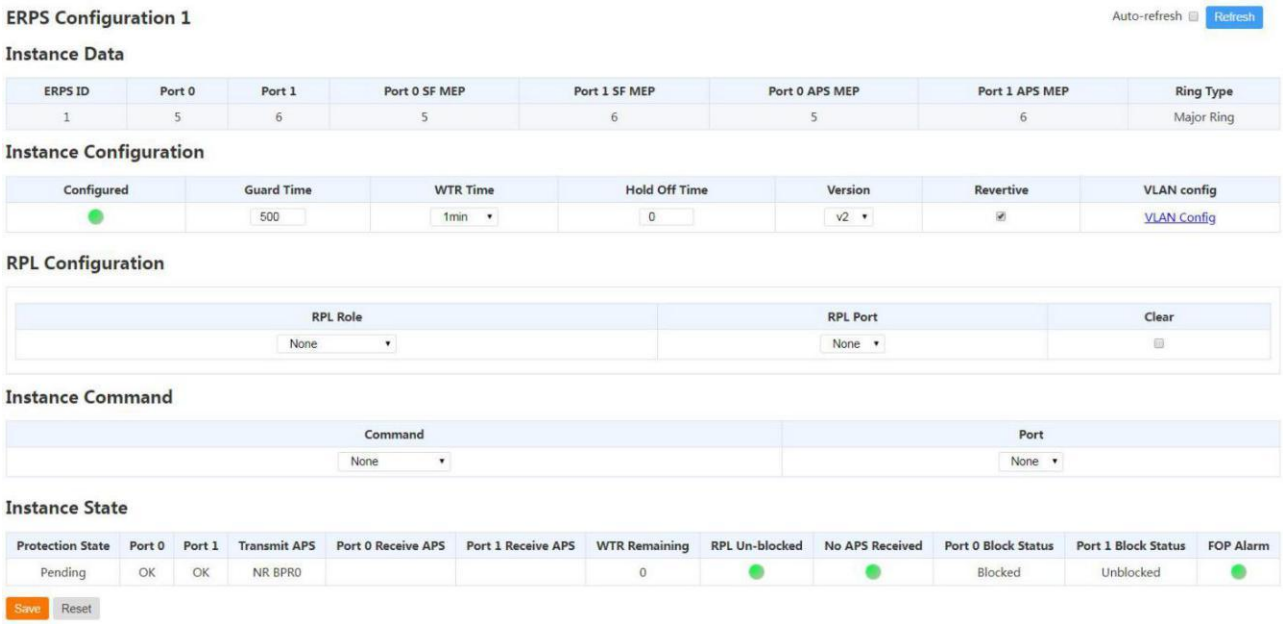


Chart Figure 12-14 ERPS protection group configuration



Item	Description
Guard Time	Protocol protection time, default 500 milliseconds.
WTR Time	Protocol cutback time, default is 1 minute.
Hold Off Time	Protocol delay time, default 0 seconds.
VERSION	Protocol version number, default v2.
Can be cut back	Whether loop backcutting is allowed. Default is allowed.

VLAN configuration	To protect the configuration of a VLAN, it is usually necessary to join all VLANs as protected VLANs. Unprotected VLANs may suffer from loop failure.
RPL role	None: Non-RPL nodes. RPL_Owner: Owner node. RPL_Neighbour: Neighbour node.
RPL port	None: No RPL port. Port0: Port0 port, also known as the east port or left port. Port1: Port1 port, also known as the west port or right port.
Remove	Tick to perform protocol failover/cutback action.
Command	None: no. Manual Switch: Manual Switch instructions. Force Switch: Force Switch instruction. Clear: Clear the command status.
Port	None: no Port0/Port1: Port where the directive takes effect.

12.3.7 ERPS protection group VLAN configuration

Click VLAN Config in the ERPS protection group configuration page to enter the VLAN configuration page, modify the VLAN configuration, and click the "Save" button to complete the configuration.

Chart Figure 12-15 ERPS protection group VLAN configuration entry

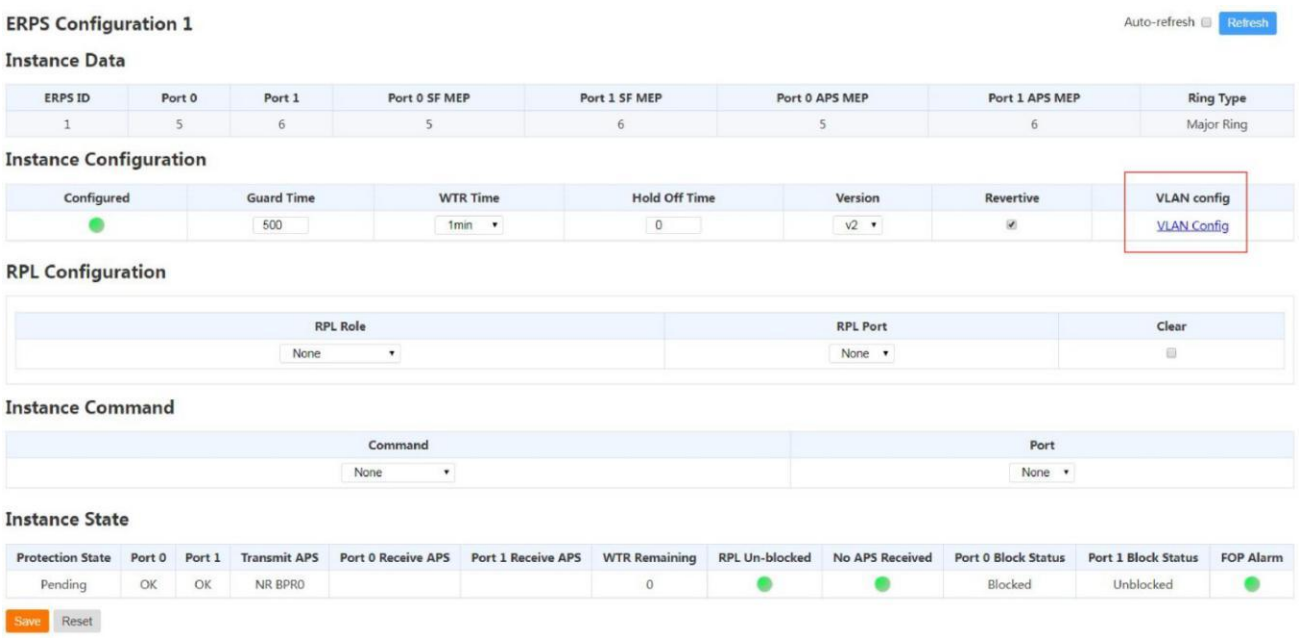
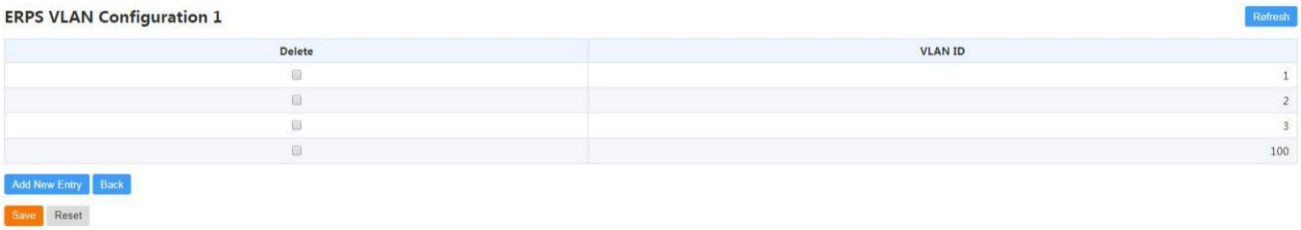


Chart Figure 12-16 ERPS protection group VLAN configuration



Item	Description
Delete	The specified configuration table is deleted the next time it is saved.
VLAN ID	Protection group VLAN ID.

12.3.8 CLI Reference Commands

Command	switch(config)# mep 7 down domain port level 0 interface GigabitEthernet 1/7 switch(config)# no mep 7 switch(config)# mep 7 vid 100 switch(config)# mep 7 aps 0 raps octet 1 switch(config)# no mep 7 aps
Description	Configure MEP to create an instance; Configure MEP to delete instances; Config the MEP instance Tagged Vid; Open RAPS and configure the last byte. Configure the MEP instance to turn off RAPS;

Command	switch(config)# erps 1 major port0 interface GigabitEthernet 1/7 port1 interface GigabitEthernet 1/8 switch(config)# no erps 1 switch(config)# erps 1 mep port0 sf 7 aps 7 port1 sf 8 aps 8 switch(config)# erps 1 rpl owner port0 switch(config)# no erps 1 rpl switch(config)#erps 1 vlan 1,2,3,100
Description	Configure the ERPS protection group to create and set the ring type and port 0, port 1; Configuration ERPS protection group delete; Configure the MEP associated with port 0 and port 1 of ERPS protection group for SF and APS; Configure the ERPS protection group RPL role and corresponding port; Configure ERPS protection group to remove RPL roles; Configure the ERPS protection group VLAN configuration;

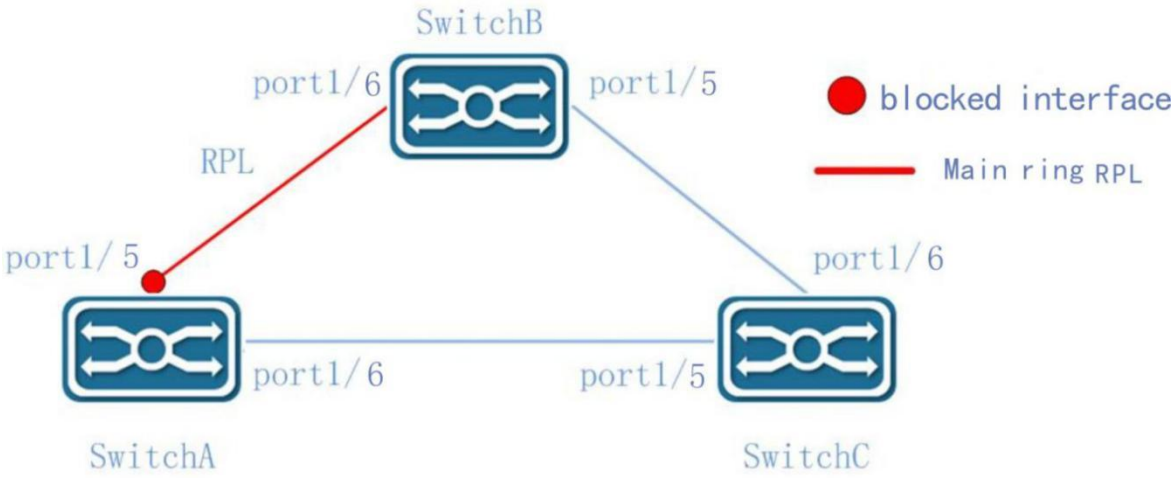
Command	switch# show mep 7 detail switch# show erps 1 detail switch# show erps 1 statistics
Description	Print the state of MEP node; Print the status of ERPS protection group; Print ERPS protection group message statistics;

12.4 Examples of single-ring configuration

12.4.1 Case requirements

Ring network of 3 switching units, as shown in the figure below, configuration default blocking port is Switcha port1/5 port, data VLAN is 1,2,3, in case of failure, the link can be restored in time to ensure the availability of network.

Chart Figure 12-17 ERPS single loop case



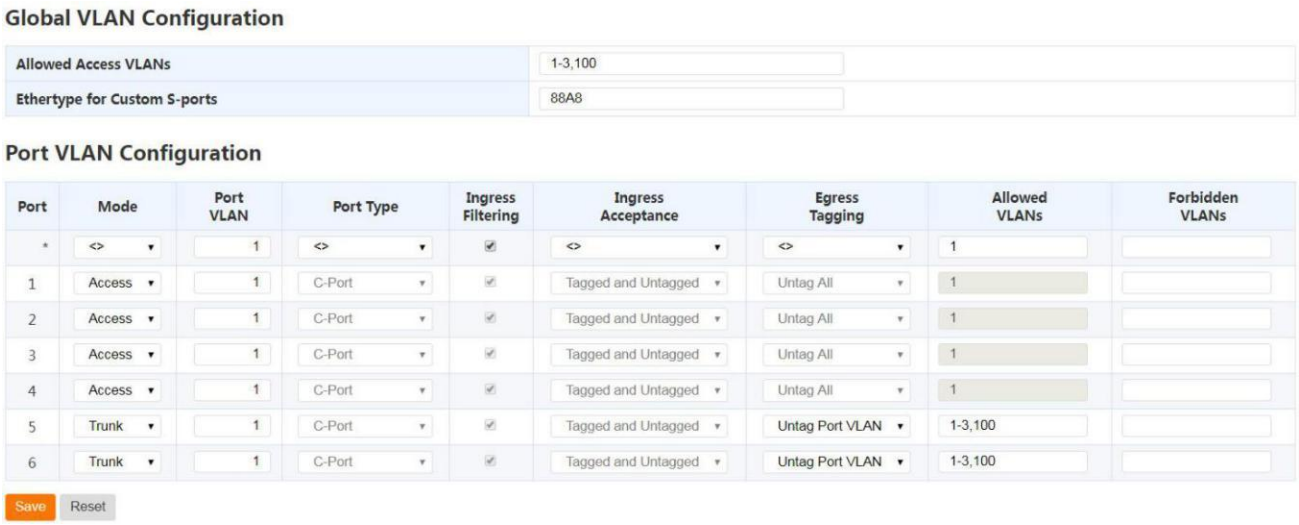
12.4.2 Configuration planning

In this example, the switchA, switchB, switchC ring definition is numbered "1", the switchA block is switchA "port1/5", and the RAPS management VLAN is "100". The specific parameters are shown below.

Equipment	Ring number	RAPS VLAN	Owner interface	Neighbor interface	Interconnected nodes	Associated instance
SwitchA	1	100	port1/5	None	\	\
SwitchB	1	100	None	port1/6	\	\
SwitchC	1	100	None	None	\	\

12.4.3 Configure SwitchA

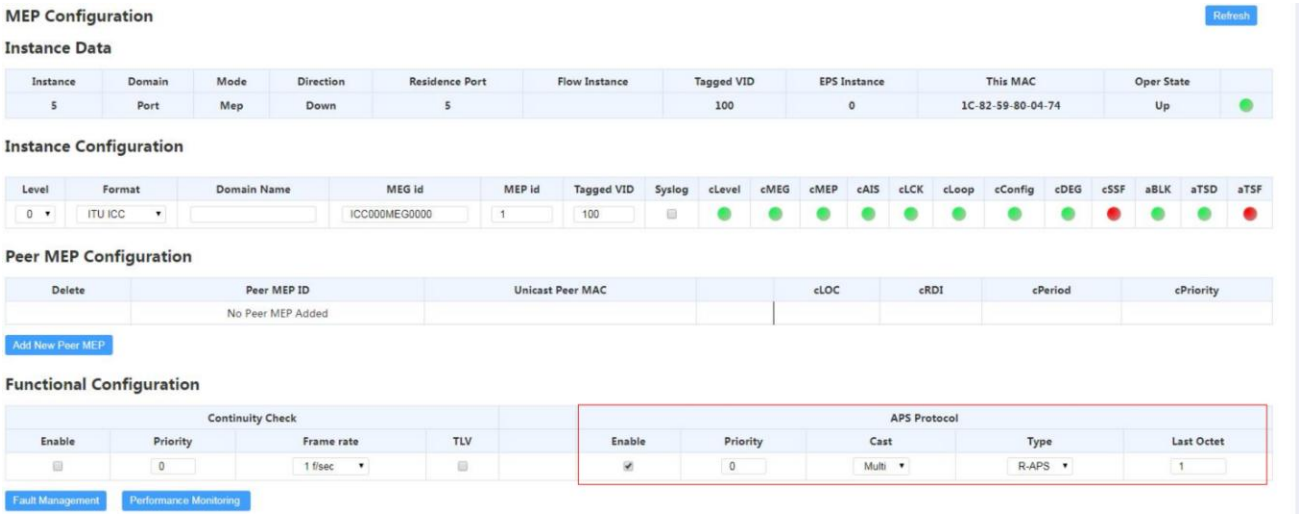
Step 1: VLAN and port configuration.
Select "VLAN" from the "Configuration" sub-item in the navigation bar. Configuration allows access to VLANs 1,2,3,100, port1/5, port1/6 mode Trunk, allows VLANs 1,2,3,100. Click "Save" to complete the configuration.
Chart Figure 12-18 Single Ring Case SwitchA VLAN Configuration



Step 2: Create and configure the MEP node.
1) Select "MEP" in the "Configuration" sub-item of the navigation bar and click "Add MEP" button to add port 5 as MEP 5 and Tagged VID as 100.
Chart Figure 12-19 Single Ring Case SwitchA MEP Configuration 1

1) Click the [Save] button to complete the addition of the entity node. Click instance 5 again to enter the instance data configuration and enable the RAPS function.

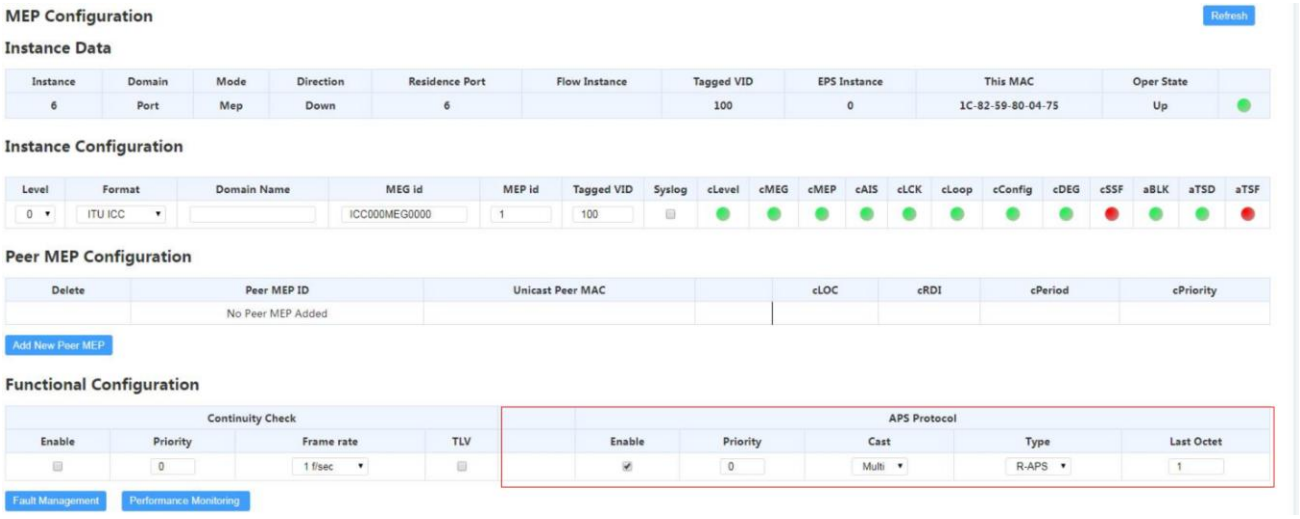
Chart Figure 12-20 Single Ring Case SwitchA MEP Configuration 2



2) Similarly, add port 6 as MEP 6, Tagged VID as 100, and enable the RAPS function in the instance data configuration.

Chart Figure 12-21 Single Ring Case SwitchA MEP Configuration 3

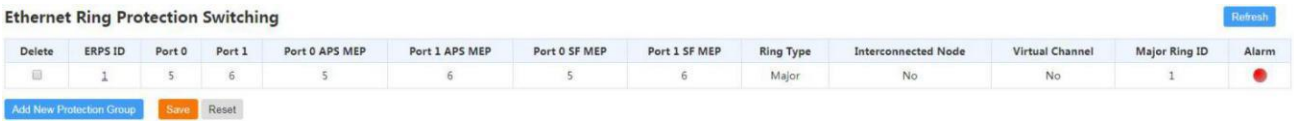
Chart Figure 12=22 Single-Ring Case Switcha MEP Configuration 4



Step 3: Create and configure ERPS protection group.

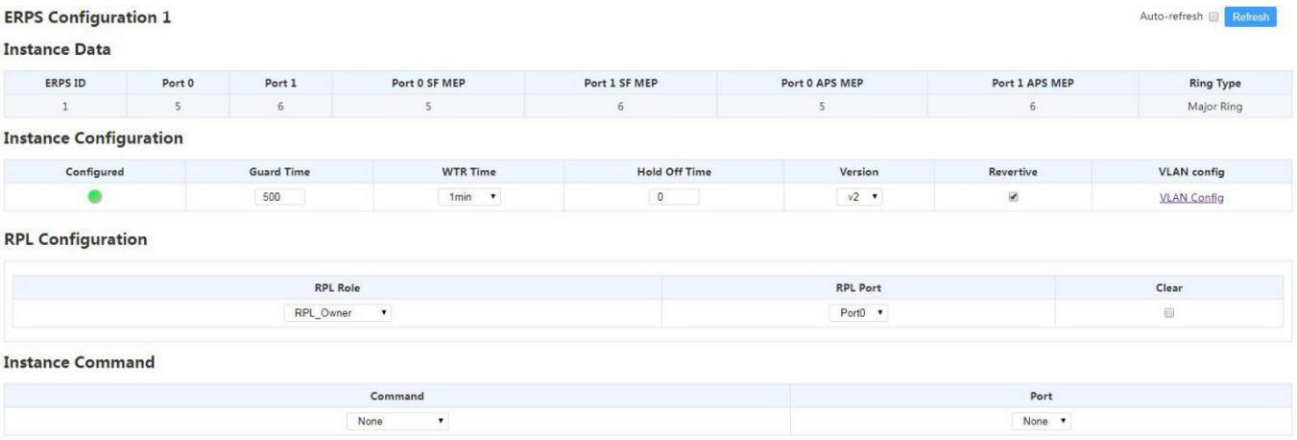
Select [ERPS] under [Configuration] in the navigation bar, enter the ERPS configuration interface, and click the [Add Protection Group] button to add protection group 1.

Chart Figure 12-23 Single Ring Case SwitchA ERPS Configuration 1



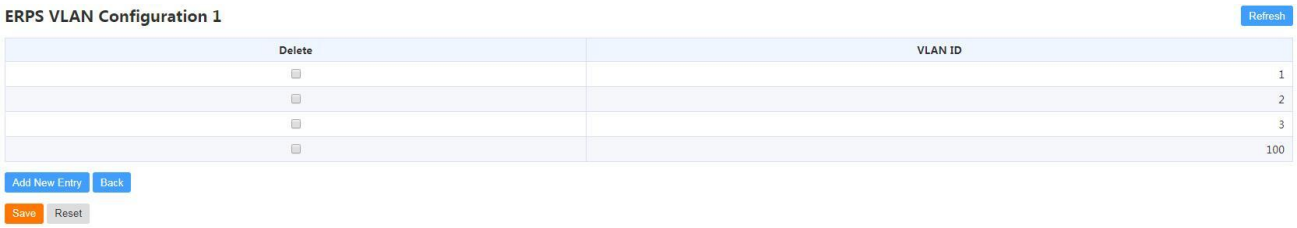
Click the [Save] button to complete the addition of the protection group. Click protection group 1 again to enter the parameter configuration interface. Set Port0 as the RPL Owner role according to the planned configuration.

Chart Figure 12-24 Single Ring Case SwitchA ERPS Configuration 2



Click [VLAN_CONFIG] to enter the VLAN configuration page, and click "Add Entry" to add VLAN 1,2,3,100 in turn. To protect the VLAN, click "Save" to complete configuration.

Chart Figure 12-25 Single Ring Case SwitchA ERPS Configuration 3

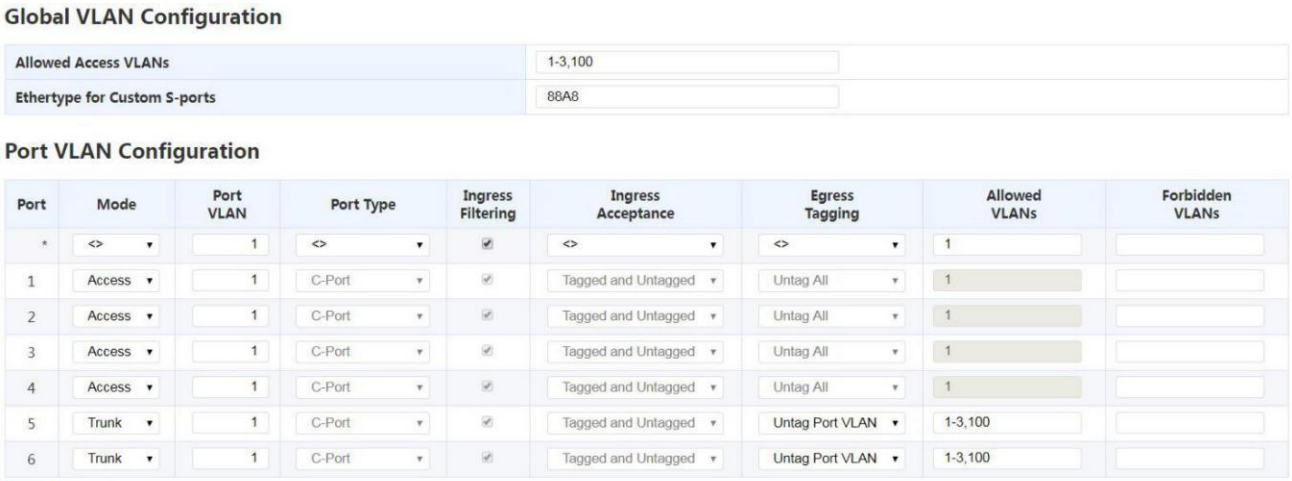


Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

12.4.4 Configure SwitchB

Step 1: VLAN and port configuration.
Select "VLAN" from the "Configuration" sub-item in the navigation bar. Configuration allows access to VLANs 1,2,3,100, port1/5, port1/6 mode Trunk, allows VLANs 1,2,3,100. Click "Save" to complete the configuration.

