Ethernet Switch Web Management User Manual

The software version corresponding to this manual: Release 5.1.x

Document version number: V.5.1

Post date: 2022.08.05

Content

1 Overview

1.1 Introduction

In order to facilitate the operation and maintenance of network equipment by network administrators, our company has introduced the web management function of the equipment. The administrator can use the web interface to intuitively manage and maintain the equipment. The operating environment of the web network management system is shown in Figure 1-1.

Figure 1-1 Web Management Operating Environment

1.2 Login the Web Administrator

The user needs to use the default account to log in when logging into the Web administrator for the first time. After logging in, in order to ensure the safety of the device, the password needs to be changed immediately. The specific steps are as follows:

- Log in to webmaster using the default account
- Change user password

instructions

- Please refer to section 5.2 of user management for the specific operation process of changing password.

When the device leaves the factory, Web server service has been enabled by default, and it has default login account: user name is admin, login password is admin, and IP address is 192.168.1.168. Users can use these information to complete the first login of Web administrator.

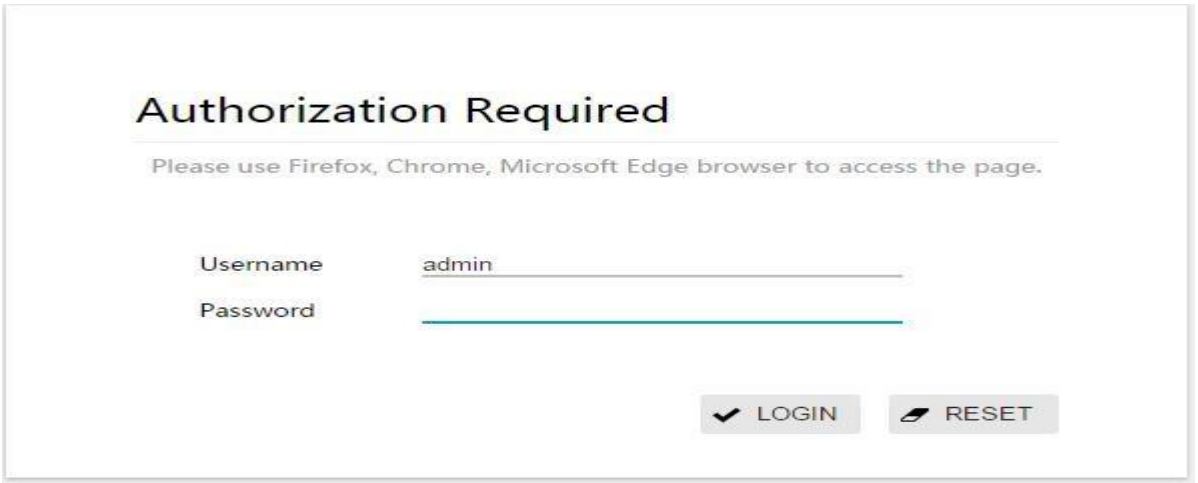
Take the 8 Port switch as an example to introduce how to log in the device via Web. The specific steps are as follows:

(1) Connect the device to the PC and connect the PC to the Ethernet port on the device (all ports belong to VLAN 1 by default) with the network cable.

(2) Configure the IP address for PC, and set the IP address of PC in the same network segment as the default VLAN interface IP address of the device (in addition to the default IP address of the device), such as 192.168.1.20.

(3) Launch the browser and enter your login information.

Figure 1-2 Web login interface



Start the browser on the PC, enter "192.168.1.168" in the address bar and enter the Web login page of the device, as shown in figure 1-2.Enter the default account "admin" and password "admin", and click the "login" button to log in to the Web administrator.The system will automatically select the language according to the operating system language used by the user, and the user can also manually switch (including Chinese and English).

(1) for the built-in browser of Windows, Edge is recommended and IE6 is not supported.

(2) In order to get better display effect, it is recommended to use Google browser, or 360 or baidu browser, as shown in figure 1-3

Figure 1-3 360 safe browser

1.3 Equipment Overview

As shown in figure 1-5, click "overview" in the menu to enter the basic information page of the system. In this page, MAC address, product serial number, software and hardware version, system running state and other information of the device can be viewed. Specific parameters are shown in table 1-1.