Chart Figure 12-26 Single Ring Case SwitchB VLAN Configuration



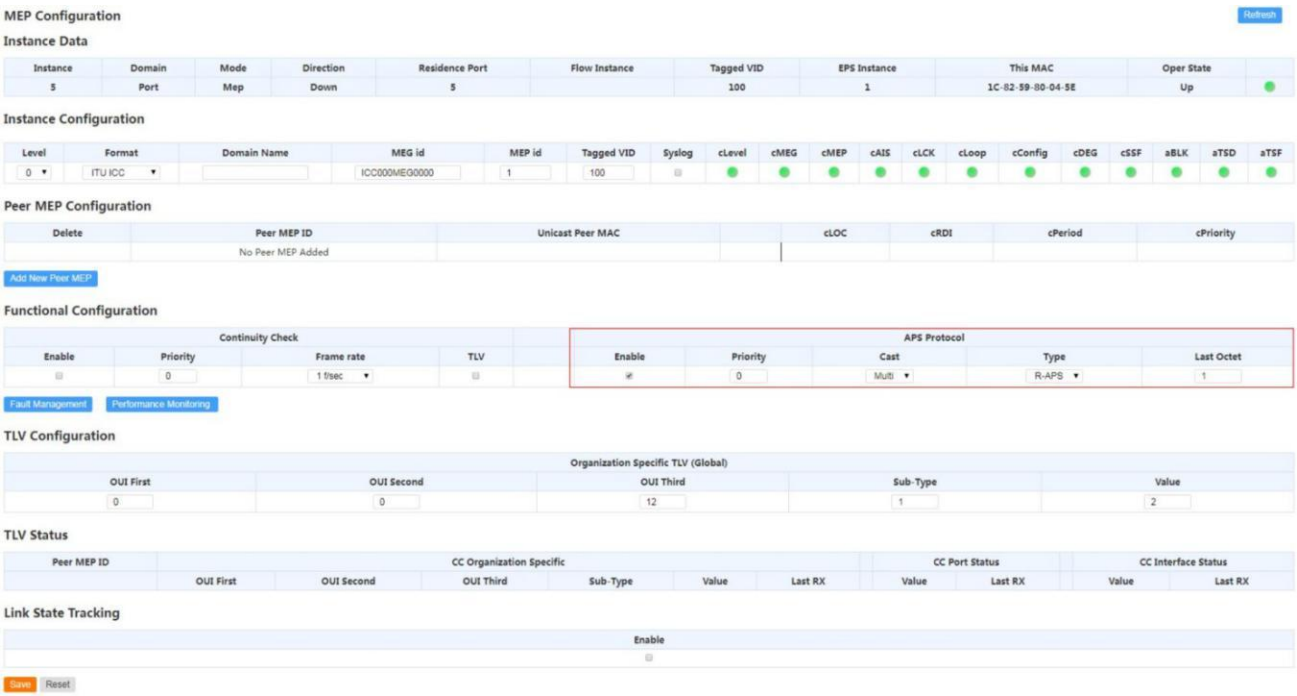
Step 2: Create and configure the MEP node.

1) Select "MEP" in the "Configuration" sub-item of the navigation bar and click "Add MEP" button to add port 5 as MEP 5 and Tagged VID as 100.

Chart Figure 12-27 Single Ring Case SwitchB MEP Configuration 1

1) Click the [Save] button to complete the addition of the entity node. Click instance 5 again to enter the instance data configuration and enable the RAPS function.

Chart Figure 12-28 Single Ring Case SwitchB MEP Configuration 2



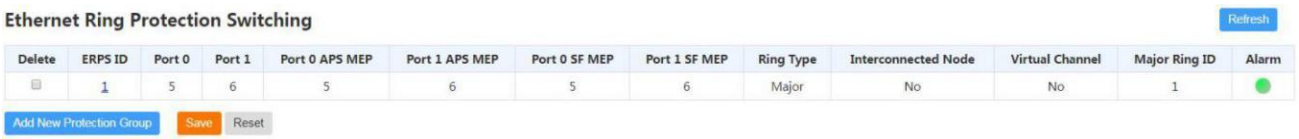
2) Similarly, add port 6 as MEP 6, Tagged VID as 100, and enable the RAPS function in the instance data configuration.

Chart Figure 12-29 Single Ring Case SwitchB MEP Configuration 3

Chart Figure 12-30 Single Ring Case SwitchB MEP Configuration 4

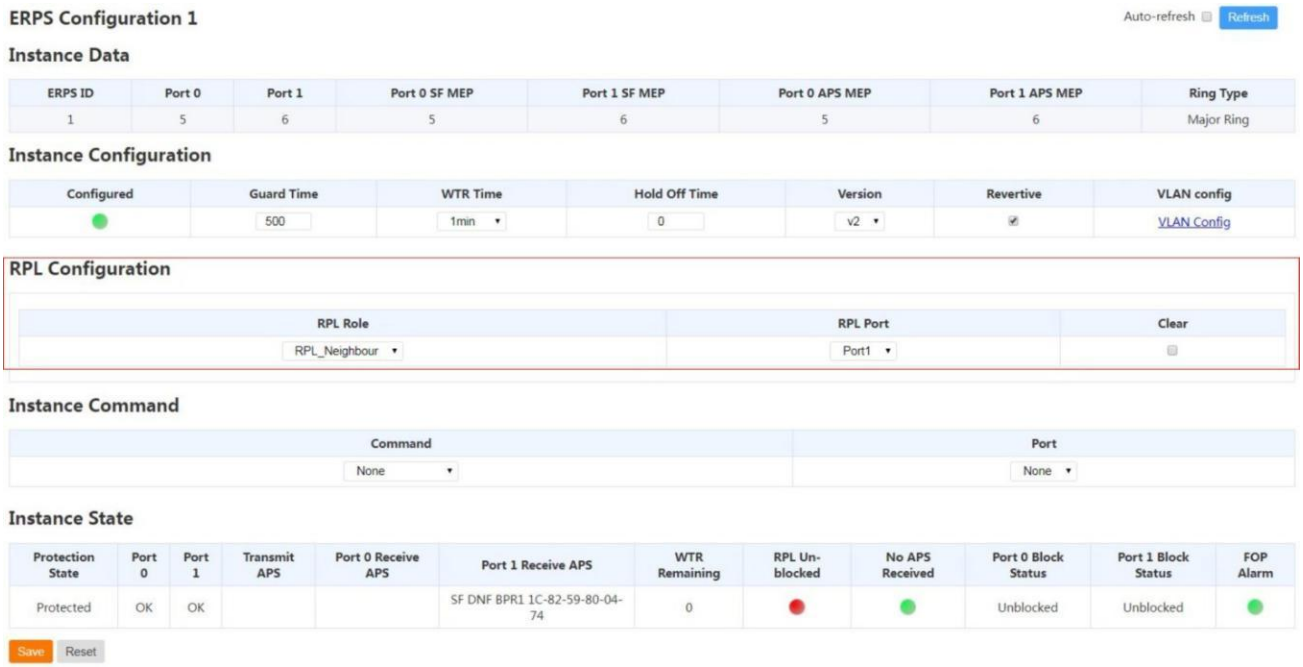
Step 3: Create and configure the ERPS protection group.
Select "ERPS" under "Configuration" in the navigation bar, enter the ERPS configuration interface, and click "Add Protection Group" button to add protection group 1.

Chart Figure 12-31 Single Ring Case SwitchB ERPS Configuration 1



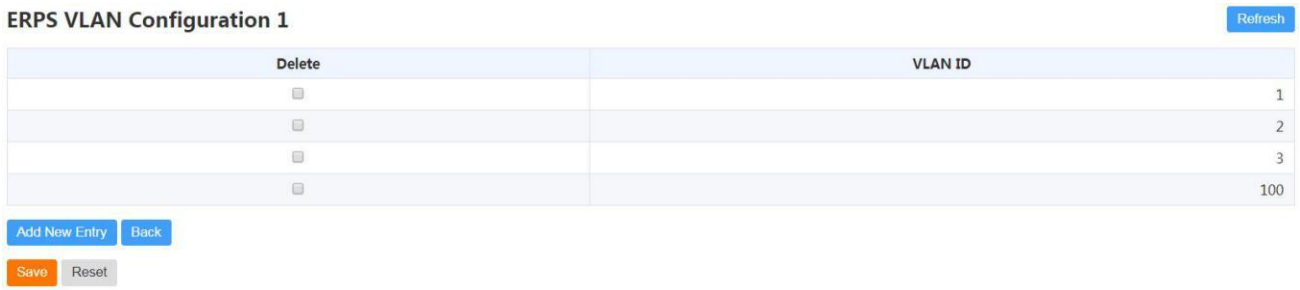
Click the [Save] button to complete the addition of the protection group. Click the protection group 1 again to enter the parameter configuration interface, and set Port1 as the RPL Neighbour role according to the planned configuration.

Chart Figure 12-32 Single Ring Case SwitchB ERPS Configuration 2



Click [VLAN_CONFIG] to enter the VLAN configuration page, and click "Add Entry" to add VLAN 1,2,3,100 in turn. To protect the VLAN, click "Save" to complete configuration.

Chart Figure 12-33 Single Ring Case SwitchB ERPS Configuration 3



Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

12.4.5 Configure switchC

Step 1: VLAN and port configuration.
Select "VLAN" from the "Configuration" sub-item in the navigation bar. Configuration allows access to VLANs 1,2,3,100, port1/5, port1/6 mode Trunk, allows VLANs 1,2,3,100. Click "Save" to complete the configuration.

Chart Figure 12-34 Single Ring Case SwitchC VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1-3,100
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
6	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	

Save Reset

Step 2: Create and configure MEP nodes.

1) Select [MEP] in the [Configuration] sub-item of the navigation bar, and click the [Add MEP] button to add port 5 as MEP 5, and Tagged VID as 100.

Chart Figure 12-35 Single Ring Case SwitchC MEP Configuration 1

Maintenance Entity Point Refresh

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
Delete	5	Port	Mep	Down	5	0	1	100		

Add New MEP Save Reset

2) Click the [Save] button to complete the addition of the entity node. Click instance 5 again to enter the instance data configuration and enable the RAPS function.

Chart Figure 12-36 Single-ring case SwitchC MEP configuration 2.

MEP Configuration Refresh

Instance Data

Instance	Domain	Mode	Direction	Residence Port	Flow Instance	Tagged VID	EPS Instance	This MAC	Oper State
5	Port	Mep	Down	5		100	0	1C-82-59-80-04-69	Up

Instance Configuration

Level	Format	Domain Name	MEG id	MEP id	Tagged VID	Syslog	cLevel	cMEG	cMEP	cAIS	cLCK	cLoop	cConfig	cDEG	cSSF	aBLK	aTSD	aTSF
0	ITU ICC		ICC000MEG0000	1	100	☐	●	●	●	●	●	●	●	●	●	●	●	●

Peer MEP Configuration

Delete	Peer MEP ID	Unicast Peer MAC		cLOC	cRDI	cPeriod	cPriority
	No Peer MEP Added						

Add New Peer MEP

Functional Configuration

Continuity Check				APS Protocol				
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet
☐	0	1 fsec	☐	☑	0	Multi	R-APS	1

Fault Management Performance Monitoring

TLV Configuration

Organization Specific TLV (Global)				
OUI First	OUI Second	OUI Third	Sub-Type	Value
0	0	12	1	2

TLV Status

Peer MEP ID	CC Organization Specific						CC Port Status		CC Interface Status	
	OUI First	OUI Second	OUI Third	Sub-Type	Value	Last RX	Value	Last RX	Value	Last RX

Link State Tracking

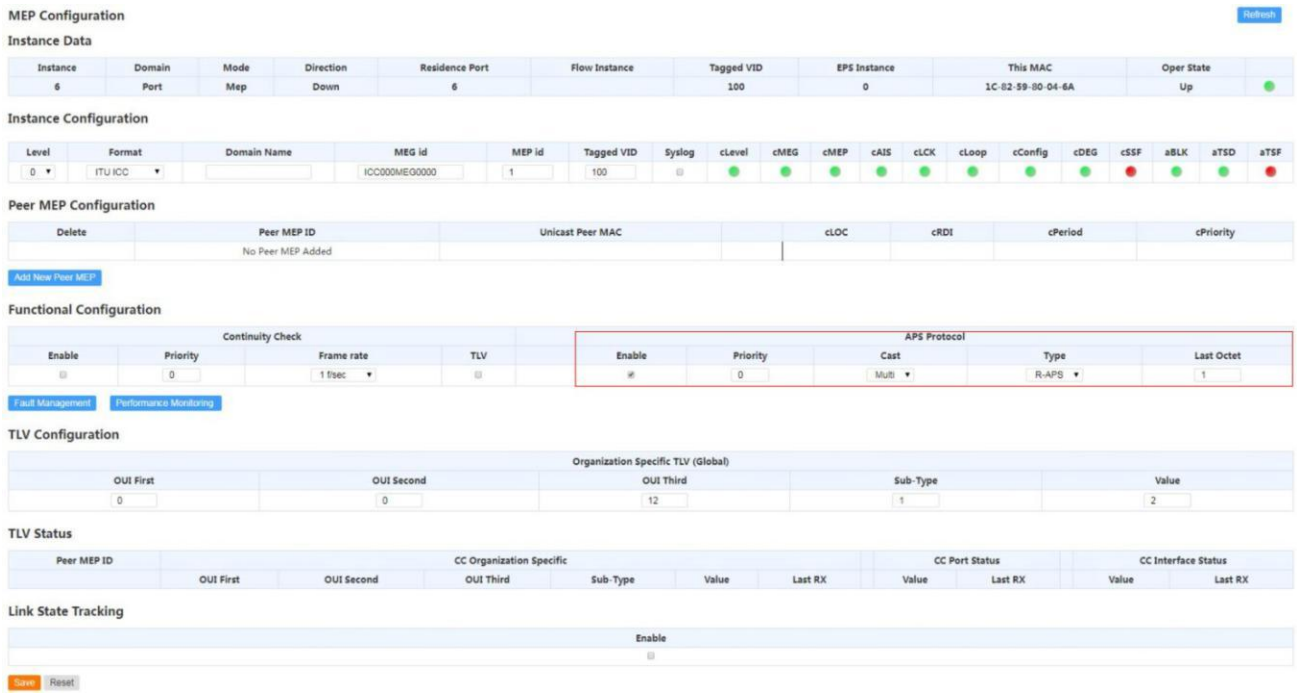
Enable
☐

Save Reset

3) Similarly, add port 6 as MEP 6, Tagged VID as 100, and enable the RAPS function in the instance data configuration.

Chart Figure 12-37 Single Ring Case SwitchC MEP Configuration 3

Chart Figure 12-38 Single Ring Case SwitchC MEP Configuration 4

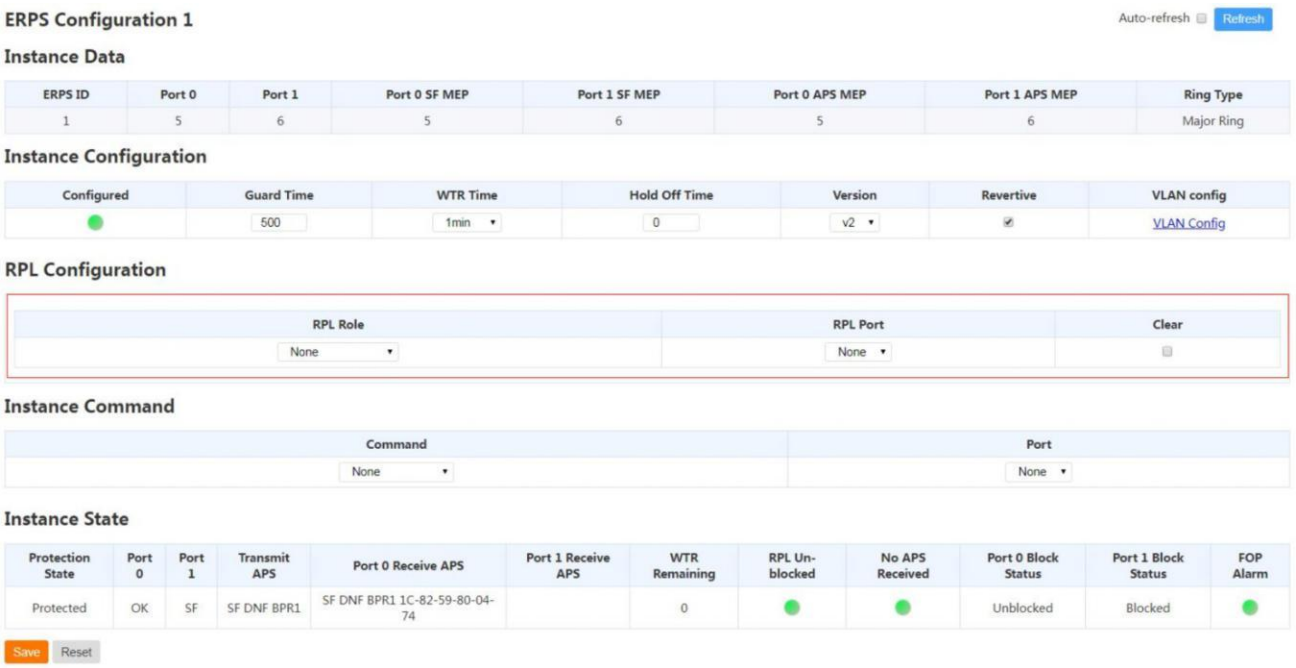


Step 3: Create and configure the ERPS protection group.
Select "ERPS" under "Configuration" in the navigation bar, enter the ERPS configuration interface, and click "Add Protection Group" button to add protection group 1.

Chart Figure 12-39 Single Ring Case SwitchC ERPS Configuration 1

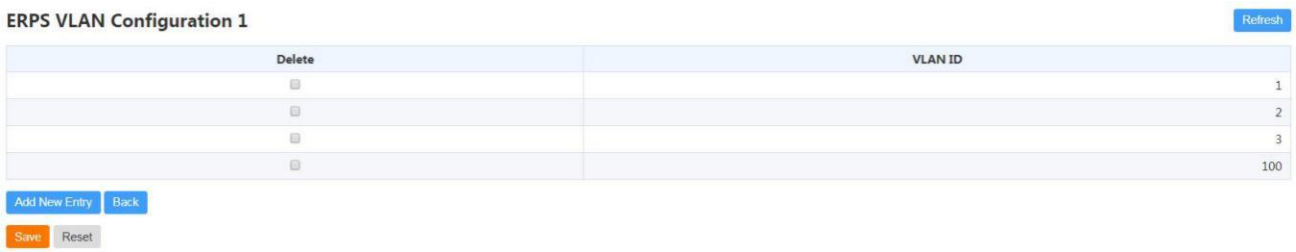
Click the [Save] button to complete the addition of the protection group. Click the protection group 1 again to enter the parameter configuration interface. According to the planned configuration, there is no need to set the RPL role.

Chart Figure 12-40 Single Ring Case SwitchC ERPS Configuration 2



Click [VLAN_CONFIG] to enter the VLAN configuration page, and click "Add Entry" to add VLAN 1,2,3,100 in turn. To protect the VLAN, click "Save" to complete configuration.

Chart Figure 12-41 Single Ring Case SwitchC ERPS Configuration 3



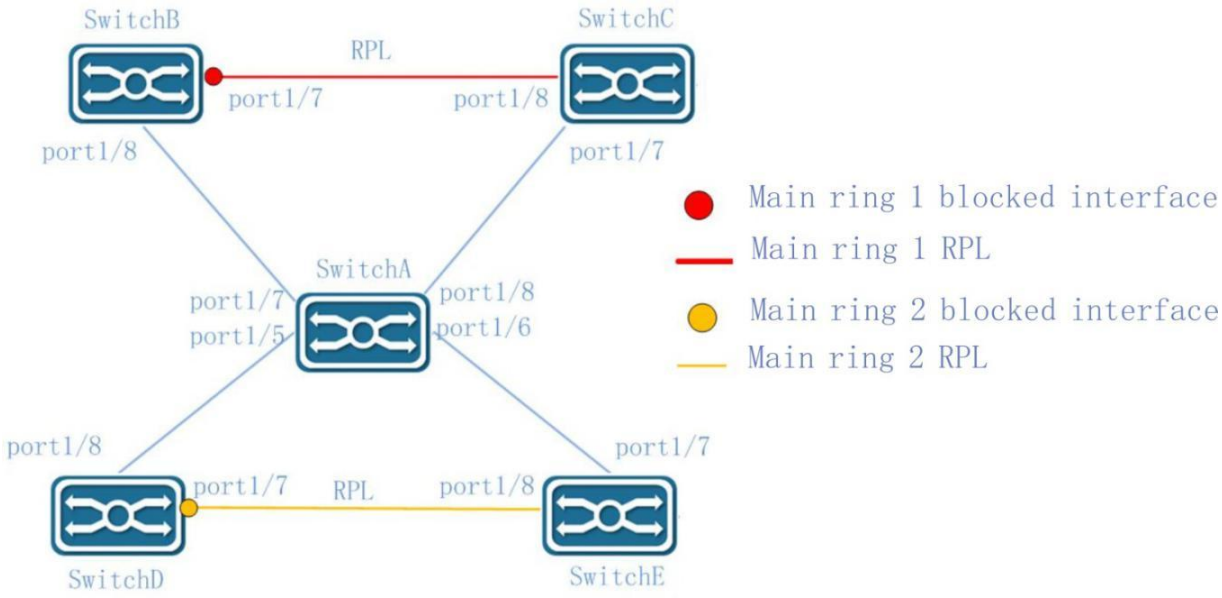
Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

12.5 Tangent ring configuration example

12.5.1 Case requirements

The topology diagram is as follows. SwitchA is located in the central computer room and can be supervised and maintained by the administrator in real time. It has high reliability; SwitchB-E is distributed in various deployment points. In order to improve the reliability of the network, avoid single-link external connections. Point of failure risk, while avoiding the risk of single-machine failure that may occur when dual-link external single-machines are connected, the method of dual-link external connections forming a ring network is adopted. The data VLANs are 1, 2, and 3 respectively, and each ring network is required to converge quickly when a single point of failure occurs to avoid user network interruption.

Chart Figure 12-42 Tangent Ring Case



12.5.2 Configuration planning

The configuration of tangential rings is similar to that of single rings in that it is equivalent to configuring two independent primary rings.

In this example, the switchA, switchB, switchC ring definition is numbered "1", the switchB "port1/7", the RAPS management VLAN is "100", the switchA, switchD, switchE ring is numbered "2",

The blocking port is "port1/7" of SWITCHD, and the RAPS management VLAN is "101". The specific parameters are shown below.

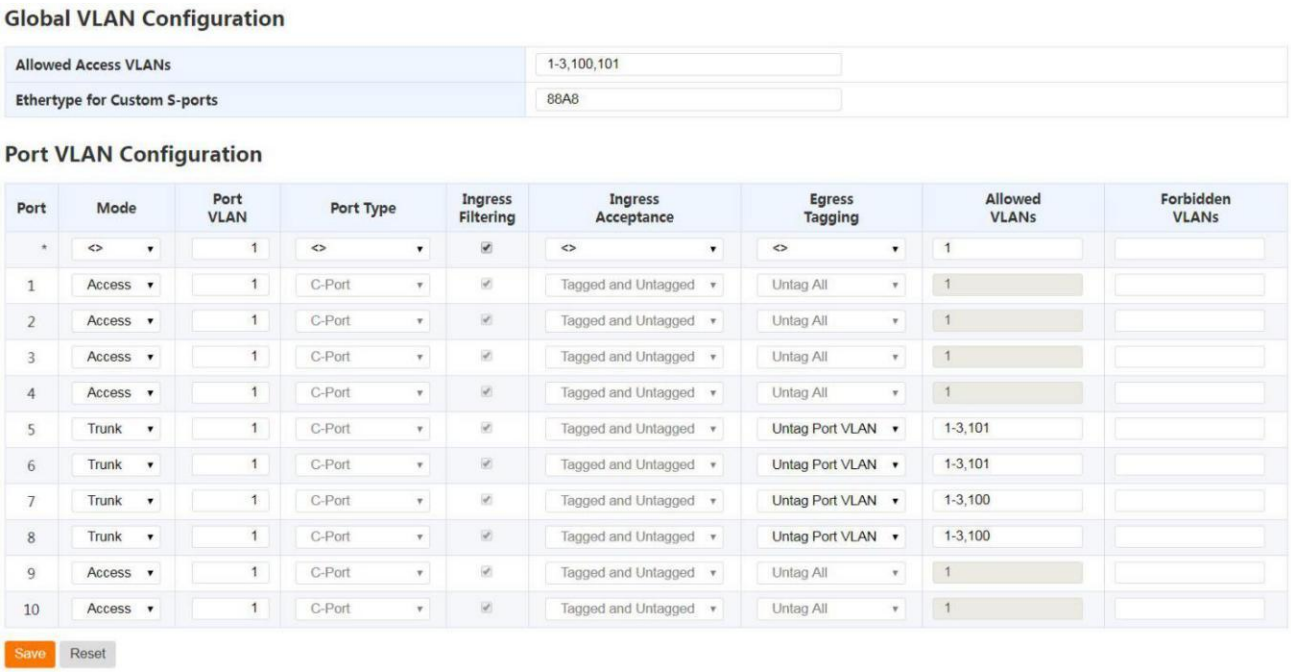
Equipment	Ring No.	RAPS VLAN	Owner Port	NeighborPort	Interconnect node	Associated main ring
SwitchA	1	100	None	None	\	\
	2	101	None	None	\	\
SwitchB	1	100	port1/7	None	\	\
SwitchC	1	100	None	port1/8	\	\
SwitchD	2	101	port1/7	None	\	\
SwitchE	2	101	None	port1/8	\	\

12.5.3 Configure SwitchA

Step 1: VLAN and port configuration.

Option in the navigation item configuration 】【, VLAN 】【 configuration allows access to VLANs to 1,2,3,100,101, port port1/5, port1/6, port1/7, port1/8 patterns for the Trunk, port port1/5, port1/6 allow VLANs for 1, 2, 3,
101, Port 1/7, Port 1/8 allow VLANs of 1,2,3,100, click "Save" button to complete the configuration.

Chart Figure 12-43 Tangent Ring Case SwitchA VLAN Configuration



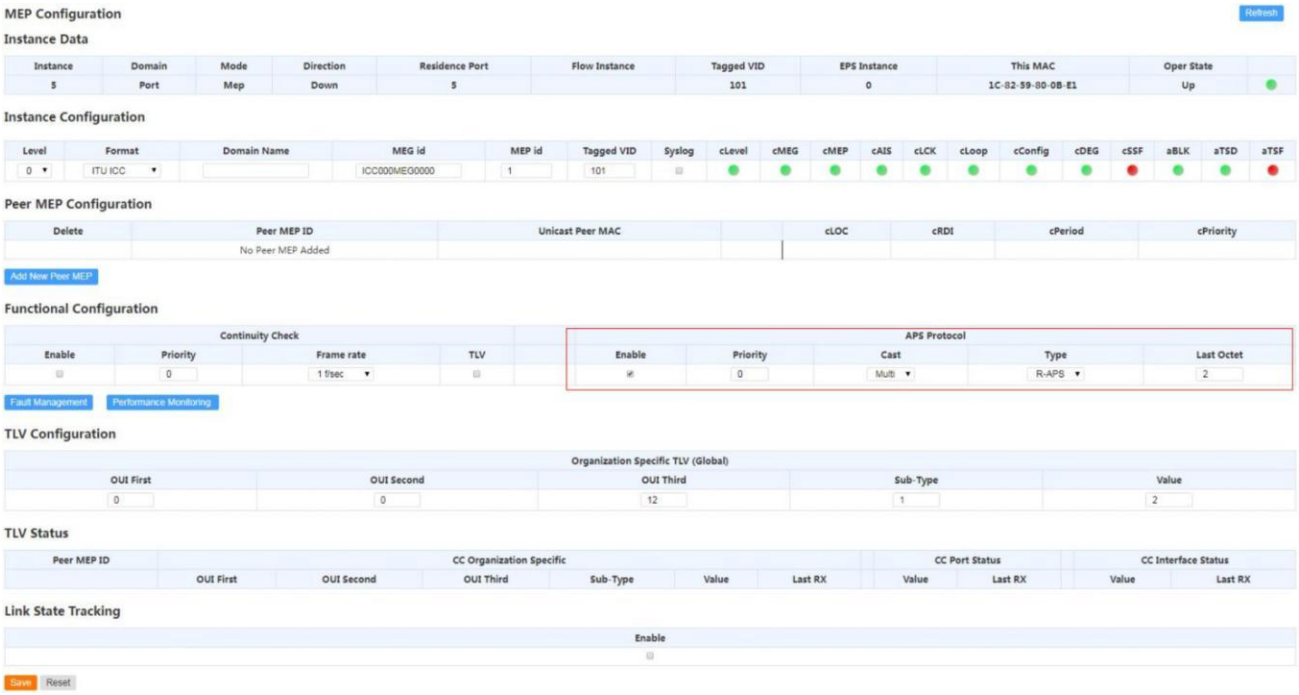
Step 2: Create and configure the MEP node.

1) Select "MEP" in the "Configuration" sub-item of the navigation bar and click "Add MEP" button to add port 5 as MEP 5 and Tagged VID as 101.

Chart Figure 12-44 Tangent Ring Case SwitchA MEP Configuration 1

2) Click the [Save] button to complete the addition of the entity node. Click instance 5 again to enter the instance data configuration, enable the RAPS function, and the last byte is consistent with the ring ID, set to 2.

Chart Figure 12-45 Tangent Ring Case SwitchA MEP Configuration 2



3) In the same way, add MEP nodes of ports 6-8, and enter the instance data configuration to enable the RAPS function; port 6 belongs to ring 2, tagged VID is 101, and the last byte of RAPS is 2; port 7-8 belongs to ring 1, and tagged VID is 100, the last byte of RAPS is 1.

Step 3: Create and configure ERPS protection group.

1) Select [ERPS] under [Configuration] in the navigation bar, enter the ERPS configuration interface, click the [Add protection group] button, add protection group 1, ports port1/7 and port1/8, and the corresponding MEPs are 7 and 8.

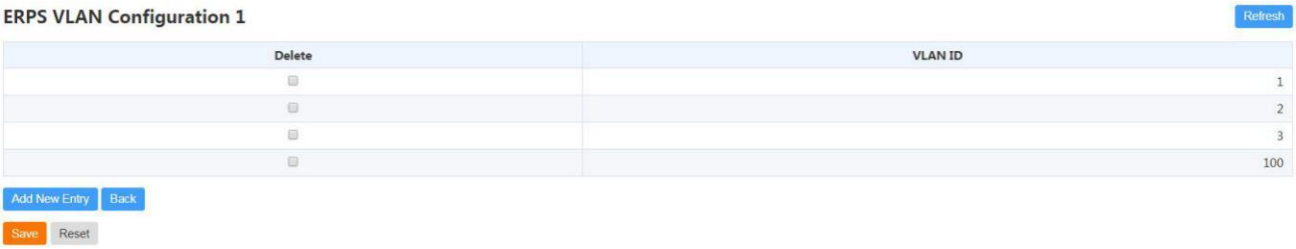
Chart Figure 12-46 Tangent Ring Case SwitchA ERPS Configuration 1

Click the [Save] button to complete the addition of the protection group. Click protection group 1 again to enter the parameter configuration interface.

Chart Figure 12-47 Tangent Ring Case SwitchA ERPS Configuration 2

Click [VLAN_CONFIG] to enter the VLAN configuration page, and click "Add Entry" to add VLAN 1,2,3,100 in turn. To protect the VLAN, click "Save" to complete configuration.

Chart Figure 12-48 Tangent Ring Case SwitchA ERPS Configuration 3



2) Similarly, add ERPS protection group 2 and configure the corresponding VLAN.

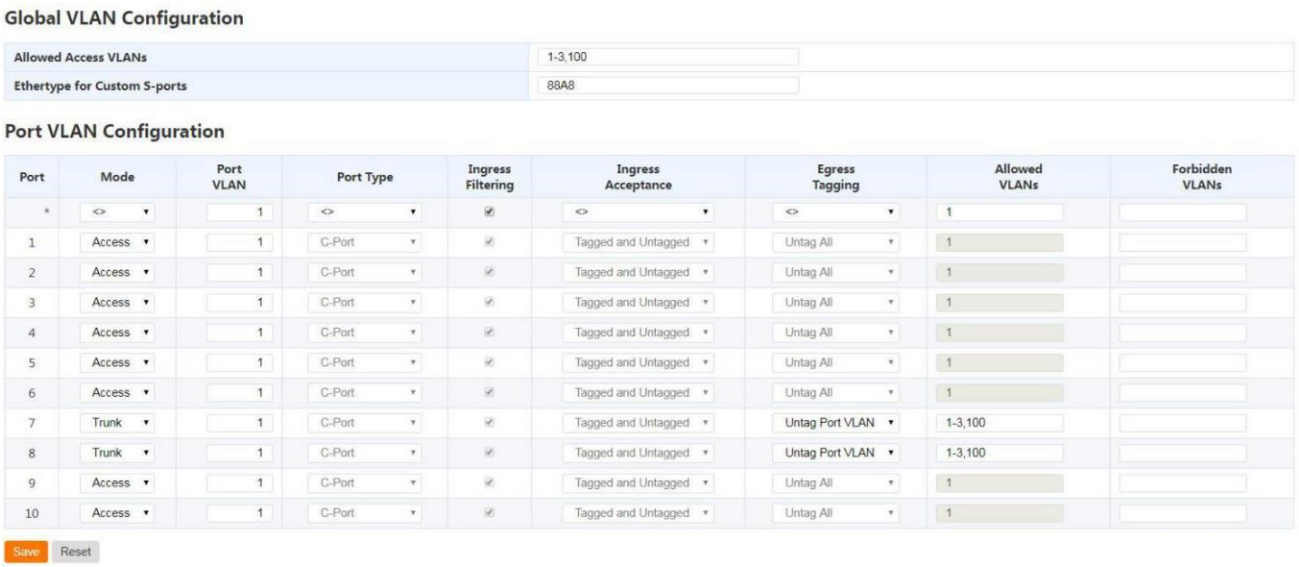
Chart Figure 12-49 Tangent Ring Case SwitchA ERPS Configuration 4

Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

12.5.4 12.5.4 Configure switchB

Step 1: VLAN and port configuration.
Select "VLAN" from the "Configuration" sub-item in the navigation bar. Configuration allows access to VLANs 1,2,3,100, port1/7, port1/8 mode Trunk, allows VLANs 1,2,3,100. Click "Save" to complete the configuration.

Chart Figure 12-50 Tangent Ring Case SwitchB VLAN Configuration



Global VLAN Configuration

Allowed Access VLANs	1-3,100
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>		<>	<>	1	
1	Access	1	C-Port		Tagged and Untagged	Untag All	1	
2	Access	1	C-Port		Tagged and Untagged	Untag All	1	
3	Access	1	C-Port		Tagged and Untagged	Untag All	1	
4	Access	1	C-Port		Tagged and Untagged	Untag All	1	
5	Access	1	C-Port		Tagged and Untagged	Untag All	1	
6	Access	1	C-Port		Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port		Tagged and Untagged	Untag Port VLAN	1-3,100	
8	Trunk	1	C-Port		Tagged and Untagged	Untag Port VLAN	1-3,100	
9	Access	1	C-Port		Tagged and Untagged	Untag All	1	
10	Access	1	C-Port		Tagged and Untagged	Untag All	1	

Save Reset

Step 2: Create and configure the MEP node.

1) Select [MEP] in the [Configuration] sub-item of the navigation bar, and click the [Add MEP] button to add port 7 as MEP 7, and Tagged VID as 100.

Chart Figure 12-51 Tangent Ring Case SwitchB MEP Configuration 1

Maintenance Entity Point

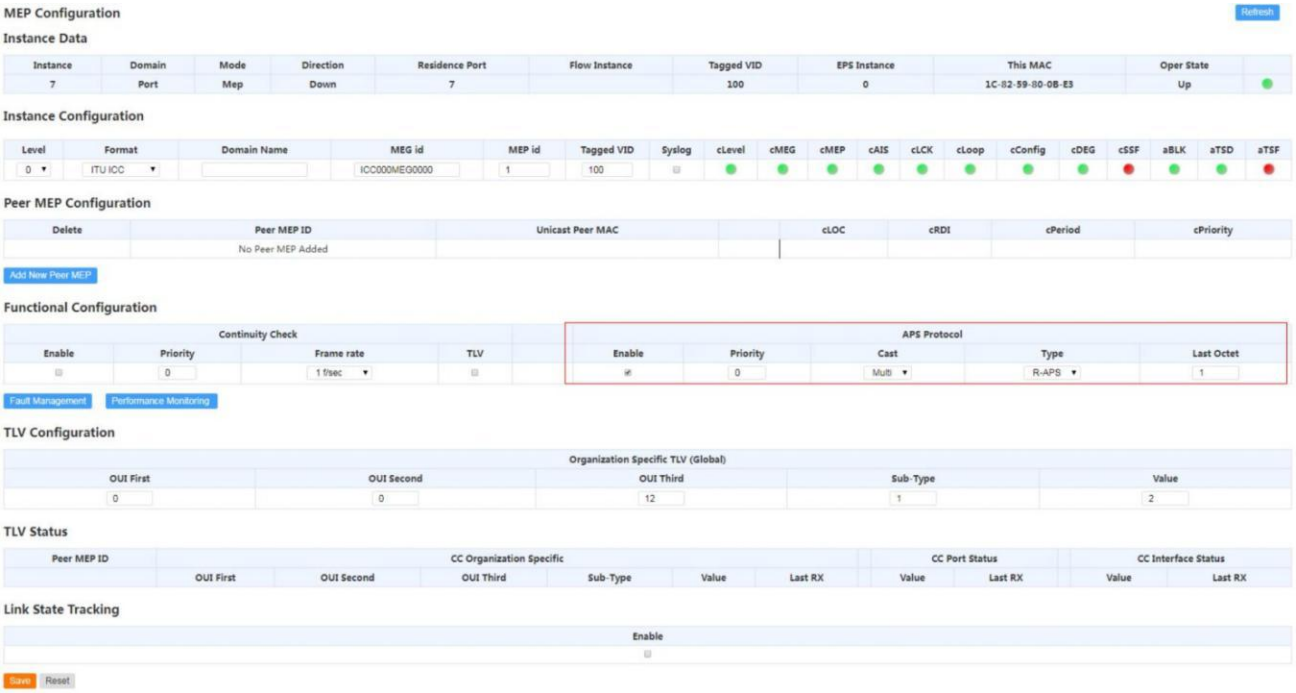
Refresh

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
Delete	7	Port	Mep	Down	7	0	1	100		

Add New MEP Save Reset

2) Click the [Save] button to complete the addition of the entity node. Re-click instance 7 to enter the instance data configuration, enable the RAPS function, the last byte is consistent with the ring ID, set to 1

Chart Figure 12-52 Tangent Ring Case SwitchB MEP Configuration 2



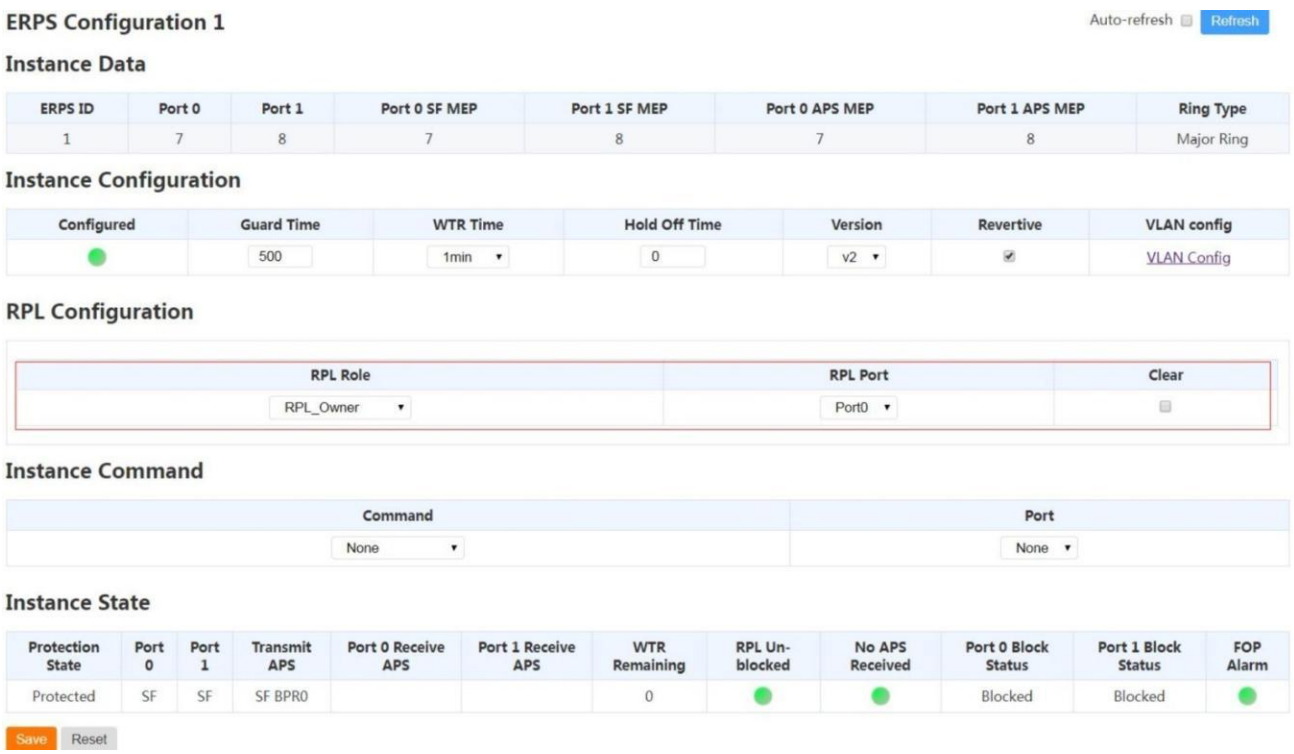
3) In the same way, add the MEP node of port 8, the Tagged VID is 100, and the RAPS function is enabled in the instance data configuration. The last byte is consistent with the ring ID and is set to 1.

Step 3: Create and configure the ERPS protection group.
Select "ERPS" under "Configuration" in the navigation bar, enter the ERPS configuration interface, click "Add Protection Group" button, add protection group 1, port port1/7 and port1/8, and the corresponding MEP is 7 and 8.

Chart Figure 12-53 Tangent Ring Case SwitchB ERPS Configuration 1

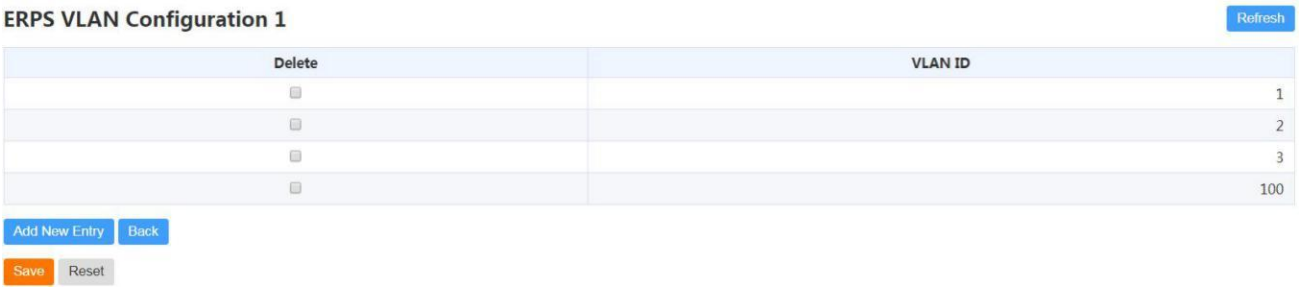
Click the [Save] button to complete the addition of the protection group. Click the protection group 1 again to enter the parameter configuration interface, and set Port0 as the RPL Owner role according to the planned configuration.

Chart Figure 12-54 Tangent Ring Case SwitchB ERPS Configuration 2



Click [VLAN_CONFIG] to enter the VLAN configuration page, and click "Add Entry" to add VLAN 1,2,3,100 in turn. To protect the VLAN, click "Save" to complete configuration.

Chart Figure 12-55 Tangent Ring Case SwitchB ERPS Configuration 3



Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

12.5.5 Configure SwitchC

Step 1: VLAN and port configuration.

Select "VLAN" from the "Configuration" sub-item in the navigation bar. Configuration allows access to VLANs 1,2,3,100, port1/7, port1/8 mode Trunk, allows VLANs 1,2,3,100. Click "Save" to complete the configuration.

Chart Figure 12-56 Tangent Ring Case SwitchC VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1-3,100
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Save Reset

Step 2: Create and configure the MEP node.

1) Select "MEP" in the "Configuration" sub-item of the navigation bar and click "Add MEP" button to add port 7 as MEP 7 and Tagged VID as 100.

Chart Figure 12-57 Tangent Ring Case SwitchC MEP Configuration 1

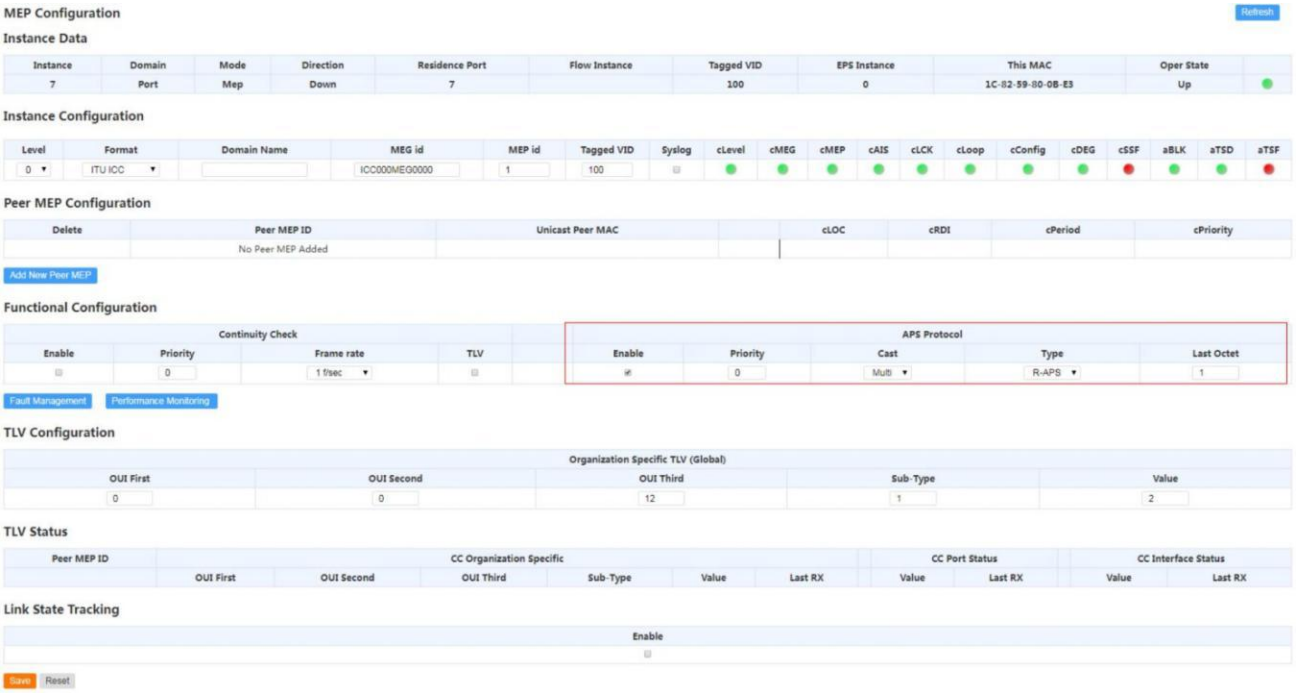
Maintenance Entity Point Refresh

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
Delete	7	Port	Mep	Down	7	0	1	100		

Add New MEP Save Reset

1) Click the [Save] button to complete the addition of the entity node. Re-click instance 7 to enter the instance data configuration, enable the RAPS function, the last byte is consistent with the ring ID, set to 1

Chart Figure 12-58 Tangent Ring Case SwitchC MEP Configuration 2



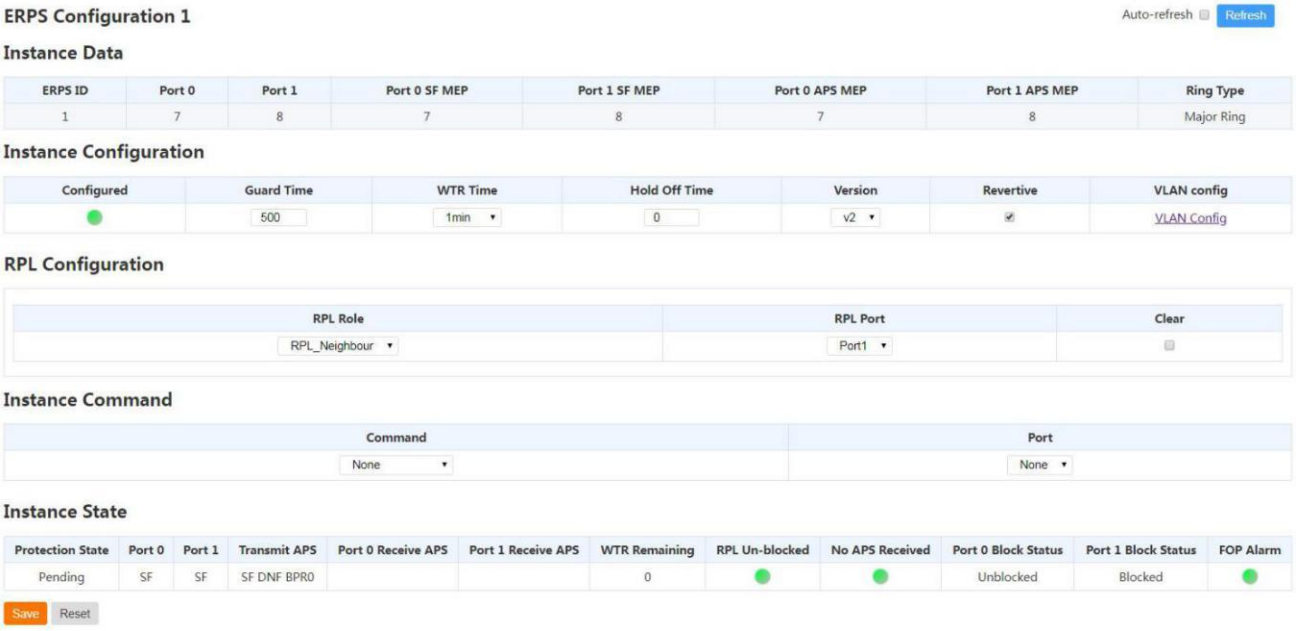
4) In the same way, add the MEP node of port 8, the Tagged VID is 100, and the RAPS function is enabled in the instance data configuration. The last byte is consistent with the ring ID and is set to 1.

Step 3: Create and configure the ERPS protection group.
Select "ERPS" under "Configuration" in the navigation bar, enter the ERPS configuration interface, click "Add Protection Group" button, add protection group 1, port port1/7 and port1/8, and the corresponding MEP is 7 and 8.

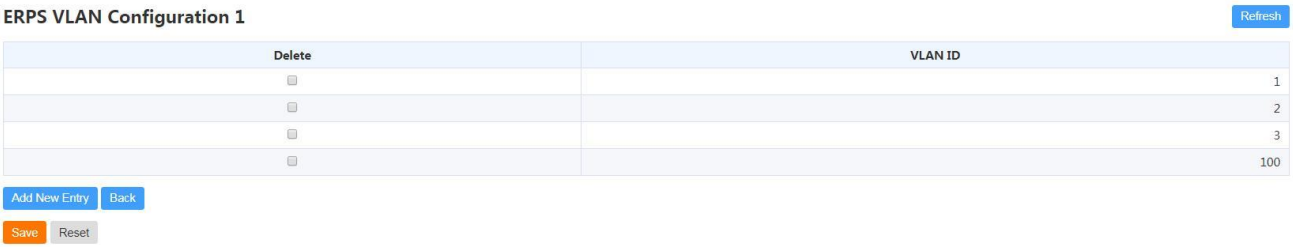
Chart Figure 12-59 Tangent Ring Case SwitchC ERPS Configuration 1

Click the [Save] button to complete the addition of the protection group. Click the protection group 1 again to enter the parameter configuration interface, and set Port1 as the RPL Neighbour role according to the planned configuration.

Chart Figure 12-60 Tangent Ring Case SwitchC ERPS Configuration 2



Click [VLAN_CONFIG] to enter the VLAN configuration page, and click "Add Entry" to add VLAN 1,2,3,100 in turn. To protect the VLAN, click "Save" to complete configuration.
Chart Figure 12-61 Tangent Ring Case SwitchC ERPS Configuration 3



Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

12.5.6 Configure SwitchD

Step 1: VLAN and port configuration.
Select "VLAN" from the "Configuration" sub-item in the navigation bar. Configuration allows VLANs to be accessed as 1,2,3,101, port1/7, port1/8 mode as Trunk, allows VLANs to be accessed as 1,2,3,101. Click "Save" to complete the configuration.
Chart Figure 12-62 Tangent Ring Case SwitchD VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1-3,101
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,101	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,101	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Save Reset

Step 2: Create and configure the MEP node.

1) Select "MEP" in the "Configuration" sub-item of the navigation bar and click "Add MEP" button to add port 7 as MEP 7 and Tagged VID as 101.

Chart Figure 12-63 Tangent Ring Case SwitchD MEP Configuration 1

维护实体节点

删除	实例	域	模式	方向	所在端口	级别	流实例	Tagged VID	MAC	告警
☐	7	Port	Mep	Down	7	0		101	1C-82-59-80-0B-12	

添加MEP 保存 复位

1) Click the [Save] button to complete the addition of the entity node. Re-click instance 7 to enter the instance data configuration, enable the RAPS function, the last byte is consistent with the ring ID, set to 2

Chart Figure 12-64 Tangent Ring Case SwitchD MEP Configuration 2

MEP Configuration Refresh

Instance Data

Instance	Domain	Mode	Direction	Residence Port	Flow Instance	Tagged VID	EPS Instance	This MAC	Oper State	
7	Port	Mep	Down	7		101	0	1C-82-59-80-0B-12	Up	

Instance Configuration

Level	Format	Domain Name	MEG id	MEP id	Tagged VID	Syslog	cLevel	cMEG	cMEP	cAIS	cLCK	cLoop	cConfig	cDEG	cSSF	aBLK	aTSD	aTSF
0	ITU ICC		ICC000MEG0000	1	101	☐	●	●	●	●	●	●	●	●	●	●	●	●

Peer MEP Configuration

Delete	Peer MEP ID	Unicast Peer MAC		cLOC	cRDI	cPeriod	cPriority
	No Peer MEP Added						

Add New Peer MEP

Functional Configuration

Continuity Check				APS Protocol				
Enable	Priority	Frame rate	TLV	Enable	Priority	Cast	Type	Last Octet
☐	0	1 f/sec	☐	☑	0	Multi	R-APS	2

Fault Management Performance Monitoring

TLV Configuration

Organization Specific TLV (Global)				
OUI First	OUI Second	OUI Third	Sub-Type	Value
0	0	12	1	2

TLV Status

Peer MEP ID	CC Organization Specific						CC Port Status		CC Interface Status	
	OUI First	OUI Second	OUI Third	Sub-Type	Value	Last RX	Value	Last RX	Value	Last RX

Link State Tracking

Enable
☐

Save Reset

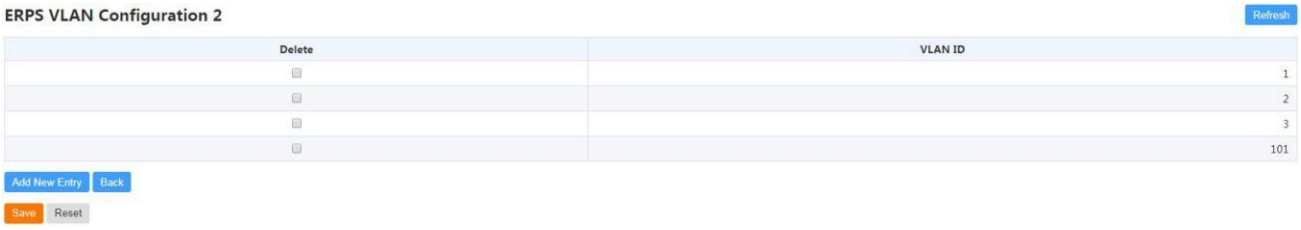
2) In the same way, add the MEP node of port 8, the Tagged VID is 101, and the RAPS function is enabled in the instance data configuration. The last byte is consistent with the ring ID and is set to 2.