Figure 1-5 basic information of the system

Configuration Items	Instructions
The Host Name	A device's electronic tag, used by the user to identify the host, can only be numeric, alphanumeric, or alphanumeric combination
The MAC Address	Used to indicate the MAC address of the device
Hardware Version	Used to indicate the hardware version number of the device
Software Version	Software version number used to indicate the device
Release Time	Used to indicate when the software version of the device will be released
Product Serial Number	To indicate the product serial number of the device
CPU	To display the current CPU utilization
Available Memory (KB)	Used to display the current system available memory
The Elapsed Time	Used to indicate the continuous running time of the device after the last startup, and the time will be restarted after the restart of the device

Table 1-1 basic information parameter description

1.4 Exit of Web Administrator

notice

- The system does not automatically save the current configuration when exiting webmaster. It is recommended that users save the current configuration before exiting webmaster.

Operation steps:

Click the "logout" button below the navigation bar on the Web administrator page (as shown in figure 1-6) to exit the Web administrator.

1.5 Save Configuration

notice

- After configuring all projects on the page, be sure to save the configuration, otherwise unsaved configuration information will be lost due to restart and other operations.

Operation steps:

Click the "save" button below the navigation bar on the Web administrator page (as shown in figure 1-6) to save the current configuration to the configuration file. The configuration is still valid after restart or power-down restart. There are two ways to save a configuration:

(1) in the current configuration interface, click "ok" or "apply" button, that is, save the current configuration into memory.Saving at this time does not really save the configuration items into the configuration file. If the switch has power failure or other failures at this time, the configuration of the interface will fail.
(2) click the "save" button below the navigation bar, and the system will automatically save the configuration of all pages to the configuration file.

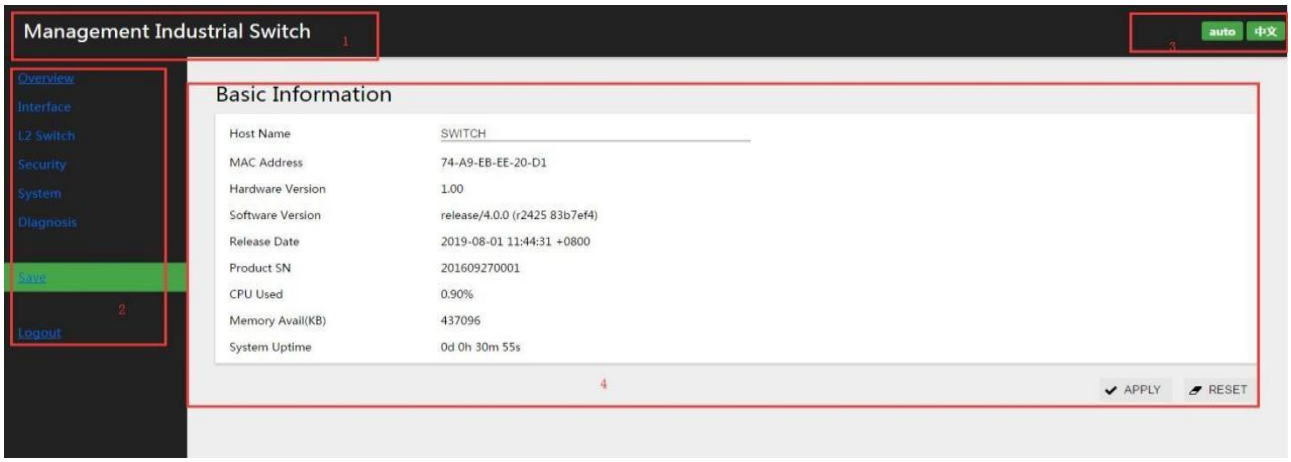
1.6 Introduction to Web Management Page Layout

As shown in figure 1-6, the main page of Web management is divided into four parts: product model, navigation bar, language selection button, and configuration area. Function description of each part is shown in table 1-2.