Step 3: Create and configure the ERPS protection group.
Select "ERPS" under "Configuration" in the navigation bar, enter the ERPS configuration interface, click "Add Protection Group" button, add protection group 2, ports port1/7 and port1/8, and the corresponding MEP is 7 and 8.
Chart Figure 12 65 Tangent Ring Case SwitchD ERPS Configuration 1

Click the [Save] button to complete the addition of the protection group. Click the protection group 2 again to enter the parameter configuration interface, and set Port0 as the RPL Owner role according to the planned configuration. .

Chart Figure 12-66 Tangent Ring Case SwitchD ERPS Configuration 2

Click "VLAN_Config" to enter the VLAN configuration page, and click "add entry" to add VLAN 1,2,3,101 in turn. To protect the VLAN, click "save" to complete configuration.
Chart Figure 12-67 Tangent Ring Case SwitchD ERPS Configuration 3



Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

12.5.7 Configure SwitchE

Step 1: VLAN and port configuration.
Select "VLAN" from the "Configuration" sub-item in the navigation bar. Configuration allows VLANs to be accessed as 1,2,3,101, port1/7, port1/8 mode as Trunk, allows VLANs to be accessed as 1,2,3,101. Click "Save" to complete the configuration.
Chart Figure 12-68 Tangent Ring Case SwitchE VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1-3,100
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Save Reset

Step 2: Create and configure MEP nodes.

1) Select [MEP] in the [Configuration] sub-item of the navigation bar, and click the [Add MEP] button to add port 7 as MEP 7, and Tagged VID as 101.

Chart Figure 12-69 Tangent Ring Case SwitchE MEP Configuration 1

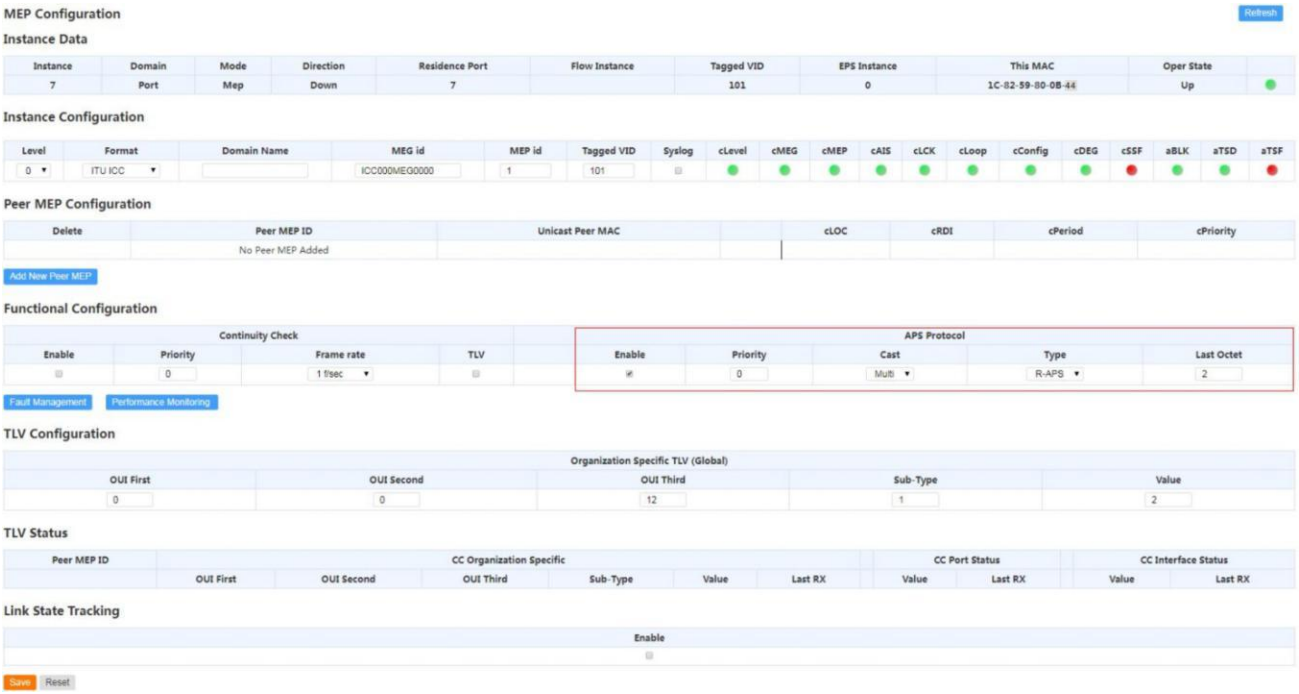
Maintenance Entity Point Refresh

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
☐	7	Port	Mep	Down	7	0		101	1C-82-59-80-08-44	

Add New MEP Save Reset

2) Click the [Save] button to complete the addition of the entity node. Re-click instance 7 to enter the instance data configuration, enable the RAPS function, the last byte is consistent with the ring ID, set to 2

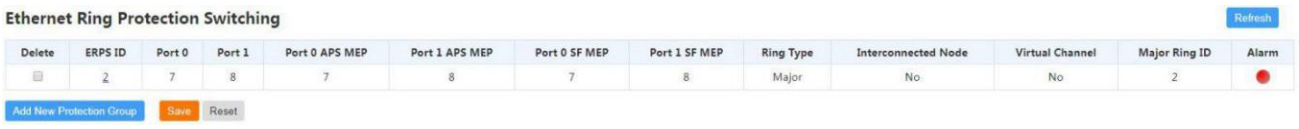
Chart Figure 12-70 Tangent Ring Case SwitchE MEP Configuration 2



3) In the same way, add the MEP node of port 8, the Tagged VID is 101, and the RAPS function is enabled in the instance data configuration. The last byte is consistent with the ring ID and is set to 2.

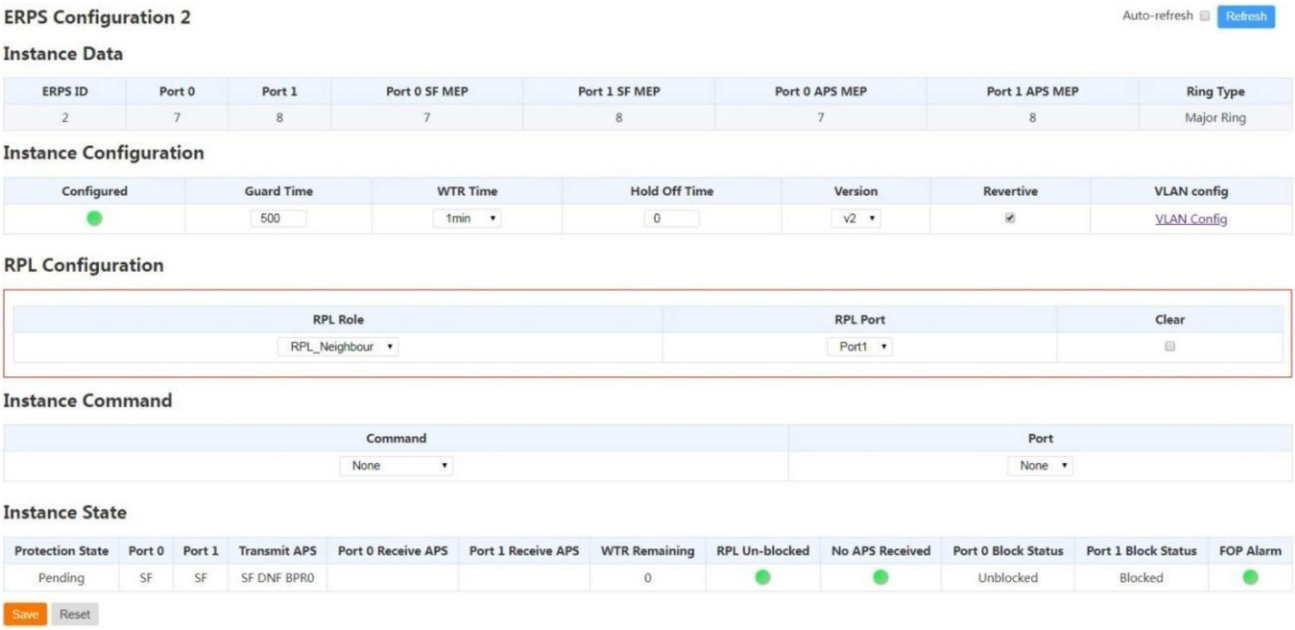
Step 3: Create and configure the ERPS protection group.
Select "ERPS" under "Configuration" in the navigation bar, enter the ERPS configuration interface, click "Add Protection Group" button, add protection group 2, ports port1/7 and port1/8, and the corresponding MEP is 7 and 8.

Chart Figure 12-71 Tangent Ring Case SwitchE ERPS Configuration 1



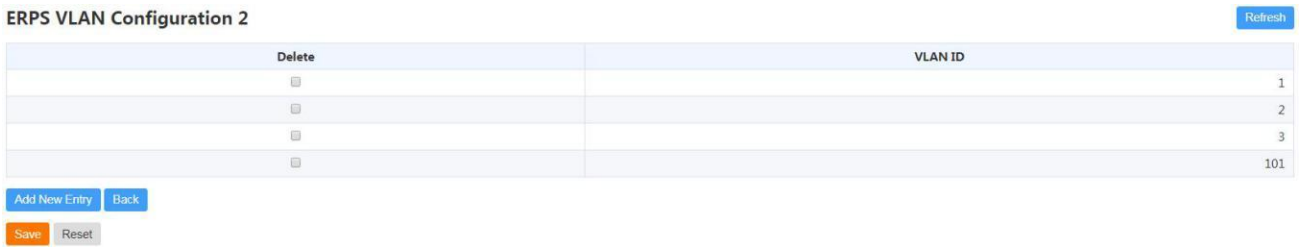
Click the [Save] button to complete the addition of the protection group. Click the protection group 2 again to enter the parameter configuration interface, and set Port1 as the RPL Neighbour role according to the planned configuration.

Chart Figure 12-72 Tangent Ring Case SwitchE ERPS Configuration 2



Click "VLAN_Config" to enter the VLAN configuration page, and click "add entry" to add VLAN 1,2,3,101 in turn. To protect the VLAN, click "save" to complete configuration.

Chart Figure 12-73 Tangent Ring Case SwitchE ERPS Configuration 3



Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

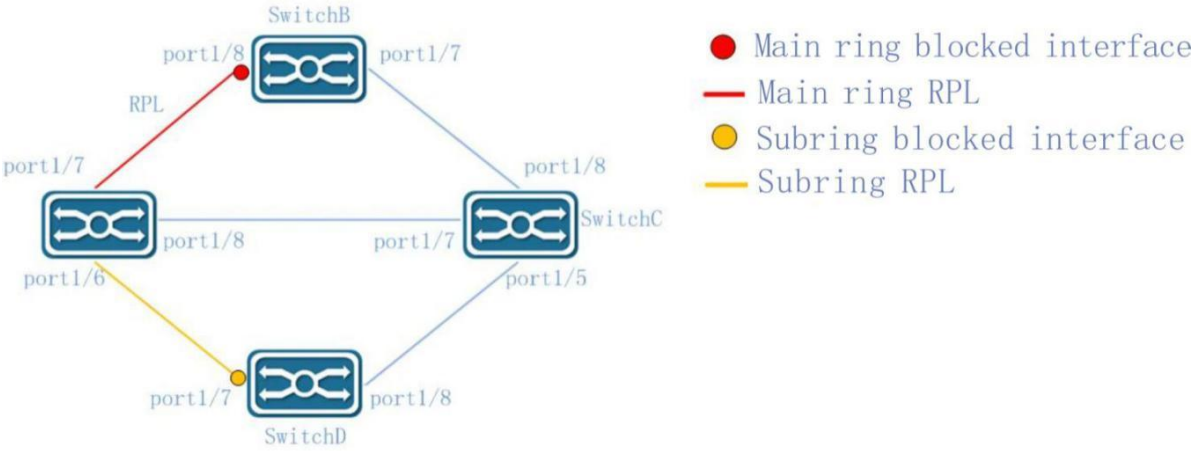
12.6 Intersecting ring configuration examples

12.6.1 Case requirements

SWITCHA, SWITCHB, SWITCHC, SWITCHD are intersecting rings, and the data VLAN is 1,2,3, which requires that fast convergence can be achieved when a single point of failure occurs in each ring.

There can be at most two fault points (different loops) in the network, and no user cut off the network, so as to achieve the optimal reliability.

Chart Figure 12-74 Intersecting Ring Case



12.6.2 Configuration planning

Note

- Primary ring and subring must have different ring IDs.
- The RAPS management VLAN within the primary ring and subring must be different
- In a subring, the device that connects the subring and the primary ring is defined as an interconnected node, and the associated instance is set to the primary ring.

There is no strict distinction between a primary ring and a subring. It is generally assumed that one of the primary rings is a subring, and the other is a subring.

In this example, the switchA, switchB, switchC ring is defined as the primary ring, the ring number is "1", the blocking point is the switchB port1/7 port, and the RAPS management VLAN is "100".

The ring composed of switchA, switchB and switchD is a sub-ring, the ring number is "2", the blocking point is the port1/7 port of switchD, and the RAPS management VLAN is "101".

Specific parameters are described below.

Equipment	Ring No.	RAPS VLAN	Owner Port	Neighbor Port	Interconnect node	Associated main ring
SwitchA	1	100	None	port1/7	\	\
	2	101	None	port1/6	Yes	1
SwitchB	1	100	port1/8	None	\	\
SwitchC	1	100	None	None	\	\

	2	101	None	None	Yes	1
SwitchD	2	101	port1/7	None	\	\

12.6.3 Configure SwitchA

Step 1: VLAN and port configuration.

Select [VLAN] in the [Configuration] sub-item of the navigation bar, configure the allowed access VLANs as 1, 2, 3, 100, 101, port port1/6, port1/7, port1/8 mode as Trunk, and port port1/6 allow VLANs are 1, 2, 3, 101, and port 1/7 and port 1/8 allow VLANs to be 1, 2, 3, 100. Click the [Save] button to complete the configuration.

Chart Figure 12-75 Intersecting Ring Case SwitchA VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1-3,100,101
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,101	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Save Reset

Step 2: Create and configure the MEP node.

1) Select [MEP] in the [Configuration] sub-item of the navigation bar, and click the [Add MEP] button to add port 6 as MEP6 and Tagged VID as 101.

Chart Figure 12-76 Intersecting Ring Case SwitchA MEP Configuration 1

Maintenance Entity Point Refresh

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
Delete	6	Port	Mep	Down	6	0	1	101		

Add New MEP Save Reset

2) Click the [Save] button to complete the addition of the entity node. Click instance 6 again to enter the instance data configuration, enable the RAPS function, the last byte is consistent with the ring ID, set to 2.

Chart Figure 12-77 Intersecting Ring Case SwitchA MEP Configuration 2

3) In the same way, add the MEP node of ports 7-8, and enter the instance data configuration to enable the RAPS function; Port 7-8 belongs to ring 1, the tagged VID is 100, and the last byte of RAPS is 1.

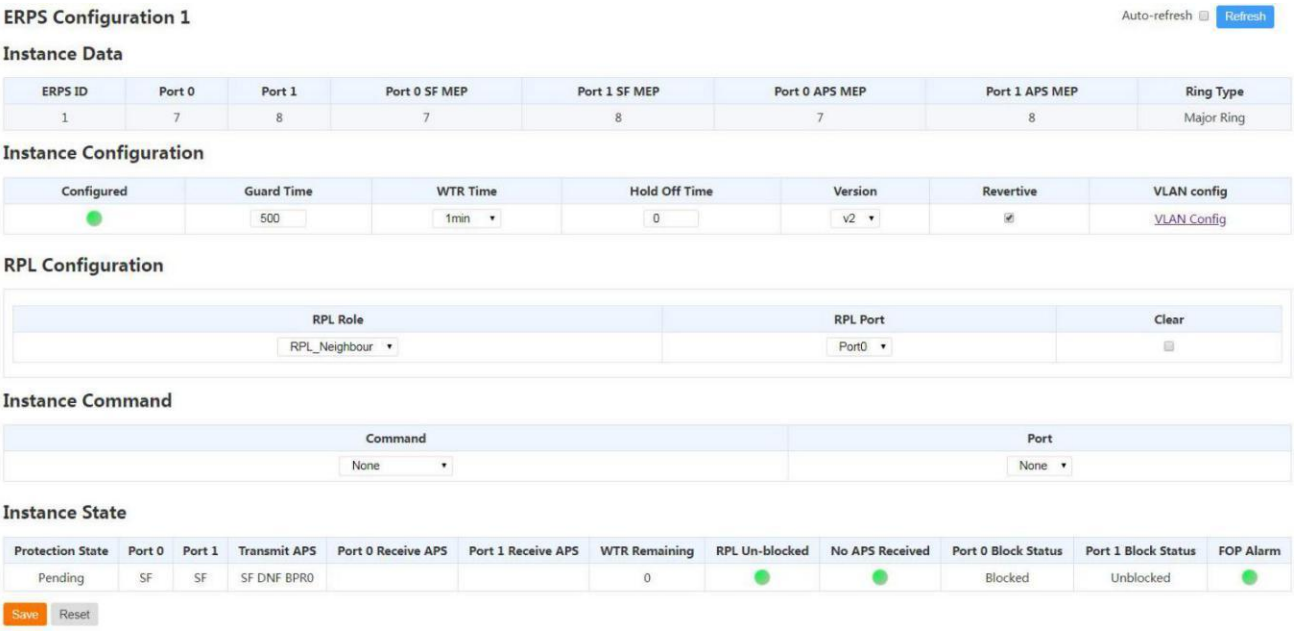
Step 3: Create and configure the ERPS protection group.

1) Select [ERPS] under [Configuration] in the navigation bar, enter the ERPS configuration interface, click the [Add protection group] button, add protection group 1, ports port1/7 and port1/8, and the corresponding MEPs are 7 and 8.

Chart Figure 12- 78 Intersecting Ring Case SwitchA ERPS Configuration 1

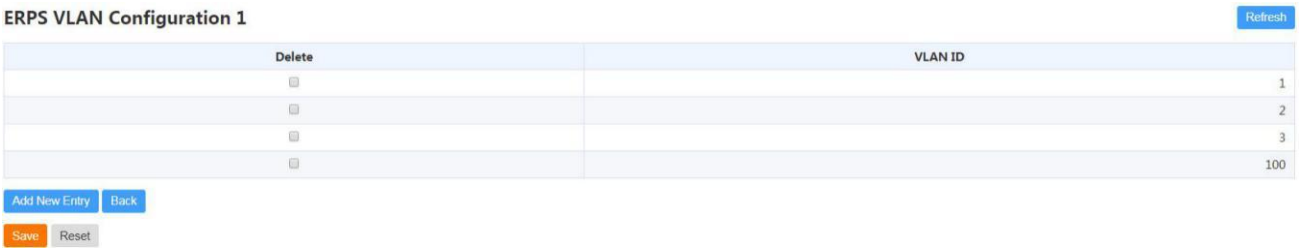
Click the [Save] button to complete the addition of the protection group. Click the protection group 1 again to enter the parameter configuration interface, and set Port0 as the RPL Neighbour role according to the planned configuration.

Chart Figure 12-79 Intersecting Ring Case SwitchA ERPS Configuration 2



Click [VLAN_Config] to enter the VLAN configuration page, click [Add Entry] to add VLAN 1, 2, 3, 100 as protected VLANs, and click [Save] to complete the configuration.

Chart Figure 12-80 Intersecting Ring Case SwitchA ERPS Configuration 3



2) Continue to add ERPS protection group 2, port 0 is port 1/6, port 1 is 0, the corresponding MEP is 6 and 0, the ring type is set to sub-ring, interconnect node, and the main ring ID is 1.

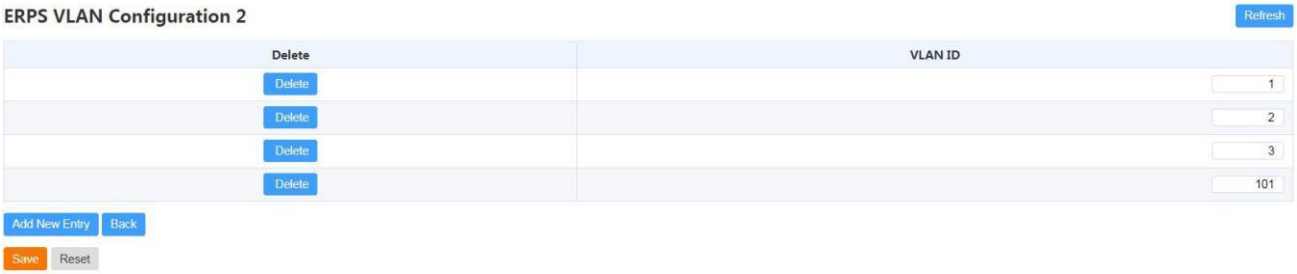
Chart Figure 12 81 Intersecting Ring Case SwitchA ERPS Configuration 4

Click the [Save] button to complete the addition of the protection group. Click the protection group 2 again to enter the parameter configuration interface, and set Port0 as the RPL Neighbour role according to the planned configuration.

Chart Figure 12-82 Intersecting Ring Case SwitchA ERPS Configuration 5

Click [VLAN_Config] to enter the VLAN configuration page, click [Add Entry] to add VLAN 1, 2, 3, and 101 as protected VLANs, and click [Save] to complete the configuration.

Chart Figure 12-83 Intersecting Ring Case SwitchA ERPS Configuration 6



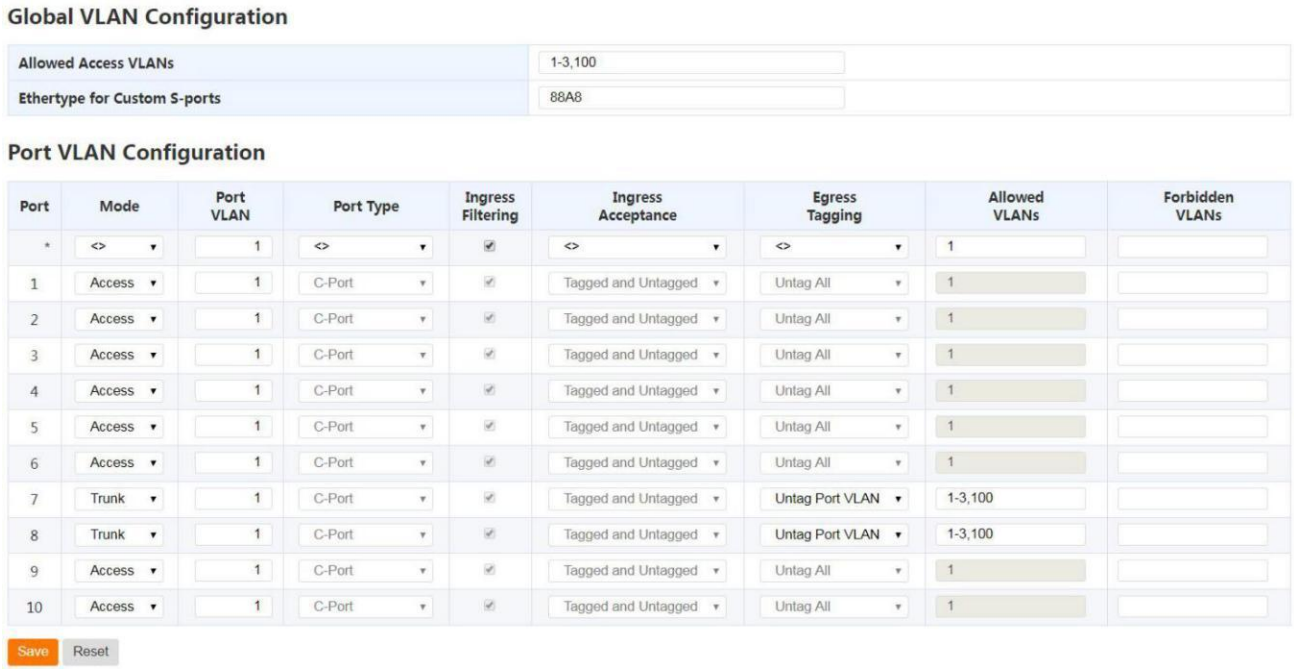
Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

12.6.4 Configure SwitchB

Step 1: VLAN and port configuration.

Select [VLAN] in the [Configuration] sub-item of the navigation bar, configure allowed access VLANs as 1, 2, 3, 100, port 1/7, port 1/8 mode as Trunk, and allow VLANs as 1, 2, 3, 100, Click the [Save] button to complete the configuration.

Chart Figure 12-84 Tangent Ring Case SwitchB VLAN Configuration



Step 2: Create and configure the MEP node.

1) Select [MEP] in the [Configuration] sub-item of the navigation bar, and click the [Add MEP] button to add port 7 as MEP 7, and Tagged VID as 100.