Table 1-2 Web layout instructions

Configuration Items	Instructions
Product Model	Used to display the product model
The Navigation Bar	Organize the Web network management function menu of the device in the form of navigation tree. Users can choose the function menu conveniently in the menu The selection results are displayed in the configuration area
Language Selection	For switching languages, currently only Chinese and English are supported
The Configuration Area	An area for users to configure and view

Figure 1-6 Web administration home page



(1) Product Model	(2) Navigation Bar	(3) Language Selection	(4) Configuration Area

1.7 Introduction to Web Management Functions

The specific description of Web network management function is shown in table 1-3.

Table 1-3 Web management function description

Menu/Tab			Functional Explanation
Overview	Basic information		Displays the device's MAC address, serial number, hardware and software version, and sets the device's electronics Tags, CPU usage, elapsed time, etc
Port	Port management		Displays information about all ports and sets the various features of the ports
	Port speed limit		Show/set port speed limit
	Storm control		Show/set the suppression ratio for broadcast, multicast, and unknown list play ports
	Port statistical		Display, query, and clear interface statistics
	Port mirror		Show/set/delete the mirror of the port
	Port isolation		Show/set/remove port isolation
	Port aggregation	Overall configuration	Show/configure an algorithm for port aggregation
		Aggregation port	Displays information about the aggregation interface, as well as information about the port members in the aggregation interface
		Aggregate member port	Configure the aggregation port ID to which the member port belongs, working mode
	PoE management	PoE Overall Configuration	Display/configure PoE power supply in non-standard mode
		PoE Interface configuration	Show/configure PD devices that PSE hangs

Exchange	VLAN	VLAN		Create, modify, and delete vlans
		Interface		Display port status, configure port properties, VLAN ownership
	ERPS	Overall situation		Shows the status of ERPS, previous event, ring number, east interface, west interface, etc.
		Configuration	Ring configuration	Configure the ERPS ring number, east interface, west interface
			Instance configuration	Configure blocking points of ERPS, manage VLAN, data VLAN, etc
	IGMP Snooping	IGMP Snooping		Turn on/off the IGMP Snooping function
		IGMP routing mouth		Show/configure IGMP routing ports
		IGMP static group		Display/configure IGMP static groups
	Spanning tree	Overall situation		Displays the MSTP port parameters
		Global configuration		Display and set MSTP global parameters
		The MST configuration		Display MSTP field information, modify the MSTP field
		The instance		Create/delete MSTP instances
		Interface		Display and set MSTP port parameters
	MAC management	MAC management		Set the aging time for MAC addresses
		Static address		Configure static MAC addresses without aging table entries
		Filter addresses		Used to discard packets containing a specific MAC address
Security	The ACL	The ACL		Create, modify, and delete vlans
		Application		Display port status, configure port properties, VLAN ownership
	QoS	Overall situation		Display/configure QoS, queue weights
		Port trust		Show/configure QoS port trust
		CoS mapping		Display/configure QoS CoS mapping
		DSCP mapping		Display/configure QoS DSCP mapping
		Strategy		Display/configure QoS policies
	DHCP Snooping	Disable/enable		Enable/disable this feature
		Trust in the mouth		Set the trust port for DHCP Snooping
	802.1 X authentication	General Situation		Display 802.1x authentication profile
		configuration		The configuration of 802.1 X
	MAC authentication	General situation		Displays a MAC authentication profile
		configuration		Configure MAC authentication
	The RADIUS	Global configuration		RADIUS global configuration
		The server		Show/configure RADIUS server configuration

System	Manage IP addresses		Set the administrative IP address of the device
	User management		Set user password
	Telnet server		Turn on/off the Telnet server
	SNMP	SNMPv1 /v2c	Configuration SNMPv1 / v2c
		SNMPv3	Configuration SNMPv3
	Date and time		Displays/sets the current system date and time
	Profile management	Download the back up	Setup to back up configuration files to localhost
		Restore the back up	Set up a local restore profile to the device
		factory Data reset	Settings to restore the device to its factory configuration
	System upgrade		Set up upload upgrade file from local host to upgrade system software
	Log/diagnosis		Generate a diagnostic information file and open it for viewing or saving on the localhost
	Restart		Set up the reboot device
The diagnosis	Web tools		Perform the ping/trace route operation and display the results
	Dying -- Gasp		Turn on/off the gas gasp alert
	Optical module information		View optical module information, such as manufacturer information, serial number, optical power, etc
Save	\		Save the currently set parameters to ensure the restart is valid
Cancellation	\		Log out

2 Interface

2.1 Port Management

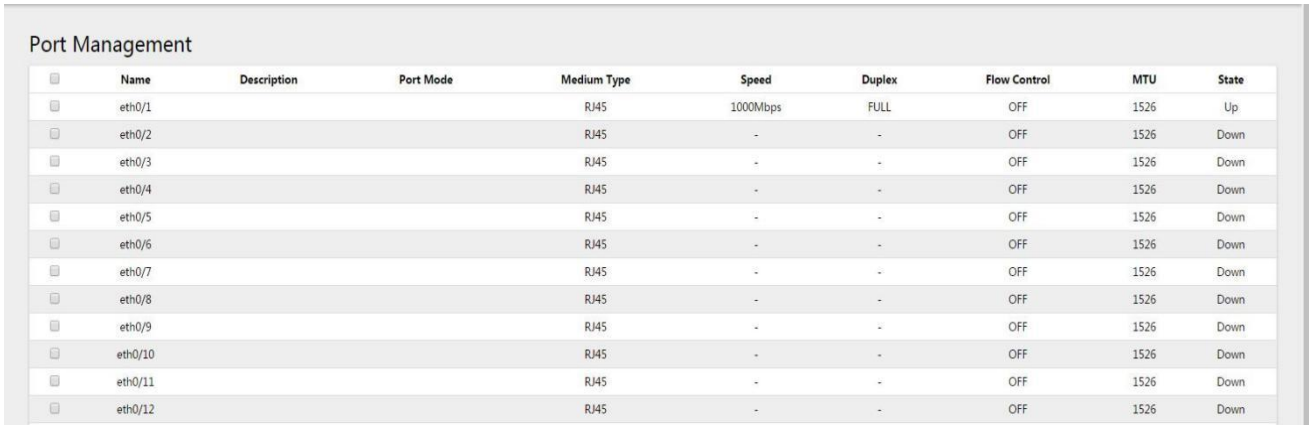
- Due to the different parameters of electrical port and optical port, it is recommended to configure electrical port and

notice

optical port separately when selecting multi-port configuration.

The port management module is used to configure and view the working parameters of the Ethernet interface, including: name, description, port mode, media type, rate, duplex state, flow control, MTU, state, as shown in figure 2-1.

Figure 2-1 interface management interface



Operation steps:

(1) select [interface] [port management] in the menu, as shown in figure 2-1.

(2) check the ports to be configured (support multiple ports) and click the "edit" button to enter the page as shown in picture 2-2.

(3) configure the working parameters of the port, as shown in table 2-1.

(4) click the "apply" button to complete the operation.

(5) click the "save" button in the menu to save the configuration.

Figure 2-2 interface configuration interface

Table 2-1 interface working parameters description

Configuration Items	Instructions
Describe	Set the description information for the port, using a combination of letters and Numbers.
Medium Type	Configure the media type of the multiplexing port, which is only valid for ports that support photoelectric multiplexing (Combo). • RJ45: set the port to work in port mode. • SFP: set the port to work in port mode.
Rate	Set the rate of the port • 10 m: 10 MBPS • M: 100 100 MBPS • M: 1000 1000 MBPS • AUTO: automatically negotiates port rates
Duplex State	Sets the duplex state of the port • AUTO: self negotiating duplex • FULL duplex • sheldon: HALF duplex
Port Mode	Set the working mode of the port to support different working modes, which need corresponding optical module support. • 100base-fx: set the port to work in 100 MB light mode. • 1000base-x: set the port to work in gigabit light mode. • SGMII: set the port to work in SGMII mode, which needs to be configured when the optical port inserts gigabit to 100 MBPS (SFP ge-fx) or light-to-electricity (mini-gbic-gt) modules. • 2500base-x: set the port to work in 2.5g optical port mode. • 10G base-x: set the port to work in 10G optical port mode.  • 2500base-x mode, there may be incompatibility with port interconnection of other manufacturers. • The optical port capability of different types of equipment is different, please refer to the specification document corresponding to the specific product model. • This feature is only supported by optical ports
Flow Control	Set Enable or Disable port traffic control functions When this end and the end of the device can enable the flow control function, if the end of the device congestion, send a message to the end of the device, notify the end of the device to temporarily stop sending messages;After receiving the message, the opposite device will temporarily stop sending the message to the opposite device. And vice versa. Thus, packet loss is avoided  Flow control can be realized only when the flow control function is turned on at both the local port and the opposite port