Chart Figure 12-85 Tangent Ring Case SwitchB MEP Configuration 1

2) Click the [Save] button to complete the addition of the entity node. Re-click instance 7 to enter the instance data configuration, enable the RAPS function, the last byte is consistent with the ring ID, set to 1

Chart Figure 12-86 Tangent Ring Case SwitchB MEP Configuration 2

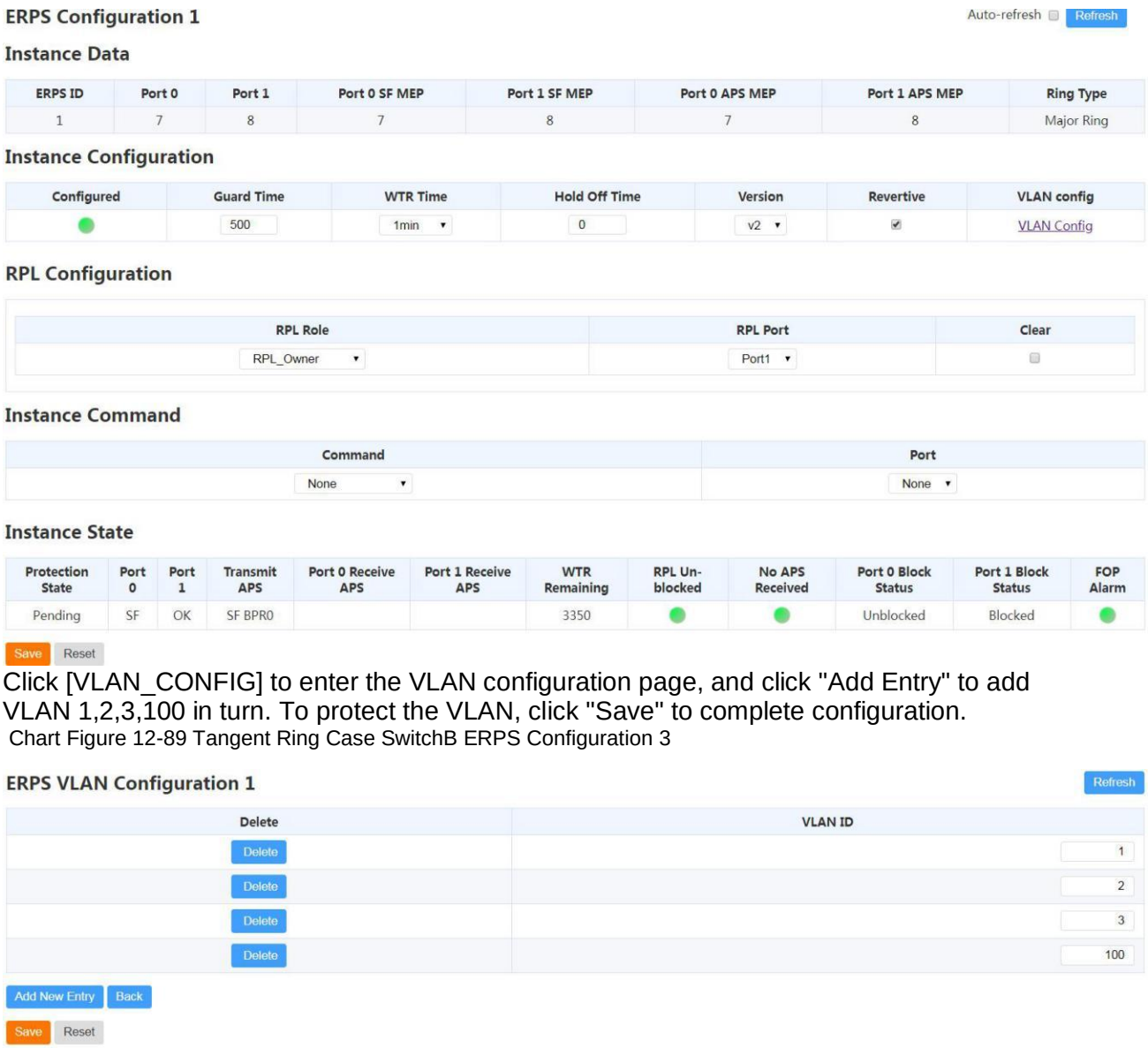
3) In the same way, add the MEP node of port 8, the Tagged VID is 100, and the RAPS function is enabled in the instance data configuration. The last byte is consistent with the ring ID and is set to 1.

Step 3: Create and configure the ERPS protection group.
Select "ERPS" under "Configuration" in the navigation bar, enter the ERPS configuration interface, click "Add Protection Group" button, add protection group 1, port port1/7 and port1/8, and the corresponding MEP is 7 and 8.

Chart Figure 12-87 Tangent Ring Case SwitchB ERPS Configuration 1

Click the [Save] button to complete the addition of the protection group. Click the protection group 1 again to enter the parameter configuration interface, and set Port1 as the RPL Owner role according to the planned configuration.

Chart Figure 12-88 Tangent Ring Case SwitchB ERPS Configuration 2



Click [VLAN_CONFIG] to enter the VLAN configuration page, and click "Add Entry" to add VLAN 1,2,3,100 in turn. To protect the VLAN, click "Save" to complete configuration.

Chart Figure 12-89 Tangent Ring Case SwitchB ERPS Configuration 3

Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

12.6.5 Configure SwitchC

Step 1: VLAN and port configuration.

Select [VLAN] in the [Configuration] sub-item of the navigation bar, configure the allowed access VLANs as 1, 2, 3, 100, 101, port port1/5, port1/7, port1/8 mode as Trunk, port port1/5 allows VLANs are 1, 2, 3, 101, and port 1/7 and port 1/8 allow VLANs to be 1, 2, 3, 100. Click the [Save] button to complete the configuration.

Chart Figure 12-90 Intersecting Ring Case SwitchC VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1-3,100,101
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,101	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,100	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Save Reset

Step 2: Create and configure the MEP node.

1) Select [MEP] in the [Configuration] sub-item of the navigation bar, and click the [Add MEP] button to add port 5 as MEP5 and Tagged VID as 101.

Chart Figure 12-91 Intersecting Ring Case SwitchC MEP Configuration 1

Maintenance Entity Point Refresh

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
Delete	5	Port	Mep	Down	5	0	1	101		

Add New MEP Save Reset

2) Click the [Save] button to complete the addition of the entity node. Click instance 5 again to enter the instance data configuration, enable the RAPS function, and the last byte is consistent with the ring ID, set to 2.

Chart Figure 12-92 Intersecting Ring Case SwitchC MEP Configuration 2

3) In the same way, add the MEP node of ports 7-8, and enter the instance data configuration to enable the RAPS function; Port 7-8 belongs to ring 1, the tagged VID is 100, and the last byte of RAPS is 1.

Step 3: Create and configure the ERPS protection group.

1) Select [ERPS] under [Configuration] in the navigation bar, enter the ERPS configuration interface, click the [Add protection group] button, add protection group 1, ports port1/7 and port1/8, and the corresponding MEPs are 7 and 8.

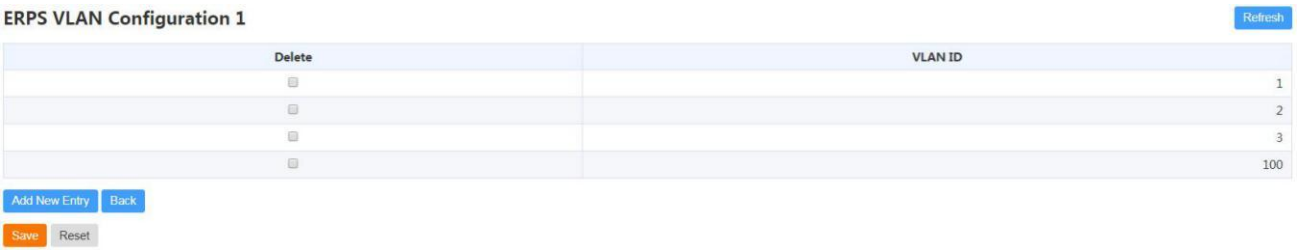
Chart Figure 12-93 Intersecting Ring Case SwitchC ERPS Configuration 1

Click the [Save] button to complete the addition of the protection group. Click protection group 1 again to enter the parameter configuration interface.

Chart Figure 12-94 Intersecting Ring Case SwitchC ERPS Configuration 2

Click [VLAN_CONFIG] to enter the VLAN configuration page, and click "Add Entry" to add VLAN 1,2,3,100 in turn. To protect the VLAN, click "Save" to complete configuration.

Chart Figure 12-95 Intersecting Ring Case SwitchC ERPS Configuration 3



2) Continue to add ERPS protection group 2, port 0 is port 1/5, port 1 is 0, the corresponding MEPs are 5 and 0, the ring type is set to sub-ring, interconnect node, and the main ring ID is 1.

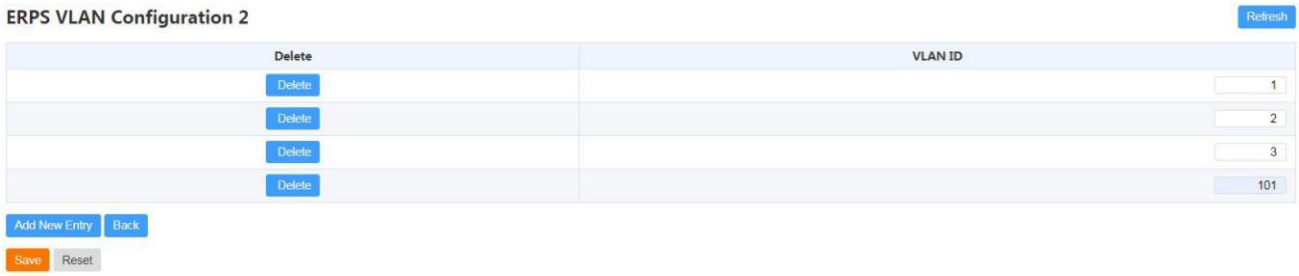
Chart Figure 12-96 Intersecting Ring Case SwitchC ERPS Configuration 4

Click the [Save] button to complete the addition of the protection group. Click protection group 2 again to enter the parameter configuration interface.

Chart Figure 12-97 Intersecting Ring Case SwitchC ERPS Configuration 5

Click "VLAN_Config" to enter the VLAN configuration page, and click "add entry" to add VLAN 1,2,3,101 in turn. To protect the VLAN, click "save" to complete configuration.

Chart Figure 12-98 Intersecting Ring Case SwitchC ERPS Configuration 6

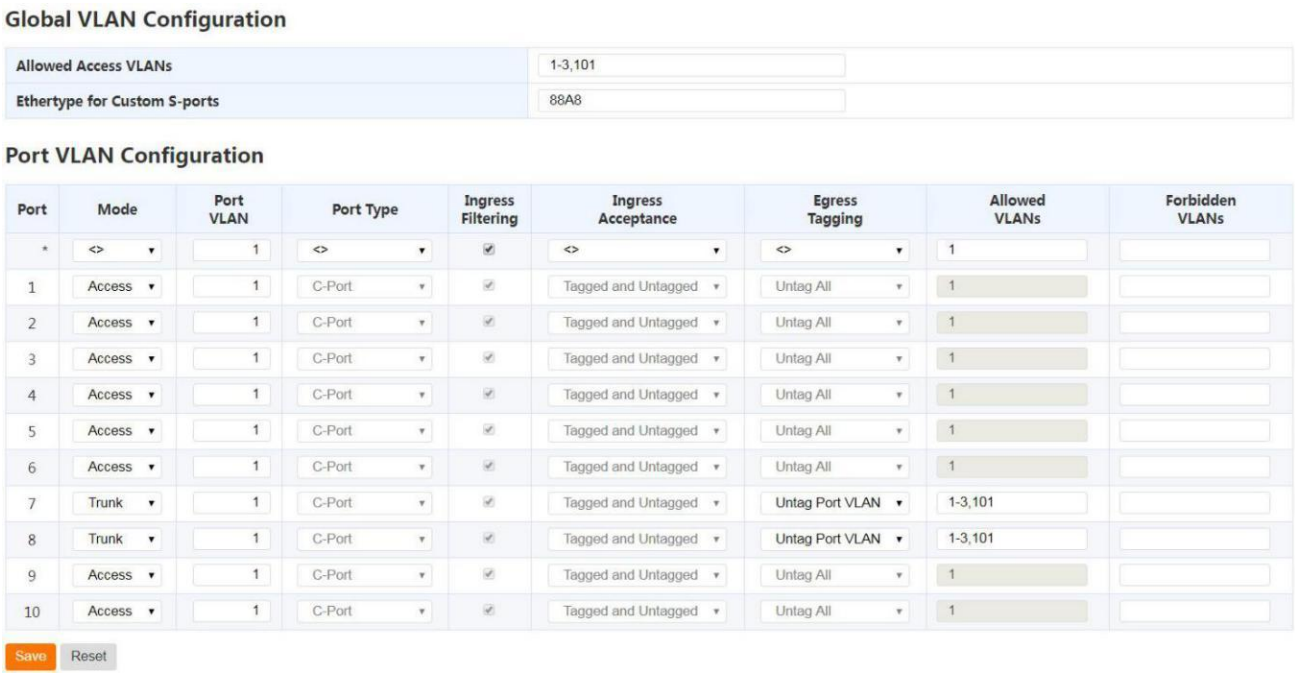


Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

12.6.6 Configure SwitchD

Step 1: VLAN and port configuration.
Select "VLAN" from the "Configuration" sub-item in the navigation bar. Configuration allows VLANs to be accessed as 1,2,3,101, port1/7, port1/8 mode as Trunk, allows VLANs to be accessed as 1,2,3,101. Click "Save" to complete the configuration.

Chart Figure 12-99 Tangent Ring Case SwitchD VLAN Configuration



Global VLAN Configuration

Allowed Access VLANs	1-3,101
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,101	
8	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-3,101	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Save Reset

Step 2: Create and configure the MEP node.

1) Select [MEP] in the [Configuration] sub-item of the navigation bar, and click the [Add MEP] button to add port 7 as MEP 7, and Tagged VID as 101.

Chart Figure 12-100 Tangent Ring Case SwitchD MEP Configuration 1

Maintenance Entity Point Refresh

Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
Delete	7	Port	Mep	Down	7	0	1	101		

Add New MEP Save Reset

2) Click the [Save] button to complete the addition of the entity node. Re-click instance 7 to enter the instance data configuration, enable the RAPS function, the last byte is consistent with the ring ID, set to 2

Chart Figure 12-101 Tangent Ring Case SwitchD MEP Configuration 2

3) Add the MEP node on port 8, Tagged VID is 101, enter the instance data configuration to enable RAPS function, the last byte is the same as the ring ID, set to 2.

Step 3: Create and configure the ERPS protection group.

Select "ERPS" under "Configuration" in the navigation bar, enter the ERPS configuration interface, click "Add Protection Group" button, add protection group 2, port port1/7 and port1/8, the corresponding MEP is 7 and 8, and the ring type is set as sub-ring.

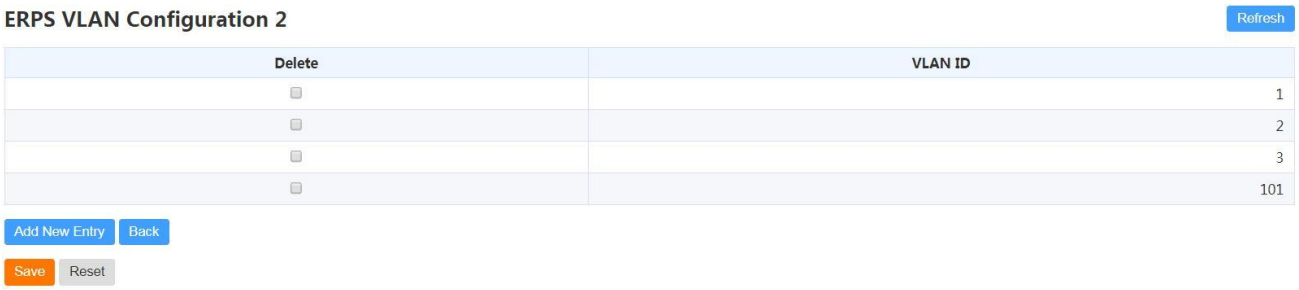
Chart Figure 12-102 Tangent Ring Case SWITCHD ERPS Configuration 1

Click the "Save" button to add the protection group. Click Protection Group 1 again to enter the parameter configuration screen and set Port0 as the RPL Owner role according to the planned configuration.

Chart Figure 12-103 Tangential Ring Case SWITCHD ERPS Configuration 2

Click "VLAN_Config" to enter the VLAN configuration page, and click "add entry" to add VLAN 1,2,3,101 in turn. To protect the VLAN, click "save" to complete configuration.

Chart Figure 12-104 Tangential Ring Case SWITCHD ERPS Configuration 3



Step 4: Select the "Maintenance" - "Configuration" - "Save Configuration" page in the navigation bar, and click the "Save Configuration" button to save the configuration.

13 MAC address table

13.1 MAC address overview

The Ethernet switch sends the message to the corresponding port by parsing the destination MAC address carried by the message, querying the MAC address table. The MAC address table records the MAC address, interface and VLAN ID information of the device connected with the device. According to the result of searching MAC address table, Ethernet switch decides to adopt the forwarding mode of well-known unicast or unknown broadcast.

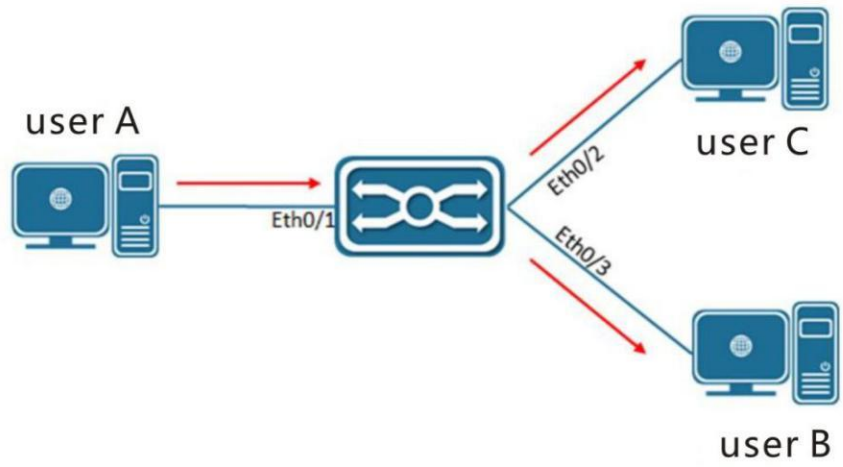
Well known unicast: the Ethernet switch finds the entry corresponding to the destination MAC address and VLAN ID of the message in the MAC address table, and the output port in the entry is unique, and the message is directly output from the port corresponding to the entry.

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

The MAC address of Ethernet switch can be obtained by dynamic acquisition or static configuration, generally by dynamic acquisition. Next, by analyzing the interaction process between user a and user C, the working principle of MAC address dynamic learning is given.

User a sends a message to port 1 of the switch. 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 vlan1 except 1 connecting user a, including the ports of user B and user C. at this time, user B can receive the message sent by user a that does not belong to it.

Chart Figure 13-1 example of MAC address learning

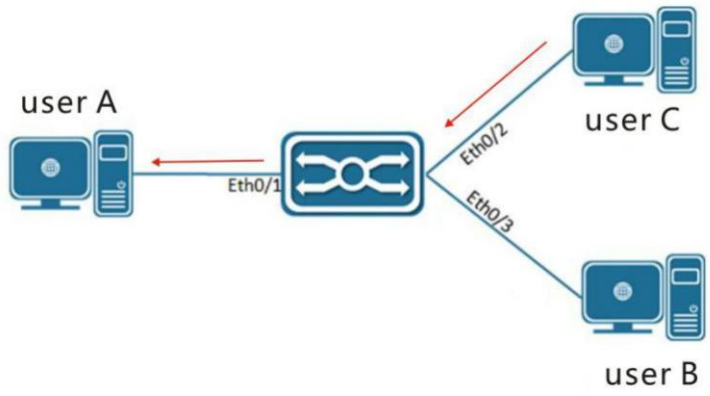


Current dynamic MAC address table information:

USER	VLAN	MAC address	Port
USER A	1	000E.C6C1.C8AB	1

After receiving the message, user B sends the response message to user a through port 2 of the Ethernet switch. At this time, the MAC address of user a already exists in the MAC address table of the Ethernet switch, and the message is forwarded to port 1 in unicast mode. At the same time, the Ethernet switch will learn the MAC address of user C, The difference is that user B cannot receive the message sent by user C to user a at this time.

Chart Figure 13-2 Unicast forwarding diagram



Current dynamic MAC address table information:

USER	VLAN	MAC address	PORT
USER A	1	000E.C6C1.C8AB	1
USER C	1	000E.C6C1.C8AD	2

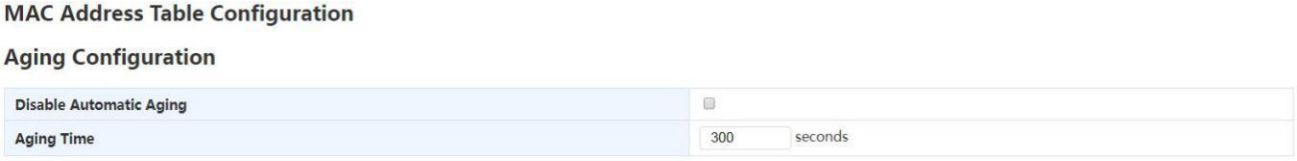
After an interaction process between user a and user C, the device learns the source MAC address of user a and user C, and then the message interaction between user a and user C is transmitted in unicast mode. After that, user B will no longer receive the interactive message between user a and user C.

13.2 Configure MAC address

Select configuration > MAC address table from the [navigation bar] drop-down menu to enter the configuration interface.

- Configure MAC address aging

Chart Figure 13-3 MAC address aging configuration



Item	Description
Disable auto aging	Enable to disable the auto aging function, which is off by default

Aging time	MAC address aging time, range 10-1000000 seconds, default 300 seconds

■ Port MAC address learning

Chart Figure 13-4 port MAC address learning configuration

Item	Description
Port member	Panel port number
automatic	When receiving the unknown source MAC address message, the port automatically learns the MAC address
Disable	Port off MAC address learning
security	If the source MAC address hits the static MAC address of the port, the message will be released, otherwise the message will be discarded

Note

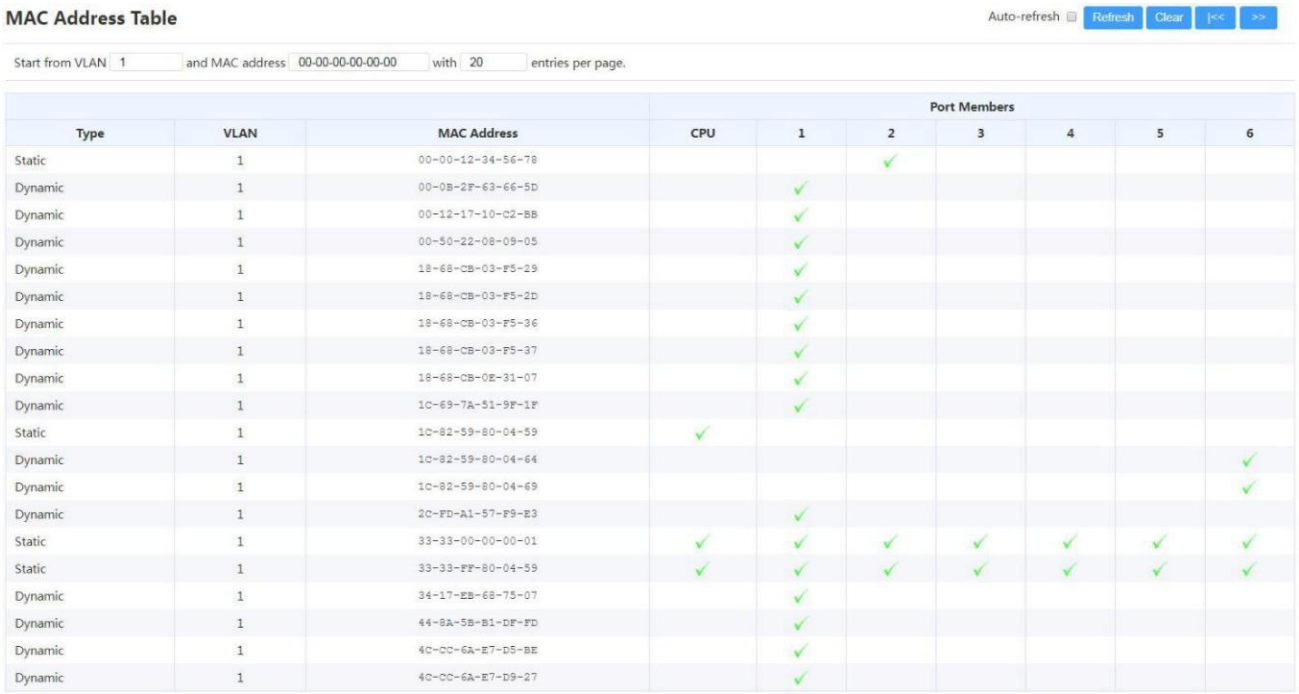
• The port security configuration is open, and the address learning mode cannot be changed.

■ Configuration

Item	Description
VLAN ID	VLAN ID
MAC ADDRESS	MAC ADDRESS
Port member	Panel port number

Select monitor > MAC address table from the [navigation bar] drop-down menu to enter the view interface.

Chart Figure 13-6 view MAC address table



Item	Description
Type	Static and dynamic
VLAN	VLAN ID
MAC ADDRESS	MAC address list, including several special MAC addresses, such as local IPv4 MAC address, broadcast MAC address, IPv6 MAC address
Port member	Panel port number and CPU port

13.3 CLI reference command

Command	switch(config)# mac address-table aging-time 300 switch(config)# mac address-table learning vlan 10 switch(config)# no mac address-table learning vlan 10 switch(config)# mac address-table static 00:00:12:34:56:78 vlan 1 interface GigabitEthernet 1/2
Description	Configure MAC address table aging time; Configure VLAN to enable MAC address learning; Configure VLAN to turn off MAC address learning; Configure MAC address table static address;

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# mac address-table learning switch(config-if)# mac address-table learning secure

	switch(config-if)# no mac address-table learning
Description	Configure the port MAC address learning mode as automatic; Configure the port MAC address learning mode as safe; Configure the MAC address learning mode of the port to disable;

Command	switch# show mac address-table
Description	Print the status of the MAC address table;

14 VLAN

VLAN is the abbreviation of virtual local area network. It is a logical network divided on a physical network. This network corresponds to the second layer network of ISO model. The division of VLAN is not limited by the actual physical location of the network port. VLAN has the same properties as ordinary physical network, except that there is no physical location limit, it is the same as ordinary LAN. The unicast, broadcast and multicast frames in the second layer are forwarded and spread in one VLAN, but not directly into other VLANs.

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

The port link types of Ethernet switch can be divided into three types: access, trunk and hybrid. These three ports will process differently when joining VLAN and forwarding messages.

Access type: the port can only belong to one VLAN, i.e. port VLAN. When the input message has VLAN and non port VLAN, it will be filtered. It is generally used for the connection between the switch and the end user;

Trunk type: the port can belong to multiple VLANs and can receive and send messages from multiple VLANs. When the input message does not have VLAN attribute, the default is port VLAN.

Hybrid type: on the basis of trunk type, functions such as port type selection and access filtering are added. It supports the following port types.

Unware: the VLAN parameters of the input message remain unchanged. If the outgoing configuration of the output port requires tag, an external tag of the output port VLAN will be added, that is, the output message has double tags.

C-Port: its basic implementation is the same as trunk. It only recognizes tag with TPID = 0x8100 for input message, and if tag is output, its TPID = 0x8100.

S-port: its basic implementation is the same as trunk. It only identifies tag with TPID = 0x88a8 for input message, and if tag is output, its TPID = 0x88a8.

S-custom-port: its basic implementation is the same as s-port, and its TPID is the user configuration value.

14.1 VLAN configuration

Select configuration > VLANs from the [navigation bar] drop-down menu to enter the configuration interface.

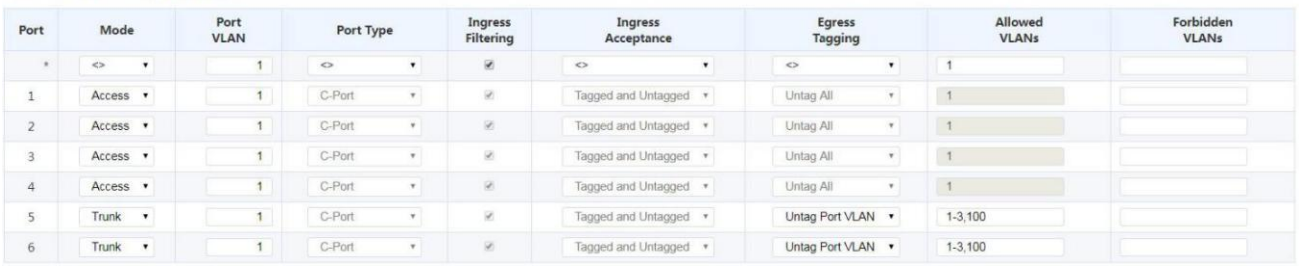
- Global VLAN configuration

Chart Figure 14-1 global VLAN configuration

Item	Description
Allow access to VLANs	Creating a VLAN supports the formats of "," and "-". "," represents multiple configuration segments. Each configuration segment can be a single VLAN or a VLAN range represented by "-". For example, "10-13" means VLAN 10, 11, 12, 13, 4. Only serve access type ports
Customize the Ethernet type of S-Ports	Define the TPID field in VLAN tag Valid for all s-custom-port type ports

- Port VLAN configuration

Chart Figure 14 2-port VLAN configuration



Item	Description
Port	Panel port number
Mode	access, trunk, hybrid three modes, default access
VLAN Port	Port default VLAN ID
Port type	Support Unaware, C-Port, S-Port, S-Custom-Port This parameter is only valid for hybrid mode
Admission filter	Enable ingress VLAN filtering This parameter is only valid for hybrid mode

Admission acceptance	Choose whether the ingress release is with TAG message, support Tagged and Untagged, Tagged, Untagged three options This parameter is only valid for hybrid mode
Tagging out	Choose whether to export the message with TAG, support Untag Port Vlan, Tag all, Untag all three options This parameter is only valid for hybrid/trunk mode
Allow VLANs	Define the allowed vlan of the trunk/hybrid port, the default is 1-4095
Ban VLANs	Define the forbidden vlan of the trunk/hybrid port, the default is empty

14.2 View VLAN

14.2.1 view VLAN and port mapping relationship

Select monitor > VLANs > membership from the [navigation bar] drop-down menu to enter the view interface.

Chart Figure 14-3 view VLAN membership

Item	Description
VLAN ID	VLAN ID
Port member	Port input VLAN, the display is green, and select

14.2.2 View VLAN port configuration

Select monitor > VLANs > port from the [navigation bar] drop-down menu to enter the view interface.

Chart Figure 14-4 view VLAN port status

Item	Description
Port	Panel port number
Port type	Configured port type
Ingress filtering	Does the port enable access filtering
Frame type	User configured admission acceptance supports all, tagged and untagged
Tx Tag	The user configured exit with tag mode supports untag port VLAN, tag all and untag all
Untagged VLAN ID	Retain
Conflict	Retain

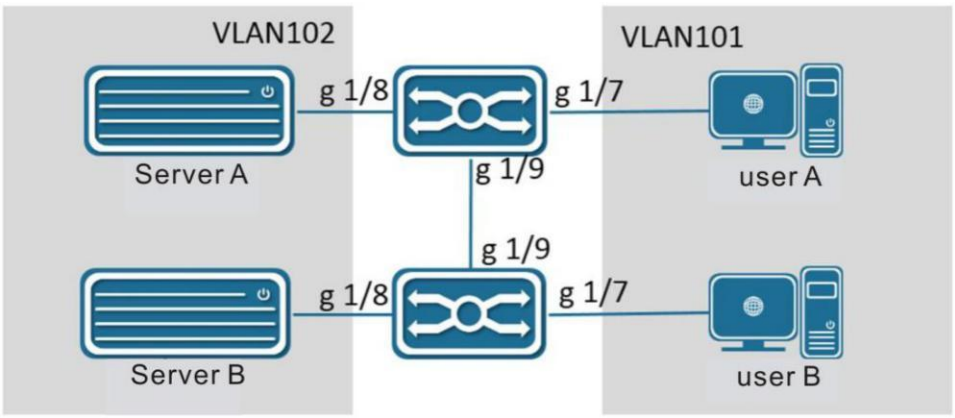
14.3 Typical VLAN configuration cases

- Case requirements

The figure below is a common office network. User a and user B are in the same VLAN domain, connecting two different switching devices. Server a and server B are in the same domain and are also connected to two different switching devices.

It is required that VLAN partition on switching equipment can meet the requirement of normal access between users, and users cannot access the server.

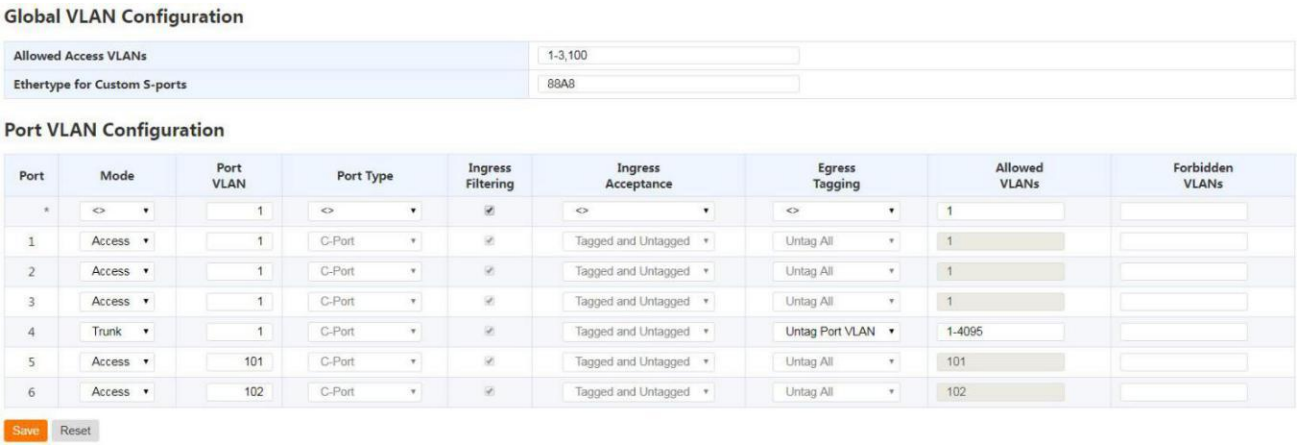
Chart Figure 14-5 VLAN case



- Operation steps

Two switching devices are configured in the same way: VLAN 101 and VLAN 102 are created globally; Port 5 is configured with vlan101, and port 6 is configured with vlan102; The configuration mode of trunk for port 4 is as follows.

Chart Figure 14-6 VLAN case configuration



Global VLAN Configuration

Allowed Access VLANs	1-3,100
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
5	Access	101	C-Port	☑	Tagged and Untagged	Untag All	101	
6	Access	102	C-Port	☑	Tagged and Untagged	Untag All	102	

Save Reset

14.4 CLI reference command

Command	switch(config)# vlan 1,20,30,1000 switch(config)# no vlan 1000 switch(config)# vlan ethertype s-custom-port 0x88a8
Description	Configure and add VLAN; Configure and delete VLAN; Configure the Ethernet type of custom S-Ports

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# switchport mode hybrid
Description	Configure port VLAN mode;

Command	switch(config-if)# switchport access vlan 1000
Description	Configure port access mode port VLAN;

Command	switch(config-if)# switchport trunk native vlan 20 switch(config-if)# switchport trunk vlan tag native switch(config-if)# no switchport trunk vlan tag switch(config-if)# switchport trunk allowed vlan 1,1000
Description	Configure port trunk mode port VLAN; Configure the port trunk mode to allow the tagging mode to be tag all; Configure the port trunk mode and the outbound tagging mode as untag port VLAN; Configure the VLANs allowed by the port trunk mode;

Command	switch(config-if)# switchport hybrid native vlan 30 switch(config-if)# switchport hybrid port-type s-port switch(config-if)# switchport hybrid ingress-filtering switch(config-if)# no switchport hybrid ingress-filtering switch(config-if)# switchport hybrid acceptable-frame-type tagged switch(config-if)# switchport hybrid egress-tag all switch(config-if)# switchport hybrid egress-tag none switch(config-if)# no switchport hybrid egress-tag switch(config-if)# switchport hybrid allowed vlan 20-23
Description	Configure port hybrid mode port VLAN; Configure the port type in hybrid mode; Configure the port hybrid mode to enable access filtering; Configure port hybrid mode to turn off access filtering; Configure the port hybrid mode and admission acceptance mode; Configure the port hybrid mode to allow tagging mode to be tag all; Configure the port hybrid mode to allow tagging mode to untag all; Configure the port hybrid mode and the outbound tagging mode as untag port VLAN; Configure VLANs allowed by port hybrid mode;

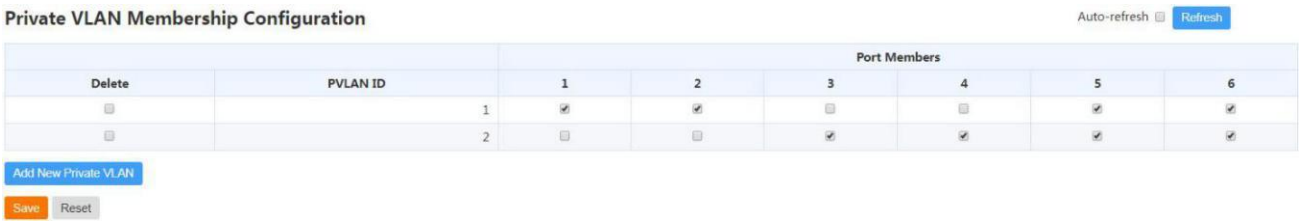
Command	switch(config-if)# switchport forbidden vlan add 20 switch(config-if)# switchport forbidden vlan remove 20
Description	Configure ports to add forbidden VLANs; Configure port deletion to prohibit VLANs;

Command	switch# show vlan brief switch# show vlan status
Description	Print VLAN membership; Print VLAN port;

15 private VLAN

15.1 Private VLAN member table

Private VLAN is based on the source port mask and has nothing to do with VLAN, which means that private VLAN ID and VLAN ID can be the same or different. The port must be a member of both VLAN and private VLAN to forward packets. By default, all ports are members of private VLAN 1.
As long as two ports belong to at least one private VLAN member at the same time, the two ports are interworking, otherwise, the two ports are isolated.
Each port can belong to multiple private VLANs. The total number of private VLANs supported is the total number of panel ports.
Select configuration > private VLAN > member table from the [navigation bar] drop-down menu to enter the configuration page.
Chart Figure 15-1 PVLAN member table configuration



- PVLAN ID: different pvlans must have different IDS, but there is no requirement that they must be continuous.
- Delete: after checking, the corresponding PVLAN will be deleted when saving next time.
- Add a new PVLAN: add a new PVLAN, PVLAN ID needs to be filled in manually.
- With the above configuration, port group 1 (1, 2) and port group 2 (3, 4) are isolated from each other.

15.2 Port isolation

Port isolation function divides port into two roles, isolated port and non isolated port.
- Isolation port and isolation port: isolation
- Isolated port and non isolated port: Interworking
- Non isolated port and non isolated port: Interworking

Select configuration > private VLAN > port isolation from the [navigation bar] drop-down menu to enter the configuration page.
Chart Figure 15-2 port isolation configuration

As shown in the figure above, the ports that are checked are isolated ports, and the ports that are not checked are non isolated ports. By default, all ports are non isolated ports.

15.3 CLI reference command

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

Command	switch(config-if)# pvlan 2 switch(config-if)# no pvlan 2 switch(config-if)# pvlan isolation switch(config-if)# no pvlan isolation
Description	Configure ports to join PVLAN (created automatically when PVLAN is associated with the first port); Configure the port to exit PVLAN (automatically delete when there is no associated port in PVLAN); Configure port to enable PVLAN port isolation; Configure port to close PVLAN port isolation;

16 Qos

16.1 QOS Overview

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

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

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

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

The following describes some commonly used terms in QOS:

CoS: Abbreviation of Class Of Service, the port is the priority mark of the message, and corresponds to the message queue selection.

DPL: Abbreviation of Drop Precedence Level, drop level, also known as drop priority. One of the switch service parameters, the value is 0, 1, or 2. Assigning drop levels to packets is also

called packet coloring. Packets with a drop level of 2 are red packets, 1 is yellow packets, and 0 is green packets. The discard level is mainly used when the switch needs to discard packets after congestion occurs

PCP: Abbreviation of Priority Code Point, VLAN Priority field of 802.1Q.

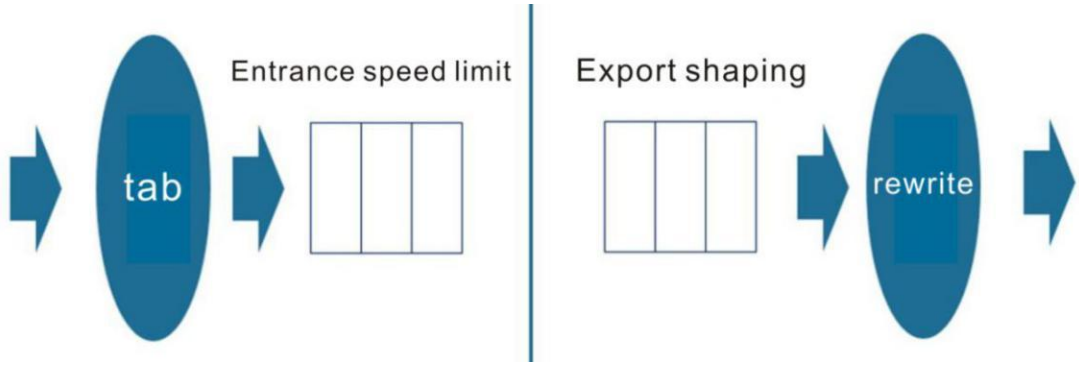
DEI: Abbreviation of Drop Eligible Indicator, VLAN CFI bit of 802.1Q.

DSCP: Abbreviation of Differentiated Services Code Point, Differentiated Services Code Point, a new definition of TOS in RFC 2474, using 6 bits to represent the priority relationship, and the value range of DSCP is 0-63.

16.2 QOS working principle

The QOS workflow starts from the message entering the port and ending when the message is sent from another port. In the middle, it goes through processes such as ingress marking, ingress rate limiting, egress shaping, and egress rewriting.

Chart Figure 16-1 QOS working principle



- Entrance mark

  The entrance marking of QOS supports DSCP-based entrance marking and non-DSCP-based entrance marking. When the following conditions are met, the ingress message is based on DSCP marking:

  - QOS access port classification, select "DSCP-based" for the port.
  - DSCP-based QOS, select to trust the value based on DSCP marking.
  - The ingress message is an IPv4 message with a DSCP field.

For non-DSCP entry marking

If the tag classification is enabled and the ingress message is tagged with TAG, the CoS is marked and the ingress queue is selected according to the mapping relationship between the PCP/DEI field of the message and the CoS/DPL; if the tag classification is disabled and the ingress message is tagged with TAG , The message comes with Cos/DPL as the tag, and the entry queue is selected; if the message does not have TAG, the port default CoS/DPL is used as the tag, and the entry queue is selected.

If the port DSCP access configuration is enabled and the classification function is enabled, the marking phase will classify the DSCP mapping relationship according to the QoS in the DSCP classification, and remark the DSCP value.

Entry mark for DSCP

Support the mapping conversion from DSCP to DSCP, and the conversion result is then converted from DSCP to CoS and output as a mark.

- Entry speed limit

Ingress speed limit includes ingress port speed limit and ingress queue speed limit. Packets enter the corresponding ingress queue according to the marked CoS, and the queue rate limit value should be less than the port rate limit.

- Export shaping

Egress shaping includes egress queue shaping, egress queue scheduling, and egress port shaping. The message enters the egress queue according to the marked CoS. First, single-queue shaping is performed. Then, the 6 queues 0-5 need to be scheduled for egress queues according to the scheduling mode and queue weight, and finally the egress port shaping is performed uniformly.

- Rewrite

The rewriting part is mainly to modify the PCP/DEI field of the message TAG and the content of the DSCP field of the message.

The rewriting of PCP/DEI supports the three methods of Classified, Default, and Mapped.

Classified is rewritten according to the port classification results, such as the default PCP/DEI for messages without TAG, and the PCP/DEI for messages with TAG;

Default compulsory write configuration value;

Based on the marked CoS/DPL, Mapped performs another mapping based on the configured CoS/DPL and PCP/DEI mapping relationship.

The rewriting of the message DSCP supports three methods: Disabled, Enable and Remap.

Disabled keeps the original DSCP value of the message unchanged;

Enable supports the modified result of entry mark;

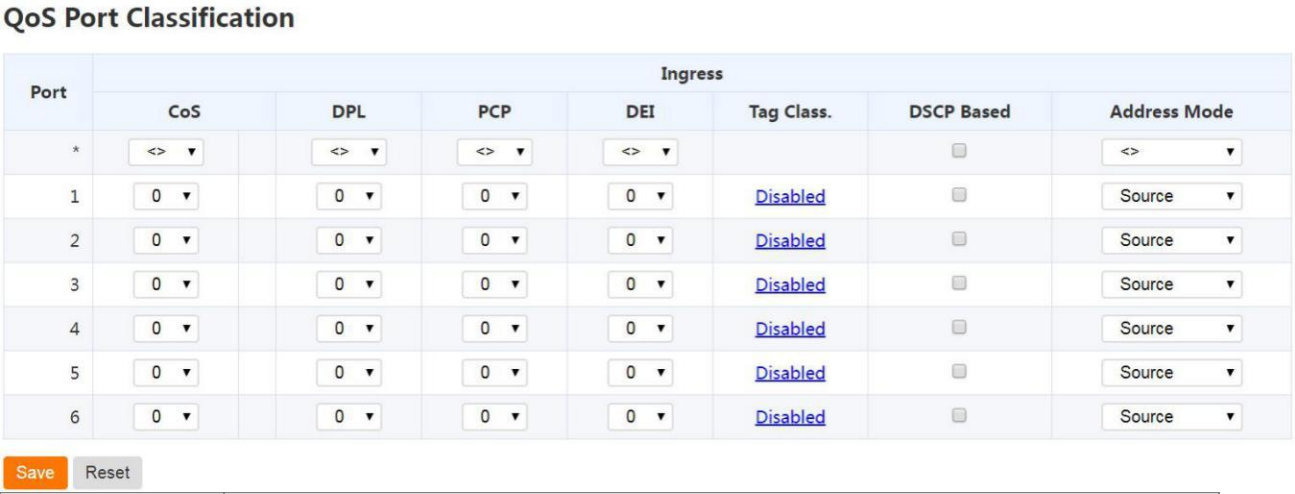
Remap, based on the entry mark, performs another mapping according to the configuration.

16.3 Configure QOS

16.3.1 Port classification

In the [Navigation Bar] drop-down menu, select: Configuration->QOS->Port Classification to enter the configuration interface.

Chart Figure 16-2 QOS port classification configuration

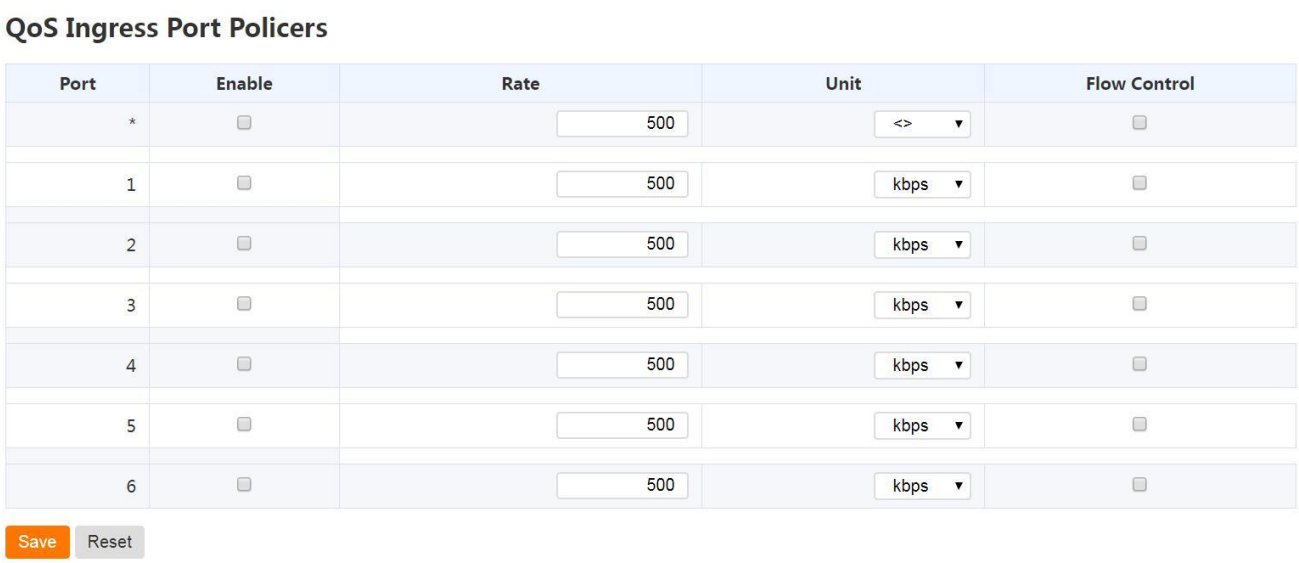


Item	Description
Port	Panel port number
Cos/DPL	Port default Cos/DPL value
PCP/DEI	Default PCP/DEI value of the port
Label classification	Enable to generate CoS/DPL by mapping the PCP/DEI field in the TAG of the message with TAG
Based on DSCP	Enable port classification based on DSCP
Address mode	Choose Qos control list classification basis, Source is based on SMAC/SIP, Destination is based on DMAC/DIP classification

16.3.2 Port policy

In the [Navigation Bar] drop-down menu, select: Configuration->QOS->Port Policy to enter the configuration interface.

Chart Figure 16-3 QOS port policy configuration



Item	Description
Port	Panel port number
Enable	Enable rate limiting port policy
Rate	Combined with the unit, the range of bps and fps is 100-3276700, and the range of kbps and kfps is 1-32767
Unit	Support bps, kbps, fps, kfps four units
Flow Control	Enable port rate limit flow control. If port flow control is enabled, pause packets will be sent, and packets that exceed the rate limit will not be discarded.

16.3.3 Queue strategy

In the [Navigation Bar] drop-down menu, select: Configuration->QOS->Queue Strategy to enter the configuration interface.

Chart Figure 16-4 QOS queue policy configuration

QoS Ingress Queue Policers

Port	Queue 0			Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	☐	500	<>	☐	☐	☐	☐	☐	☐	☐
1	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
2	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
3	☑	500	kbps	☐	☐	☐	☐	☐	☐	☐
4	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
5	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐
6	☐	500	kbps	☐	☐	☐	☐	☐	☐	☐

Save Reset

Item	Description
Port	Panel port number
E	Enable port queue entry rate limit policy
Queue 0-7	Speed limit value, range 100-3276700bps, or 1-32767kbps

16.3.4 Port scheduling

In the [Navigation Bar] drop-down menu, select: Configuration->QOS->Port Scheduling to enter the configuration interface.

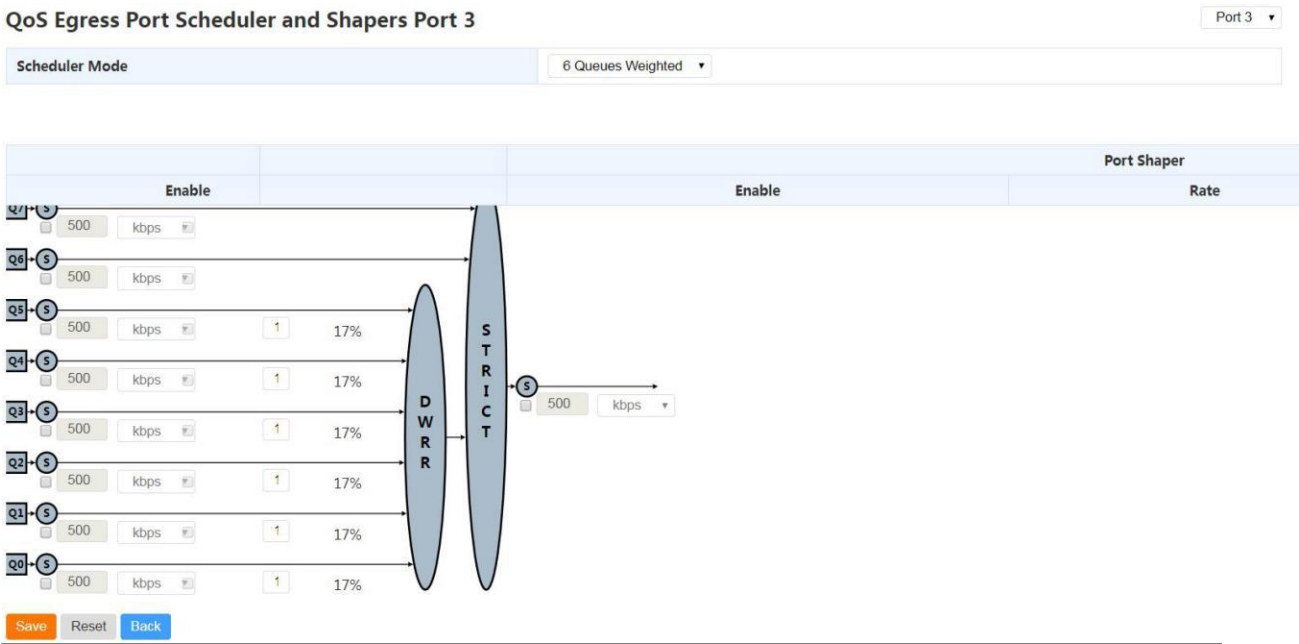
Chart Figure 16-5 QOS port scheduling configuration

QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	6 Queues Weighted	17%	17%	17%	17%	17%	17%
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-

Item	Description
Port	Panel port number, click to enter the port quasi-out scheduling shaping configuration interface
Mode	Support Strict Priority and 6 Queues Weighted two modes
Weight 0-6	Export queue weight, valid in mode 6 Queues Weighted

Chart Figure 16-6 QOS port scheduling and shaping configuration



Item	Description
Scheduling mode	Support Strict Priority and 6 Queues Weighted two modes
Queue shaping	Based on the queue enable control, the range is 100-3281943kbps, or 1-3281Mbps, support the enable queue to use the excess bandwidth
Queue scheduling	Configure queue weight, ranging from 1-100, 6 queues recalculate the queue proportions according to the configuration
Port shaping	Based on port enable control, the range is 100-3281943kbps, or 1-3281Mbps

16.3.5 Port shapers

In the [Navigation Bar] drop-down menu, select: Configuration -> QOS -> Port Shapers enter the configuration interface

Chart Figure 16-7 QOS port shaping configuration

Item	Description
Port	Panel port number, click to enter the port quasi-out scheduling shaping configuration interface
Shaper/Q0-Q7	Queue shaping rate limit

Shaper/Port	Port rate limit value

16.3.6 Port Tag

In the [Navigation Bar] drop-down menu, select: Configuration->QOS->Port Tag to enter the configuration interface.