MTU	Settheframelengthallowedforforwardingfrom64to10240bytes.Thedefault is 1526 bytes.
Manage State	Set the open/closed state of the port. • Shutdown: the port setting is working normally. • Shutdown: setting up the port is in the Shutdown state.

Configuration examples:

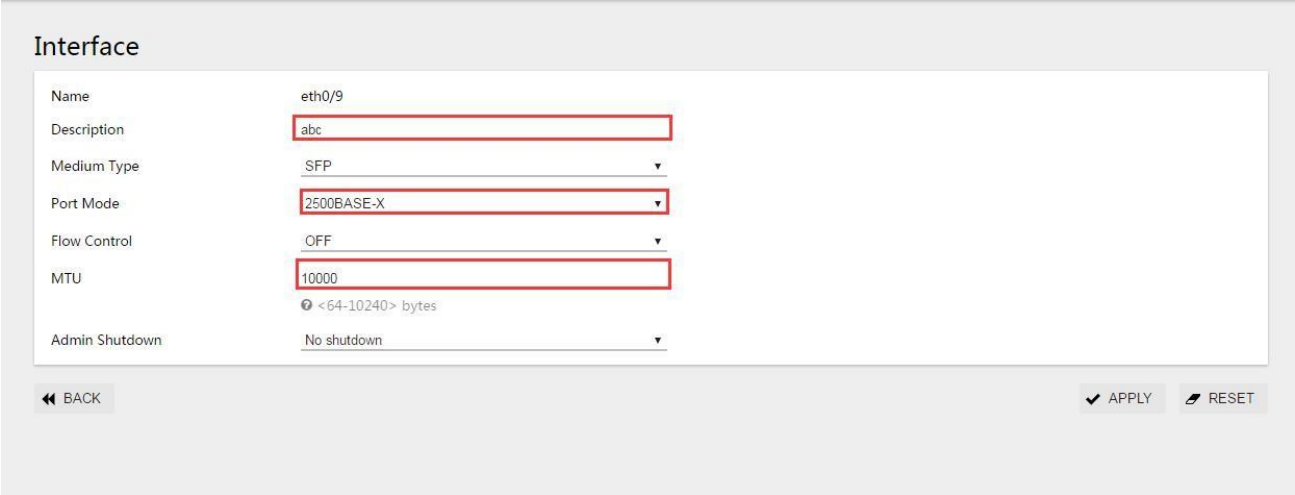
Case requirements: configure port eth0/9 to work in 2.5g mode, turn off flow control, set MTU to 10000 bytes, and port description to ABC.

Step1: select "interface" and "port management" in the menu to enter the port management interface.

Step 2: select port eth0/9 and click the "edit" button to enter the port configuration interface, as shown in figure 2-3.

Step 3: as shown in figure 2-3, follow the description of "ABC", medium type "SFP", portmode "2500base-x", flow control "OFF", MTU "10000", management state "No shutdown", and configure parameters.

Figure 2-3 interface configuration example



Step 4: click the apply button to complete the operation.

Step 5: click the "save" button in the menu to save the configuration.

2.2 Port Speed Limit

Port speed limit is a port-based speed limit, which limits the total speed of port input and output messages.Before the flow is sent from the interface, speed limit is configured on the direction of the

interface to control all outgoing message flow. Before the traffic is received from the interface, the speed limit is configured in the direction of the interface to control all incoming message traffic.

Operation steps:

(1) select [interface] [port speed limit] in the menu and enter the port speed limit configuration interface, as shown in figure 2-4.

(2) for ports that need to be configured with speed limit, enter corresponding values in the dialog box, and the specific parameters are defined as shown in table 2-2.

(3) click the "apply" button on the corresponding port to complete the operation.

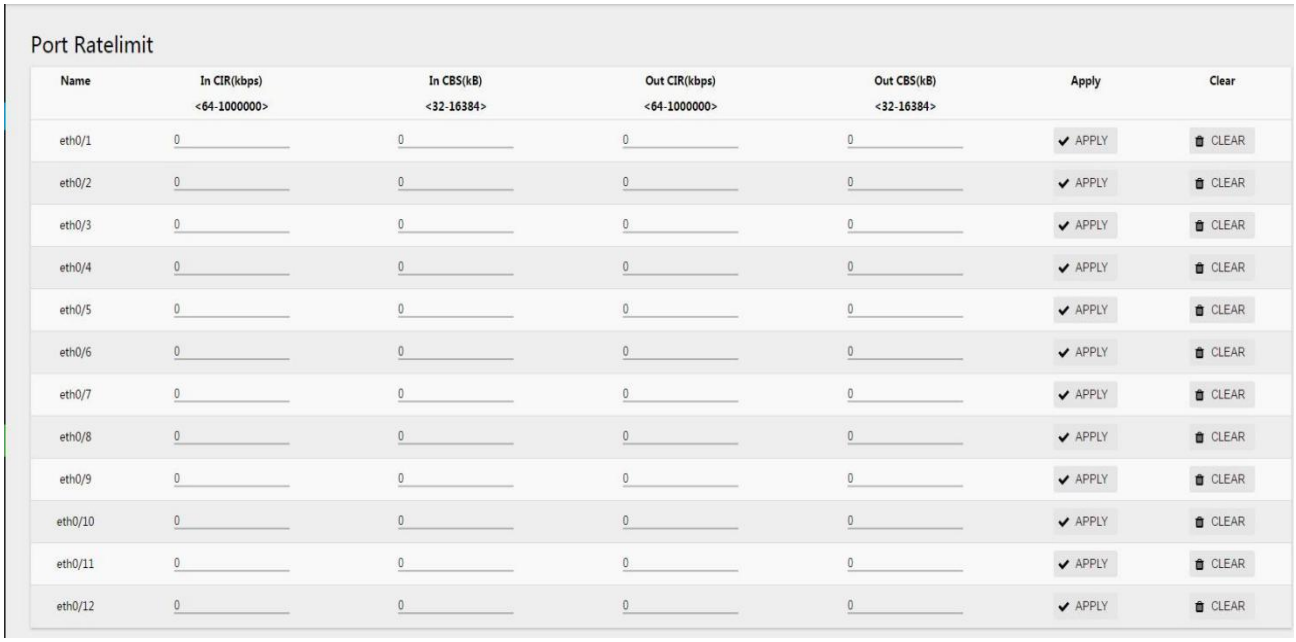
(4) click the "save" button in the menu to save the configuration.

note

- This feature only supports single-port configuration, such as eth0/1, and if parameters are entered on other ports, when eth0/1's apply button is clicked,

  Parameters for other ports are cleared (configuration does not take effect).

Figure 2-4 port speed limit interface



instructions

- Limit values are deterministic, such as 1M, and 1024, but burst values are derived from empirical values. When the burst
  The numerical distribution is large, the flow peak is higher, the speed limit is stable, but the average speed may be higher than the speed limit. When the burst value is small, the flow peak is low and the speed limit is limited
  The average speed may be less than the speed limit. It is recommended to configure burst with a value of 4 times limit and a small value of 16384.

Table 2-2 parameter description

Configuration Items	Instructions
Input Rate (KBPS)	Bandwidth limit per second of input direction (KBits).
Input Burst Flow (KB)	Burst traffic limits in the input direction (Kbytes).
Output Rate (KBPS)	Bandwidth limit per second in the output direction (KBits).
Output Burst Flow (KB)	Output direction burst traffic limit (Kbytes).
Application	Sets the port speed limit function that enables the specified port.
Remove	Clear the dialog box of what has been filled in.