Chart Figure 16-8 QOS port label configuration

Item	Description
Port	Panel port number, click to enter the mode configuration interface
Mode	The Classified model will not be changed at the export; Default mode uses the PCP/DEI value of the default configuration Mapped modifies the PCP/DEI value according to the mapping relationship between QOS/DP and PCP/DEI

16.3.7 Port DSCP

In the [Navigation Bar] drop-down menu, select: Configuration->QOS->Port DSCP to enter the configuration interface.

Chart Figure 16-9 QOS port DSCP configuration

Item	Description
Port	Panel port number
Admission/Conversion	Enable the admission conversion function, the specific configuration is

	in the "DSCP conversion configuration interface"
Access/Classification	Supports four classification methods: Disable, DSCP=0, Selected, and ALL. Disable means that classification is not supported; DSCP=0 means that only DSCP=0 packet classification is supported; Selected means that only the items selected in the DSCP conversion configuration page are supported for classification; Indicates classification of all DSCP values
Quasi-out/rewrite	The DSCP content of the rewrite message is accurately output, and it supports four methods: Disable, Enable, Remap DP Unware, and Remap DP Aware. Disable means that rewriting is not supported; Enable means that rewriting is supported, but DSCP conversion is not supported. Remap DP Unware Means that the DP0 table is rewritten according to the DSCP conversion; Remap DP Aware means that the DP0/DP1 table is rewritten according to the DSCP conversion

16.3.8 Qos based on DSCP

In the [Navigation Bar] drop-down menu, select: Configuration->QOS->DSCP-based Qos to enter the configuration interface.

Chart Figure 16 10 QOS classification configuration based on DSCP

DSCP-Based QoS Ingress Classification

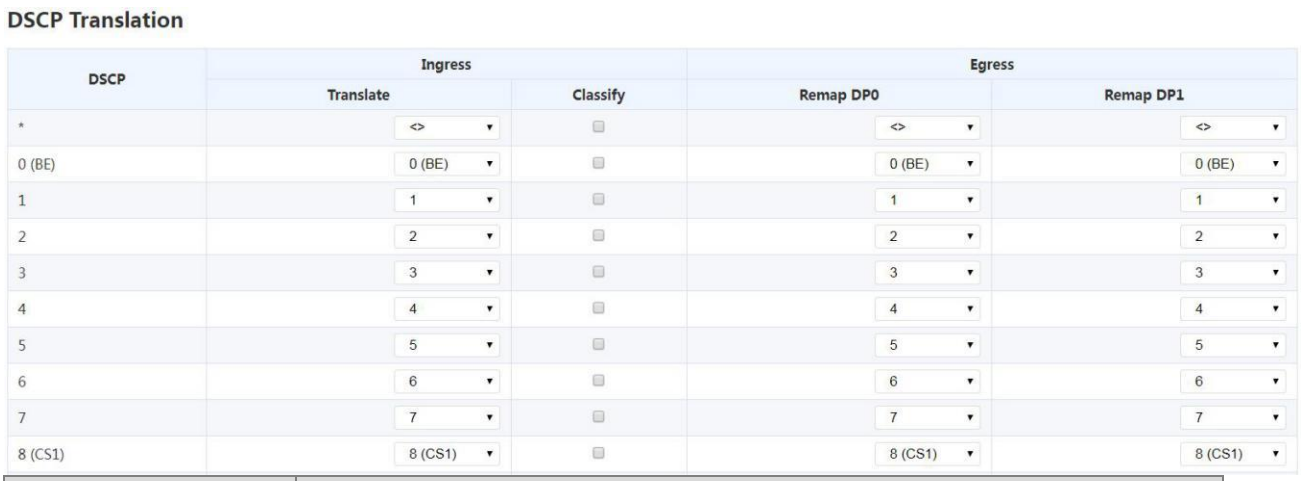
DSCP	Trust	CoS	DPL
*	☐	<>	<>
0 (BE)	☐	0	0
1	☐	0	0
2	☐	0	0
3	☐	0	0
4	☐	0	0
5	☐	0	0
6	☐	0	0
7	☐	0	0
8 (CS1)	☐	0	0
9	☐	0	0
10 (AF11)	☐	0	0

Item	Description
DSCP	DSCP value, range 0-63
Trust	Enable trusting a specific DSCP value
QOS classification	QOS classification value, range 0-7
DPL	DPL value, range 0-1

16.3.9 DSCP conversion

In the [Navigation Bar] drop-down menu, select: Configuration->QOS->DSCP conversion to enter the configuration interface.

Chart Figure 16-11 QOS DSCP conversion configuration



Item	Description
DSCP	DSCP value, range 0-63
Transfer in/Convert	DSCP to DSCP conversion configuration, range 0-63
Access/Classification	Enable admission based on DSCP classification
Quasi-out/remap DP0	DP=0 quasi-out mapping relationship
Quasi-out/remap DP1	The quasi-out mapping relationship with DP=1

16.3.10 DSCP classification

In the [Navigation Bar] drop-down menu, select: Configuration->QOS->DSCP classification, enter the configuration interface.

Chart Figure 16-12 QOS DSCP classification configuration

DSCP Classification

CoS	DSCP DP0	DSCP DP1
*	<>	<>
0	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)

Save Reset

Item	Description
QOS classification	QOS classification, range 0-7
DSCP DP0	COS to DSCP conversion configuration when DP=0, range 0-63
DSCP DP1	COS to DSCP conversion configuration when DP=1, range 0-63

16.3.11 Qos control list

In the [Navigation Bar] drop-down menu, select: Configuration->Qos->QOS control list to enter the configuration interface.

Chart Figure 16-13 QOS control list configuration

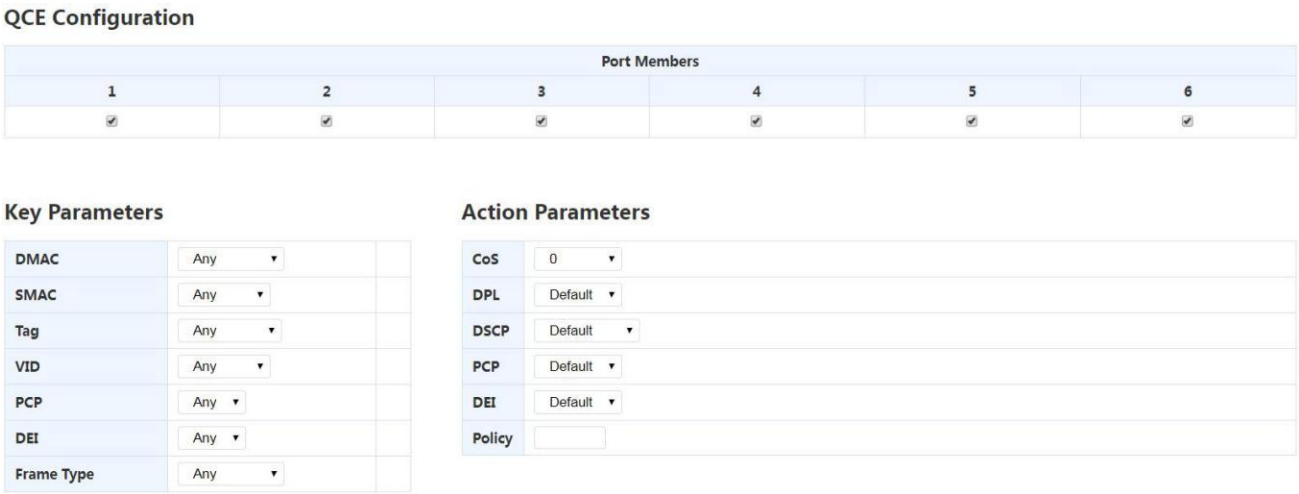
QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action						
									CoS	DPL	DSCP	PCP	DEI	Policy	
1	Any	Any	Any	Any	Any	Any	Any	Any	0	Default	Default	Default	Default	Default	

Display the brief information of QCE, support QCE table entry up and down movement, add before, add after, delete, edit operations.

Click the Add button to enter the QCE creation interface.

Chart Figure 16-14 QCE configuration

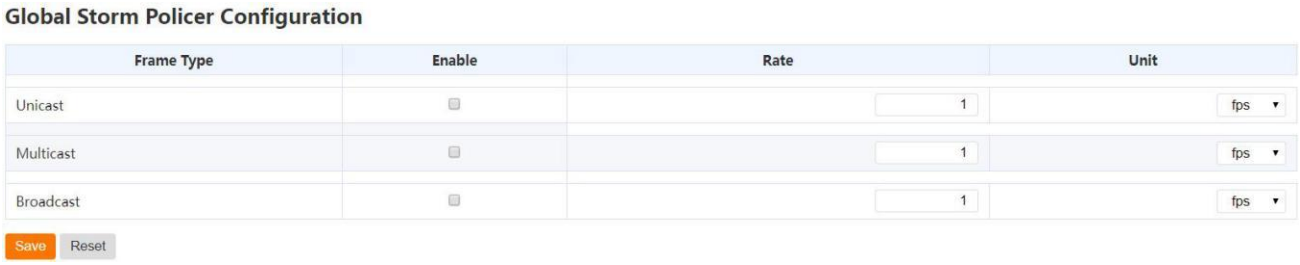


Item	Subtopic	Description
Port member	-	Panel port number, support for selecting multiple ports, all ports are selected by default
Key parameter	DMAC	Support Any, Unicast, Multicast, Broadcast options
	SMAC	Support Any, Specific options
	Label	Support Any, Untagged, Tagged, C-Tagged: with C-tagged and S-Tagged options
	VID	Support Any, Specific, Range options
	PCP	Support Any, 0-7 combination options
	DEI	Support Any, 0-7 combination options
	Frame type	Support Any, EtherType, LLC, SNAP, IPv4, IPv6 options
Behavioral parameters	CoS	QOS classification, range 0-7
	DPL	Default: unchanged 0-7: target value
	DSCP	Default: unchanged 0-63: target value
	PCP	Default: unchanged 0-7: target value
	DEI	Default: unchanged 0-1: Target value
	Strategy	Keep

16.3.12 Storm control

In the [Navigation Bar] drop-down menu, select: Configuration->QOS->Storm Control to enter the configuration interface.

Chart Figure 16-15 Storm Control Configuration



Item	Description
Frame type	Support broadcast, multicast, unicast selection
Enable	Enable this type of frame storm control function
Rate	Speed limit based on the number of messages, ranging from 1-1024000fps, or 1-1024kfps
Unit	Support fps and kfps two options

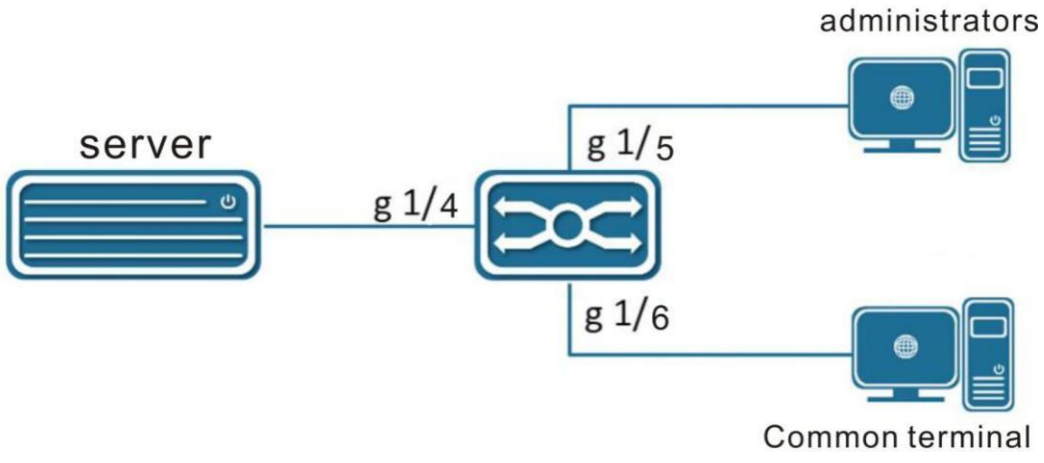
16.4 QOS typical configuration case

16.4.1 Priority Forwarding Service

- Case requirements

The picture below is a common office network. The server has a 10Mbits entry speed limit due to performance problems. When the business is busy, the administrator is required to be able to sample the server normally.

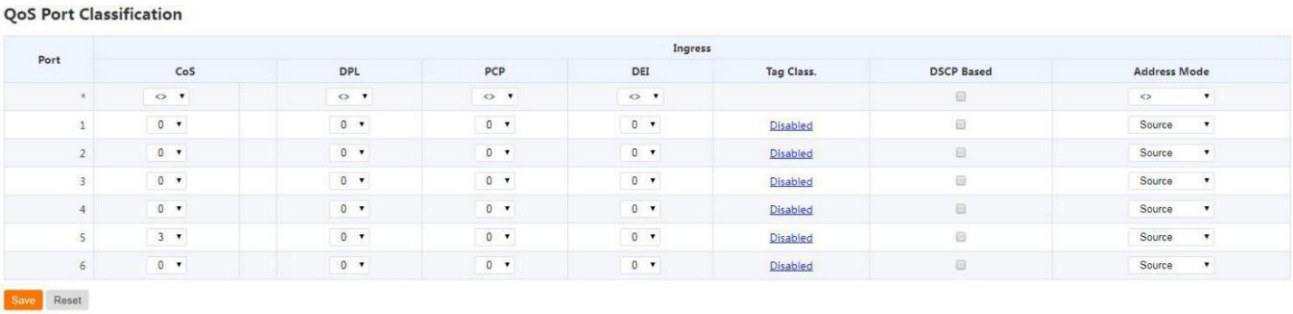
Chart Figure 16-16 QOS case



- Operation steps

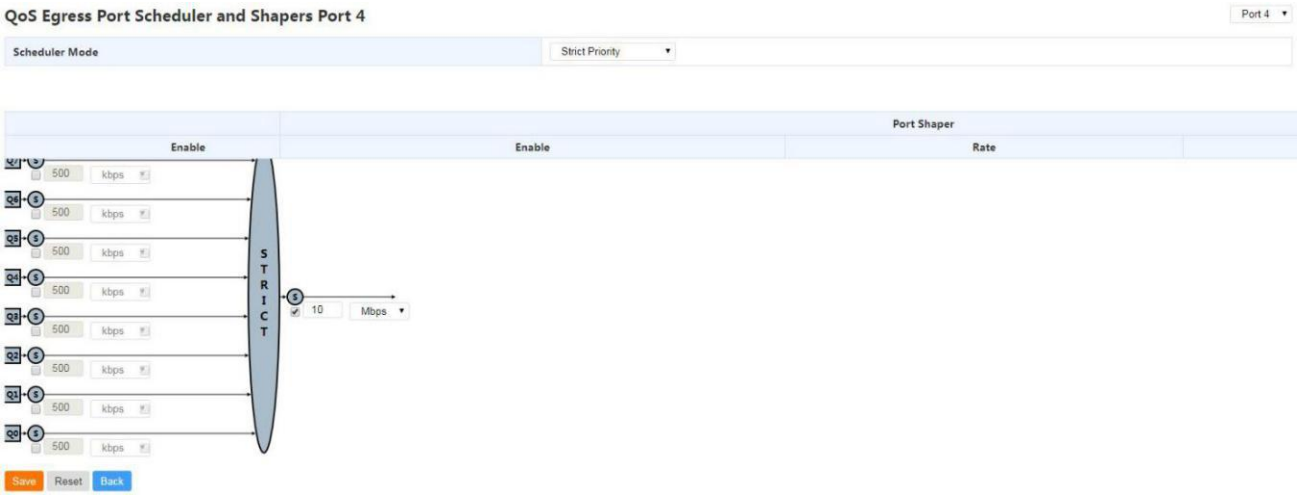
Configure the priority of the 5-port flag to 3 and the priority of the 6-port flag to 0.

Chart Figure 16-17 QOS case port classification configuration



Configure 4-port egress shaping at a rate of 10Mbits, and configure the scheduling mode as strict priority scheduling.

Chart Figure 16-18 QOS case port scheduling and shaping configuration



16.4.2 Storm control

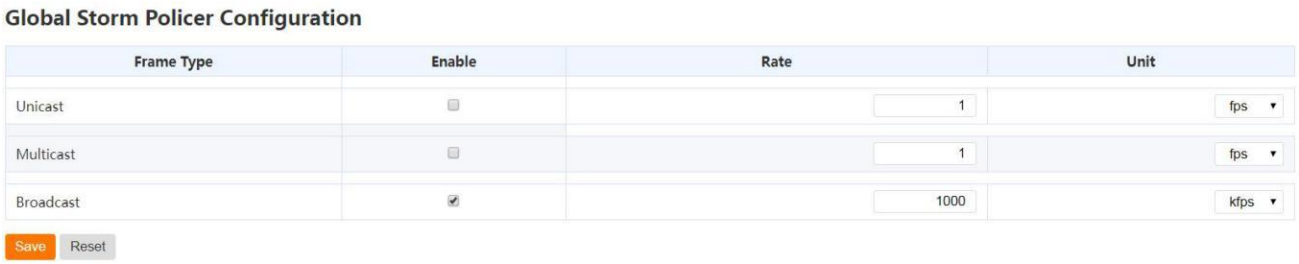
- Case requirements

Equipment broadcast storm suppression requires that the broadcast message does not exceed 1000kfps.

- Operation steps

Enter the storm control configuration interface, enable broadcast frames, and set the rate limit.

Chart Figure 16-19 Storm control case configuration.



17 Port mirroring

17.1 Mirror overview

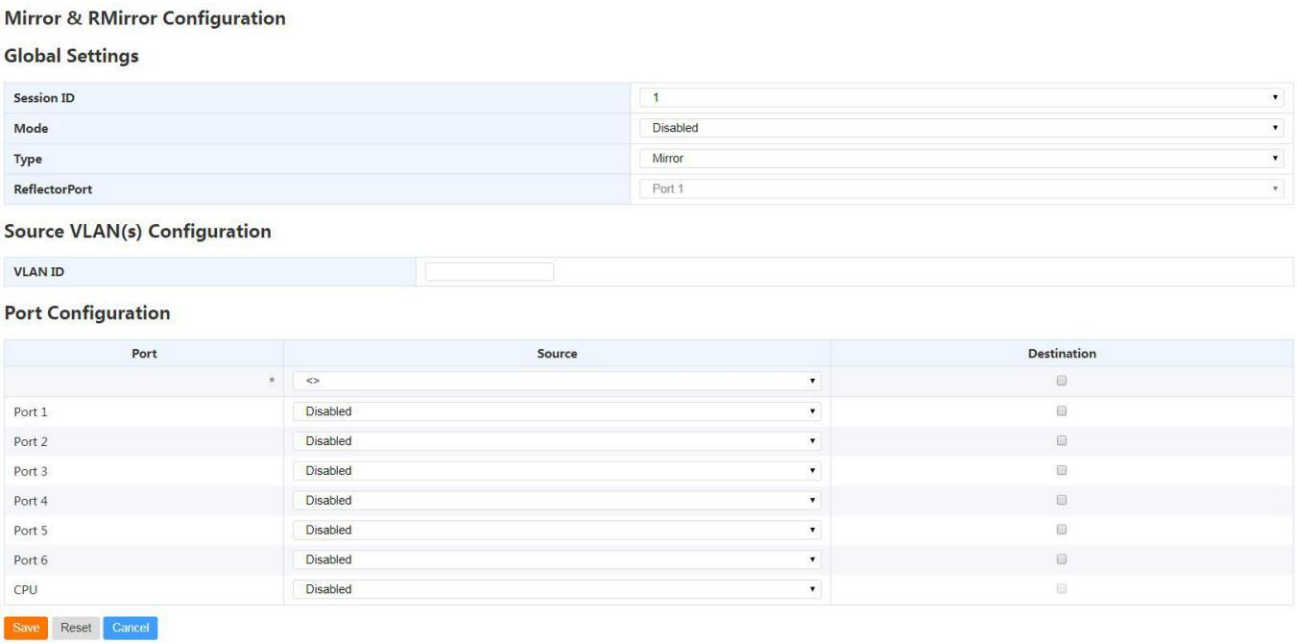
SPAN (Local Switched Port Analyzer) is a local mirroring function. The SPAN function copies the packets of the specified port to the destination port. Generally, the SPAN destination port will be connected to the data detection device. The user uses these devices to analyze the packets received by the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

When the port is configured as a mirroring destination port, the port is in the block state and all incoming packets are discarded. Do not configure the management port as a mirroring destination port to avoid remote connection disconnection.

17.2 Configure mirroring

In the [Navigation Bar] drop-down menu, select: Configuration -> Mirror to enter the mirroring session interface.
Chart Figure 17-1 Mirroring session

The current series of products only support one session. Click the corresponding session ID as shown in the figure above to enter the mirror configuration interface.
Chart Figure 17-2 Mirror configuration



- Global settings

  The current series only supports mode configuration.
  - Disable: Disable the current mirroring session, the default is disabled.
  - Enable: enable the current mirroring session.

- Source VLAN settings

  Two formats of "," and "-" are supported. "," means multiple configuration sections. Each configuration section can be a single VLAN or a range of VLANs indicated by "-". For example, "10-13" means the 4 vlans of vlan10, 11, 12, and 13.
  The traffic of the VLAN set by the source VLAN will be mirrored to the mirroring destination port. .

- Port settings

Item	Description
Port	Panel port number and CPU port
Source	Select the mirror mode. To Disabled: The transmitted frame and the received frame will not be mirrored. This is the default mode. Two-way: The received frame and the transmitted frame are mirrored on the target port. Input: The destination port of the frame mirroring received by this port. The transmitted frame is not mirrored. Output: The frames sent on this port are mirrored on the target port. The received frame is not mirrored.
Purpose	Checking the above means that the port is the mirroring destination port, and only one port can be used as the mirroring destination port.

Note: 1. Port-based mirroring and VLAN-based mirroring cannot be configured at the same time. If VLAN-based mirroring is configured, port-based mirroring configuration will be

prohibited; if port-based mirroring is configured, then VLAN-based mirroring is configured. Port-based mirroring configuration will be cancelled.
2. If the port is configured as a mirroring destination port, the "source" configuration of the port can only be "disabled" or "input". If it was previously configured as "two-way" or "output", the port will be used as the destination. It is forbidden to be checked.

17.3 CLI reference commands

Command	switch(config)# monitor session 1 switch(config)# no monitor session 1 switch(config)# monitor session 1 source vlan 20 switch(config)# no monitor session 1 source vlan 20 switch(config)# monitor session 1 source cpu tx switch(config)# no monitor session 1 source cpu tx switch(config)# monitor session 1 source interface GigabitEthernet 1/1-2,5 both switch(config)# no monitor session 1 source interface GigabitEthernet 1/2 rx switch(config)# monitor session 1 destination interface GigabitEthernet 1/8 switch(config)# no monitor session 1 destination interface GigabitEthernet 1/8
Description	Configure mirroring to be enabled; Configure mirroring off; Configure the mirroring source VLAN to add; Configure mirroring source VLAN deletion; Configure the mirror source port to add the CPU port and direction; Configure the mirror source port to delete the CPU port and direction; Configure the mirror source port to add the panel port and direction; Configure the mirror source port to delete the panel port and direction; Configure the mirroring destination port to add; Configure the mirroring destination port to delete;

18 GVRP

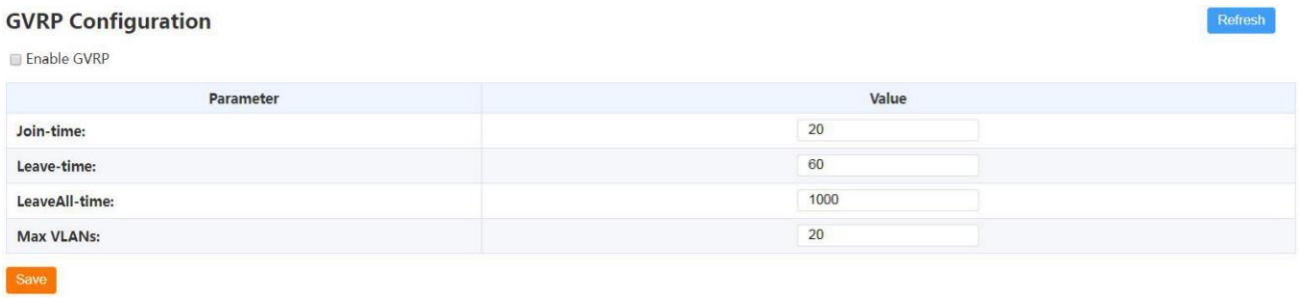
GVRP (GARP VLAN Registration Protocol, GARP VLAN Registration Protocol) is an application of GARP (Generic Attribute Registration Protocol). GARP provides a mechanism to assist exchange members in the same LAN. , Disseminate and register certain information (such as VLAN, multicast address, etc.). GARP itself does not exist in the device as an entity. An application entity that follows the GARP protocol is called a GARP application, and GVRP is an application of GARP.

Based on the working mechanism of GARP, GVRP maintains the VLAN dynamic registration information in the device and propagates the information to other devices. After the device activates the GVRP feature, it can receive VLAN registration information from other devices, and dynamically update the local VLAN registration information, including the current VLAN members, which port these VLAN members can reach, etc. Moreover, the device can spread the local VLAN registration information to other devices, so that the VLAN information of all devices in the same local area network can be agreed. The VLAN registration information

propagated by GVRP includes not only the static registration information manually configured locally, but also the dynamic registration information from other devices.

18.1 Global configuration

In the [Navigation Bar] drop-down menu, select: Configuration->GVRP->Global to enter the configuration page.
Chart Figure 18-1 GVRP global configuration



- Enable GVRP

  By default, GVRP is disabled globally. Check to enable GVRP globally.
- GVRP protocol timer

  Join timeout: The unit is centiseconds (that is, 0.01 seconds), the range is 1-20, and the default value is 20.
  Leave timeout: The unit is centiseconds, the range is 60-300, and the default value is 60.
  All leaving timeout: The unit is centiseconds, the range is 1000-5000, and the default value is 1000.
- Maximum number of VLANs

  After GVRP is enabled, the maximum number of VLANs supported by GVRP. The default value is 20. This parameter can only be changed when GVRP is turned off.

18.2 Port configuration

In the [Navigation Bar] drop-down menu, select: Configuration->GVRP->Port to enter the configuration page.
Chart Figure 18-2 GVRP port configuration

Enable or disable GVRP based on the switch panel port, all ports are disabled by default. Only when GVRP is enabled globally and on the port, the GVRP protocol will run on the port.

18.3 CLI eference command

Command	switch(config)# gvrp switch(config)# no gvrp switch(config)# gvrp time join-time 20 leave-time 60 leave-all-time 1000 switch(config)# gvrp max-vlans 20
Description	Configure GVRP to enable; Configure GVRP to close; Configure GVRP join timeout, leave timeout, and all leave timeout periods; Configure the maximum number of VLANs for GVRP;

Command	switch(config)# interface GigabitEthernet 1/3
Description	Enter the configuration port;

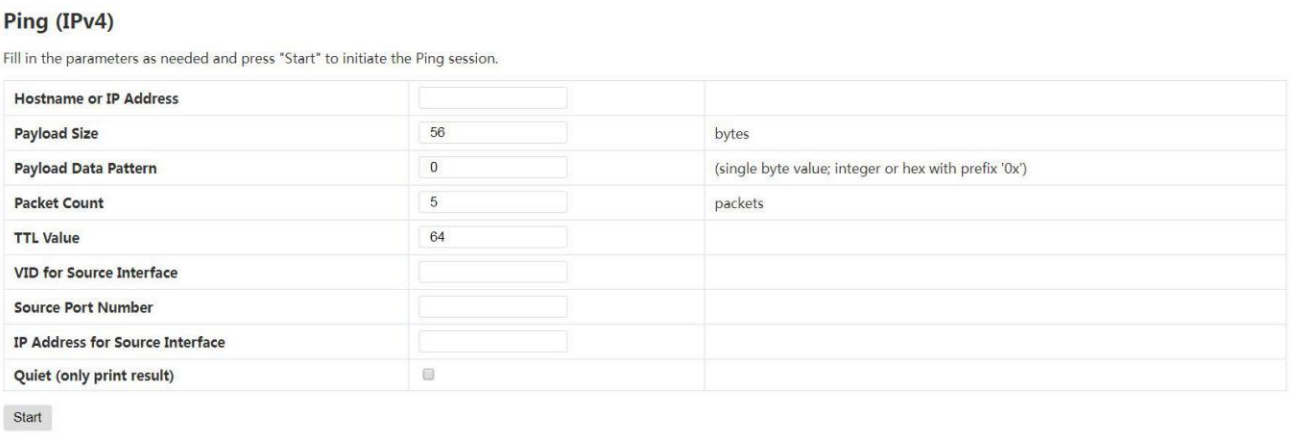
Command	switch(config-if)# gvrp switch(config-if)# no gvrp
Description	Configure port GVRP to enable; Configure port GVRP to close;

19 diagnosis

19.1 Ping(IPv4)

In the [Navigation Bar] drop-down menu, select: Diagnosis -> Ping (IPv4) to enter the diagnosis interface.

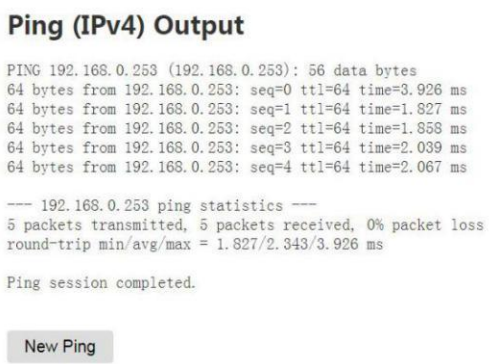
Chart Figure 19-1 ping (IPv4) diagnosis



Item	Description
Hostname or IP address	The address of the target host can be a symbolic host name or an IP address. (Does not support DNS, only IP address)

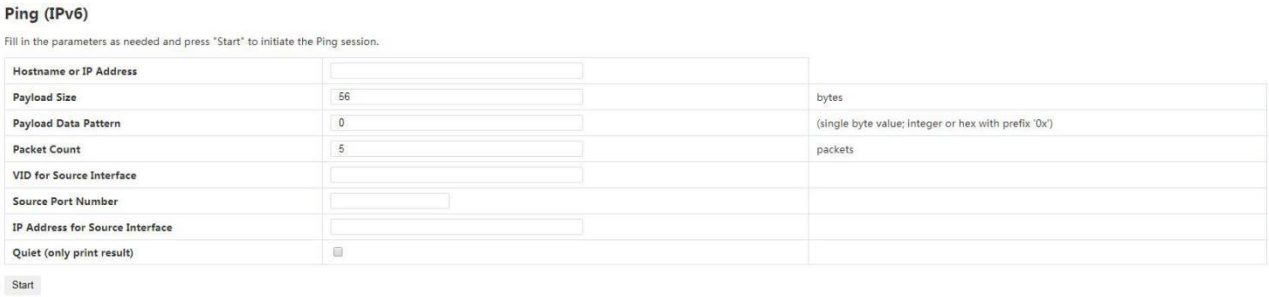
Load size	Determine the size of the ICMP data payload (in bytes) (excluding the size of the Ethernet, IP, and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.
Load data mode	Determine the mode used in the effective content of the ICMP data (that is, the message filling content). The default value is 0. The valid range is 0-255.
Packet count	Determine the number of PING requests sent. The default value is 5. The valid range is 1-60.
TTL value	Determine the value of the TTL field in the IPv4 packet header. The default value is 64. The valid range is 1-255.
Source interface VLAN	This field can be used to force the test to use a specific native VLAN interface as the source interface. Leave this field blank to automatically select based on the routing configuration.
Source port number	This field can be used to force the test to use a specific local interface with the specified port number as the source interface. Leave this field blank to automatically select based on the routing configuration.
Source interface IP address	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on the local interface. Leave this field blank to automatically select based on the routing configuration.
Stillness	Checking this option will not print the result of each ping request, only the final result will be displayed.

Note: The source interface VLAN, source port number, and source interface IP address can be configured with at most one (or none of them).
Click the "Start" button to enter the ping diagnosis display page.
Chart Figure 19-2 ping (IPv4) diagnosis result



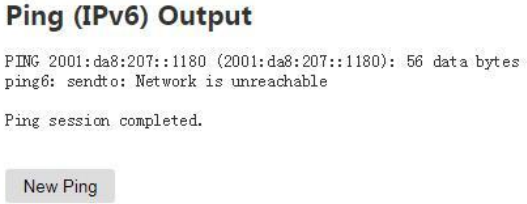
19.2 Ping(IPv6)

In the [Navigation Bar] drop-down menu, select: Diagnosis -> Ping (IPv6) to enter the diagnosis interface.
Chart Figure 19-3 ping (IPv6) diagnosis



Item	Description
Hostname or IP address	The address of the target host can be a symbolic host name or an IP address. (Does not support DNS, only IP address)
Load size	Determine the size of the ICMPv6 data payload (in bytes) (excluding the size of the Ethernet, IPv6 and ICMPv6 headers). The default value is 56 bytes. The valid range is 2-1452 bytes.
Load data mode	Determine the mode used in the effective content of the ICMPv6 data (that is, the message padding content). The default value is 0. The valid range is 0-255.
Packet count	Determine the number of PING requests sent. The default value is 5. The valid range is 1-60.
Source interface VLAN	This field can be used to force the test to use a specific native VLAN interface as the source interface. Leave this field blank to automatically select based on the routing configuration.
Source port number	This field can be used to force the test to use a specific local interface with the specified port number as the source interface. Leave this field blank to automatically select based on the routing configuration.
Source interface IP address	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on the local interface. Leave this field blank to automatically select based on the routing configuration.
Stillness	Checking this option will not print the result of each ping request, only the final result will be displayed.

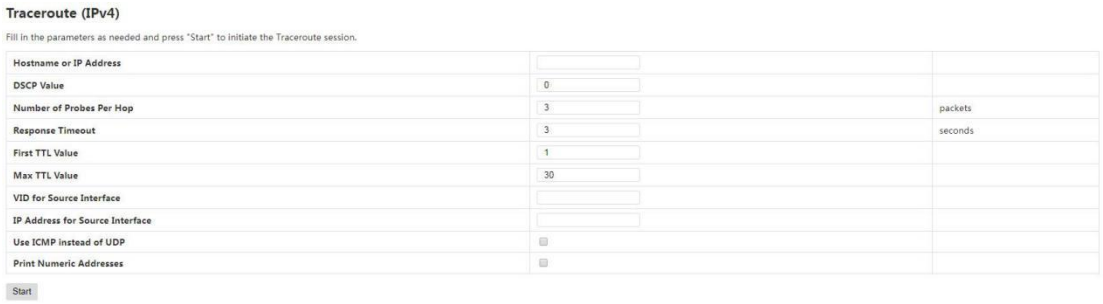
Note: The source interface VLAN, source port number, and source interface IP address can be configured with at most one (or none of them).
Click the "Start" button to enter the ping diagnosis display page.
Chart Figure 19-4 ping (IPv6) diagnosis result



19.3 Traceroute(IPv4)

In the [Navigation Bar] drop-down menu, select: Diagnosis -> Traceroute (IPv4) to enter the diagnosis interface.

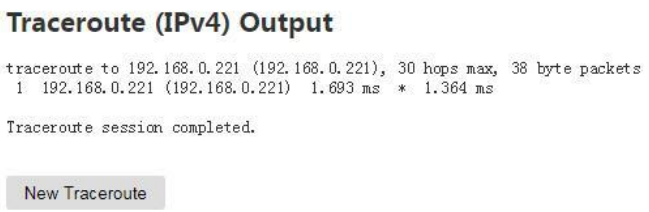
Chart Figure 19-5 Traceroute (IPv4) diagnosis



Item	Description
Hostname or IP address	The address of the target host can be a symbolic host name or an IP address. (Does not support DNS, only IP address)
DSCP value	This value is used for the DSCP value in the IPv4 packet header. The default value is 0. The valid range is 0-63.
Number of probes per hop	Determine the number of probes (data packets) sent per hop. The default value is 3. The valid range is 1-60.
Response timeout	Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.
The first TTL value	Determine the value of the time-to-live (TTL) field in the IPv4 header of the first data packet sent. The default number is 1. The valid range is 1-30.
Maximum TTL value	Determine the maximum value of the time-to-live (TTL) field in the IPv4 packet header. If this value is reached before the specified remote host is reached, the test will stop. The default number is 30. The valid range is 1-255.
Source interface VLAN	This field can be used to force the test to use a specific native VLAN interface as the source interface. Leave this field blank to automatically select based on the routing configuration.
Source interface IP address	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on the local interface. Leave this field blank to automatically select based on the routing configuration.
Use ICMP instead of UDP	By default, the traceroute command will use UDP packets. Selecting this option will force it to use ICMP ECHO packets.
Print numeric address	By default, the traceroute command will use reverse DNS lookup to print out each piece of relevant information for the obtained host IP address. If DNS information is not available, this may slow down the display speed. Selecting this option will prevent reverse DNS lookups and force the traceroute command to print digital IP addresses instead.

Click the "Start" button to enter the traceroute diagnostic display page.

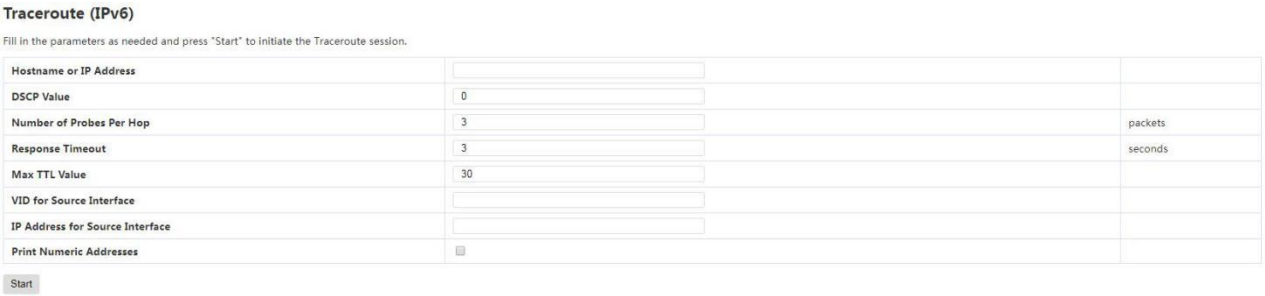
Chart Figure 19-6 Traceroute (IPv4) diagnosis results



19.4 Traceroute(IPv6)

In the [Navigation Bar] drop-down menu, select: Diagnosis -> Traceroute (IPv6) to enter the diagnosis interface.

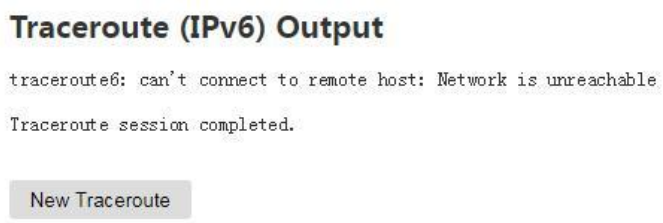
Chart Figure 19-7 Traceroute (IPv6) diagnosis



Item	Description
Hostname or IP address	The address of the target host can be a symbolic host name or an IP address. (Does not support DNS, only IP address)
DSCP value	This value is used for the DSCP value in the IPv4 packet header. The default value is 0. The valid range is 0-63.
Number of probes per hop	Determine the number of probes (data packets) sent per hop. The default value is 3. The valid range is 1-60.
Response timeout	Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.
Maximum TTL value	Determine the maximum value of the time-to-live (TTL) field in the IPv6 packet header. If this value is reached before the specified remote host is reached, the test will stop. The default number is 30. The valid range is 1-255.
Source interface VLAN	This field can be used to force the test to use a specific native VLAN interface as the source interface. Leave this field blank to automatically select based on the routing configuration.
Source interface IP address	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on the local interface. Leave this field blank to automatically select based on the routing configuration.
Print numeric address	By default, the traceroute command will use reverse DNS lookup to print out each piece of relevant information for the obtained host IP address. If DNS information is not available, this may slow down the display speed. Selecting this option will prevent reverse DNS lookups and force the traceroute command to print digital IP addresses instead.

Click the "Start" button to enter the traceroute diagnostic display page.

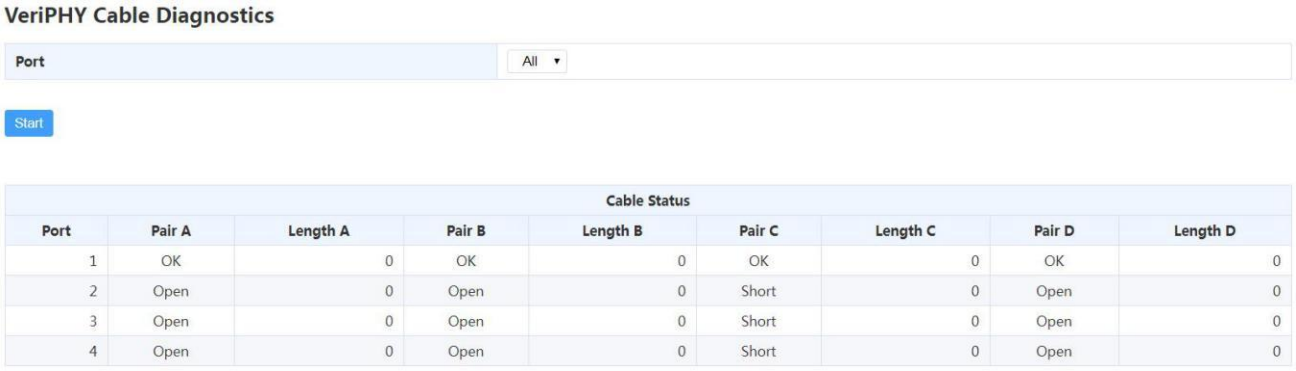
Chart Figure 19-8 Traceroute (IPv6) diagnosis results



19.5 Cable detection

In the [Navigation Bar] drop-down menu, select: Diagnosis -> Cable Detection to enter the configuration interface.

Chart Figure 19-9 Cable detection



Item	Description
Port	Select the test port, select ALL to indicate all ports
Cable status/port	Panel port number
Cable status/pair A-D	The wire pair status includes Open, Short, OK, Cross, etc.
Cable status/length A-D	Pair length, in cm

19.6 CLI reference commands

Command	switch# ping ip 192.168.6.1 size 56 data 0 repeat 5 ttl 64 switch# ping ip 192.168.6.1 saddr 192.168.6.2 switch# ping ip 192.168.6.1 sif vlan 20 switch# ping ip 192.168.6.1 sif GigabitEthernet 1/2 switch# ping ip 192.168.6.1 quiet
Description	IPv4 ping specified parameters; IPv4 ping specifies the IP address of the source interface; IPv4 ping specifies the source interface VLAN; IPv4 ping specifies the source port number; IPv4 ping quiet mode;

Command	switch# ping ipv6 2001::1 size 56 data 0 repeat 5 switch# ping ipv6 2001::1 saddr 2001::2

	switch# ping ipv6 2001::1 sif vlan 30 switch# ping ipv6 2001::1 sif GigabitEthernet 1/2 switch# ping ipv6 2001::1 quiet
Description	IPv6 ping specified parameters; IPv6 ping specifies the IP address of the source interface; IPv6 ping specifies the source interface VLAN; IPv6 ping specifies the source port number; IPv6 ping quiet mode;

Command	switch# traceroute ip 192.168.6.1 dscp 0 probes 3 timeout 3 firstttl 1 maxttl 30 switch# traceroute ip 192.168.6.1 saddr 192.168.6.2 switch# traceroute ip 192.168.6.1 sif vlan 20 switch# traceroute ip 192.168.6.1 sif GigabitEthernet 1/2 switch# traceroute ip 192.168.6.1 icmp switch# traceroute ip 192.168.6.1 numeric
Description	IPv4 traceroute specified parameters; IPv4 traceroute specifies the IP address of the source interface; IPv4 traceroute specifies the source interface VLAN; IPv4 traceroute specifies the source port number; IPv4 traceroute uses ICMP instead of UDP; IPv4 traceroute prints digital addresses;

Command	switch# traceroute ipv6 2001::1 dscp 0 probes 3 timeout 3 maxttl 30 switch# traceroute ipv6 2001::1 saddr 2001::2 switch# traceroute ipv6 2001::1 sif vlan 20 switch# traceroute ipv6 2001::1 sif GigabitEthernet 1/2 switch# traceroute ipv6 2001::1 numeric
Description	IPv6 traceroute specified parameters; IPv6 traceroute specifies the IP address of the source interface; IPv6 traceroute specifies the source interface VLAN; IPv6 traceroute specifies the source port number; IPv6 traceroute prints digital addresses;

Command	switch# veriphy switch# veriphy interface GigabitEthernet 1/3
Description	Cable detection of all ports; Cable detection designated port;

20 maintain

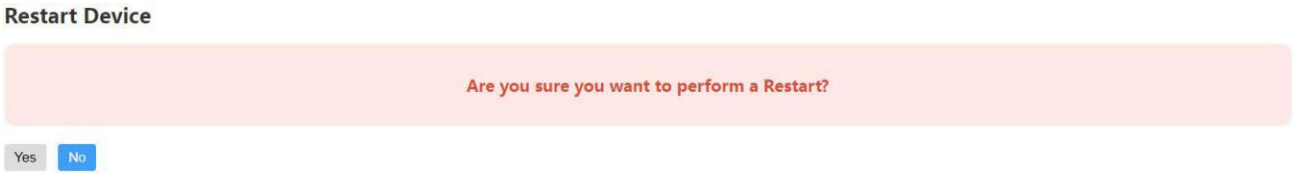
20.1 Restart the device

Note

Restarting the device will not automatically save the modified configuration, you need to go to the save configuration page to save it manually.

In the [Navigation Bar] drop-down menu, select: Maintenance -> Restart the device to enter the configuration interface.

Chart Figure 20-1 Restart the device

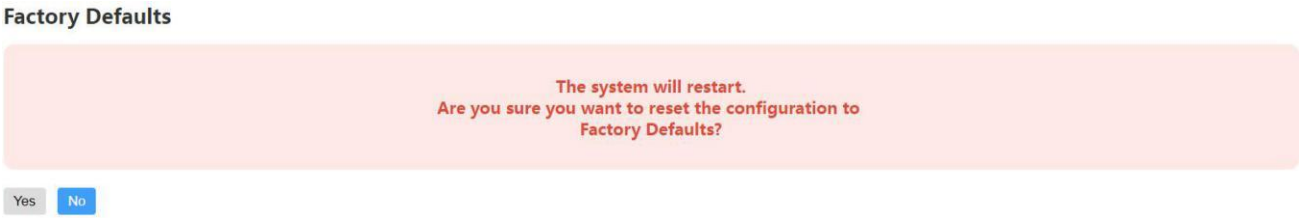


Click "Yes" to restart the device, click "No" to jump back to the port overview page.

20.2 Restore factory defaults settings

In the [Navigation Bar] drop-down menu, select: Maintenance->Restore Factory Settings to enter the configuration interface.

Chart Figure 20-2 Restore factory settings



Click "Yes" to restore the device to the default configuration, click "No" to jump back to the port overview page.

20.3 Software

20.3.1 Upgrade

In the [Navigation Bar] drop-down menu, select: Maintenance -> Software -> Upgrade to enter the configuration interface.

Chart Figure 20-3 Software upgrade

Click "Select File", select the local program file, and click "Upload" to start the software upload.

Before the upload is over, the device will be restarted to complete the software upload operation. If the management IP is inconsistent with the current management IP after the device restarts, it will be impossible to return to this interface.

20.4 Configuration

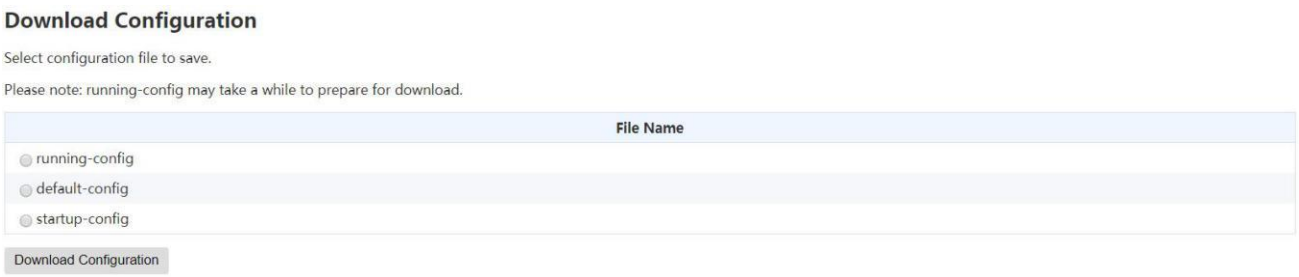
20.4.1 Save configuration

In the [Navigation Bar] drop-down menu, select: Maintenance -> Configuration -> Save Configuration to enter the configuration interface.
Chart Figure 20-4 Save configuration

Click "Save Configuration", the page will prompt the operation result.

20.4.2 Download

In the [Navigation Bar] drop-down menu, select: Maintenance -> Configuration -> Download to enter the configuration interface.
Chart Figure 20-5 Download configuration



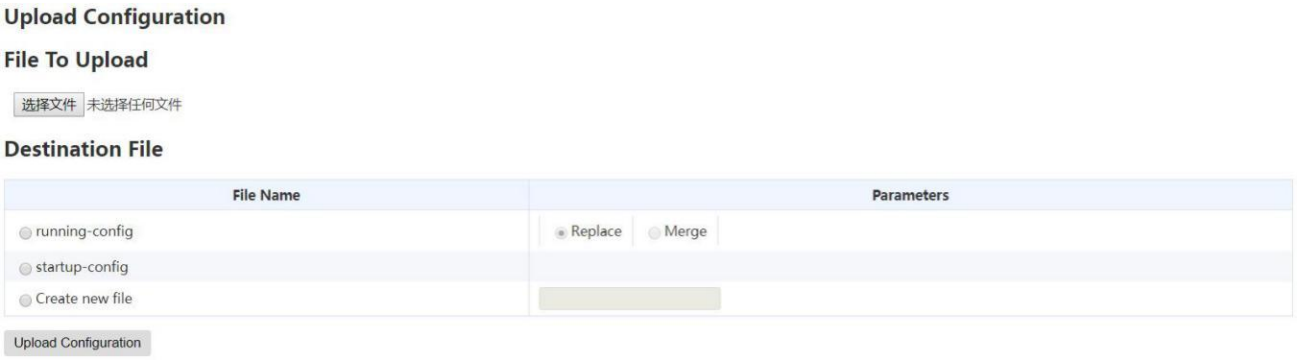
running-config: current configuration information of the system, displayed on the CLI command line.

default-config: The factory configuration of the device.

startup-config: The default configuration when power-on. If you execute "Save Configuration", it will be the system configuration information when "Save Configuration" is executed.

20.4.3 Upload

In the [Navigation Bar] drop-down menu, select: Maintenance -> Configuration -> Upload to enter the configuration interface.
Chart Figure 20-6 Upload configuration



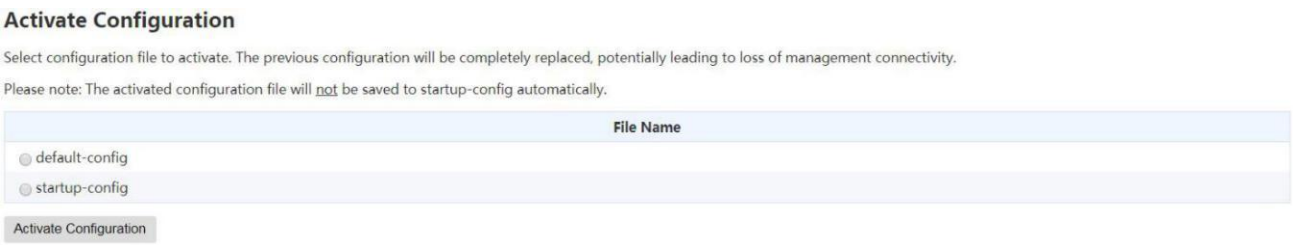
Click the "Select File" button to select the local file to be uploaded.

Select the upload object. If you select running-config, the Replace and Merge options are supported. Replace is to directly replace the current file of the system, and Merge is to merge into the current file of the system.

Click Upload configuration to complete the configuration upload, and the page will return to the operation result.

20.4.4 Activation

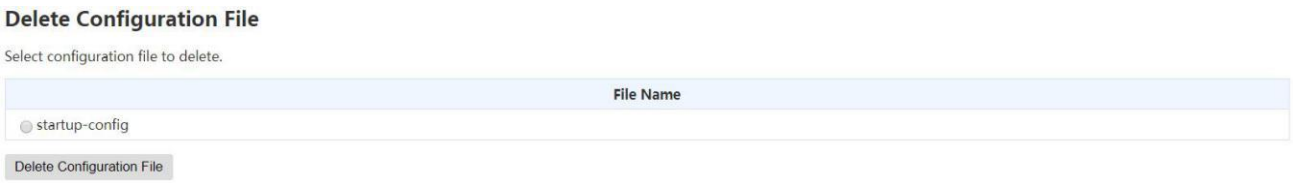
In the [Navigation Bar] drop-down menu, select: Maintenance -> Configuration -> Activate to enter the configuration interface.
Chart Figure 20-7 Activation configuration



Select the file name, click "Activate Configuration", the system will run according to the selected configuration, and the current system configuration no longer exists.

20.4.5 Delete

In the [Navigation Bar] drop-down menu, select: Maintenance -> Configuration -> Delete to enter the configuration interface.
Chart Figure 20-8 Delete configuration



Only the configuration file is deleted, and the current system operation is not affected.

20.5 CLI reference commands

Command	switch# reload cold
Description	Restart the device;

Command	switch# reload defaults
Description	Restore factory configuration;

Command	switch# firmware upgrade http://192.168.6.183/is2500-release.mfi
Description	Software upgrade;

Command	switch# copy running-config startup-config switch# copy running-config tftp://192.168.6.183/running-config switch# copy flash:backup-config tftp://192.168.6.183/backup-config switch# copy tftp://192.168.6.183/running-config running-config switch# copy tftp://192.168.6.183/backup-config flash:backup-config switch# copy startup-config running-config switch# copy flash:backup-config running-config switch# delete flash:startup-config
Description	Configuration save; Configuration download; Configure to download custom files; Configuration upload; Configure to upload custom files; Configuration activation; Configure and activate custom files; Configuration delete;