Configuration examples:

Case requirements: suppose the port eth0/1 of the switch is connected to the Internet, the traffic limit at the port eth0/1 outlet is required, the bandwidth limit is 102400KBits per second, and the burst traffic limit is 256Kbytes per second.

Step 1: select [interface] [port speed limit] in the menu to enter the port speed limit configuration interface.

Step 2: fill in the corresponding parameter dialog box for port eth0/1, as shown in figure 2-5. Step 3: click the [apply] button of port eth0/1 to complete the configuration.

Figure 2-5 port speed limit configuration interface

Step 4: click the "save" button in the menu to save the configuration.

2.3 Storm Control

When there is excessive broadcast, multicast or unknown unicast data stream in local area network, the network performance will decline, or even the phenomenon of network paralysis, called broadcast storm.Storm control for broadcast and multicast and unicast unknown data flow speed, when the switch port receives the broadcast and unknown unknown multicast or unicast data flow rate exceeds the bandwidth set, the device will only be allowed through the data stream set bandwidth, beyond the bandwidth of data flow will be discarded, so as to avoid excessive flood storms formed in the data stream into the LAN.
Storm control module for setting port suppression ratio for broadcast, multicast, unknown list broadcast.The storm control mode based on bandwidth percentage is adopted.When the speed of data stream received by the device port exceeds the set bandwidth, the device will only allow the data stream passing through the set bandwidth, and the data stream exceeding the set bandwidth will be discarded until the data stream returns to normal.

Configuration steps:

(1) select [interface] [storm control] in the menu and enter the storm control interface, as shown in FIG. 2-6.
(2) check the ports to be configured (support multiple ports) and click [edit] to enter the page shown in figure 2-7.
(3) configure storm suppression types and bandwidth suppression ratios of ports, as shown in table 2-3.

(4) click the "apply" button to complete the operation.

(5) click the "save" button in the menu to save the configuration

Figure 2-6 interface of storm control state

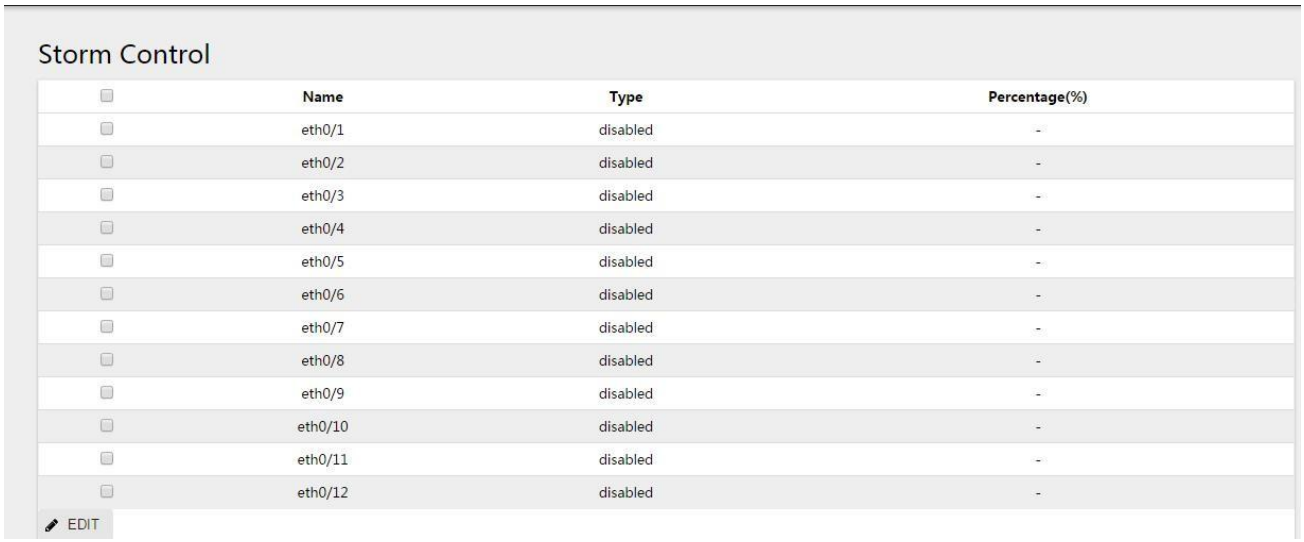
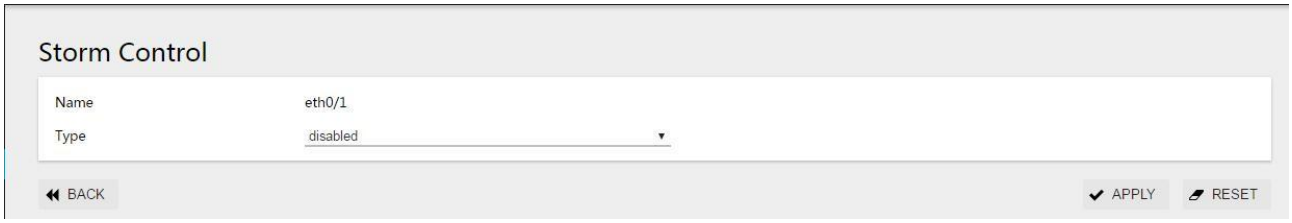


Figure 2-7 port configuration interface



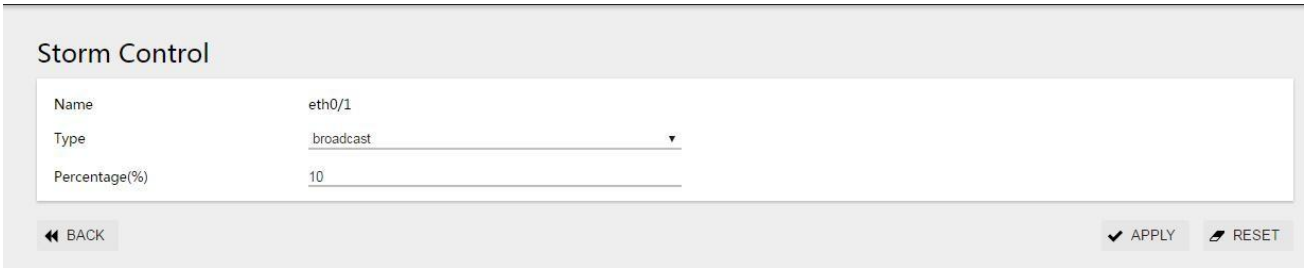
Configuration Items		Instructions
Name		Selected port
Type	disabled	Turn this feature off.
	broadcast	Turn on the broadcast message storm suppression function to realize the traffic limit of broadcast message.
	multicast	Open unknown group broadcast text storm suppression function, can realize the unknown group broadcast text traffic Restrictions.
	unicast	Open unknown list broadcast text storm suppression function, can realize the unknown list broadcast text traffic Restrictions.
	Multicast and broadcast	Turn on the storm suppression function of group broadcast message + broadcast message to realize the unknown group broadcast message and wide Traffic restrictions for broadcast text.
	Unicast and broadcast	Open unknown list broadcast text + broadcast message storm suppression function, can realize the unknown list broadcast Traffic limits for text and broadcast messages.
	all	Select suppress broadcast, multicast, unknown list broadcast.
Bandwidth ratio (%)		The maximum broadcast traffic allowed as a percentage of the port's transmission capacity Enter a specific percentage.

Table 2-3 parameter description

Configuration examples:

Case requirements: enable storm control on port eth0/1, and set the suppression ratio of broadcast messages to 10%.
Step 1: select [interface] [storm control] in the menu to enter the storm control interface.
Step 2: select port eth0/1 and click the "edit" button to enter the configuration screen. Step 3: select broadcast as type and set the bandwidth ratio to 10, as shown in figure 2-8. Step 4: click the apply button to complete the operation.

Figure 2-8 storm control configuration interface



Step 5: click the "save" button in the menu to save the configuration.

2.4 Port Statistics

The port statistics function is used to display statistics about the number of messages received and sent by ports.
(1) Select [interface] -> [port statistics] in the menu and enter the port statistics page, as shown in figure 2-9.
(2) In the page, check the number of messages received and sent by each port of the device, the number of bytes, and the rate of sending and receiving. The specific parameters are shown in the table 2 to 4.

Figure 2-9 port statistics page

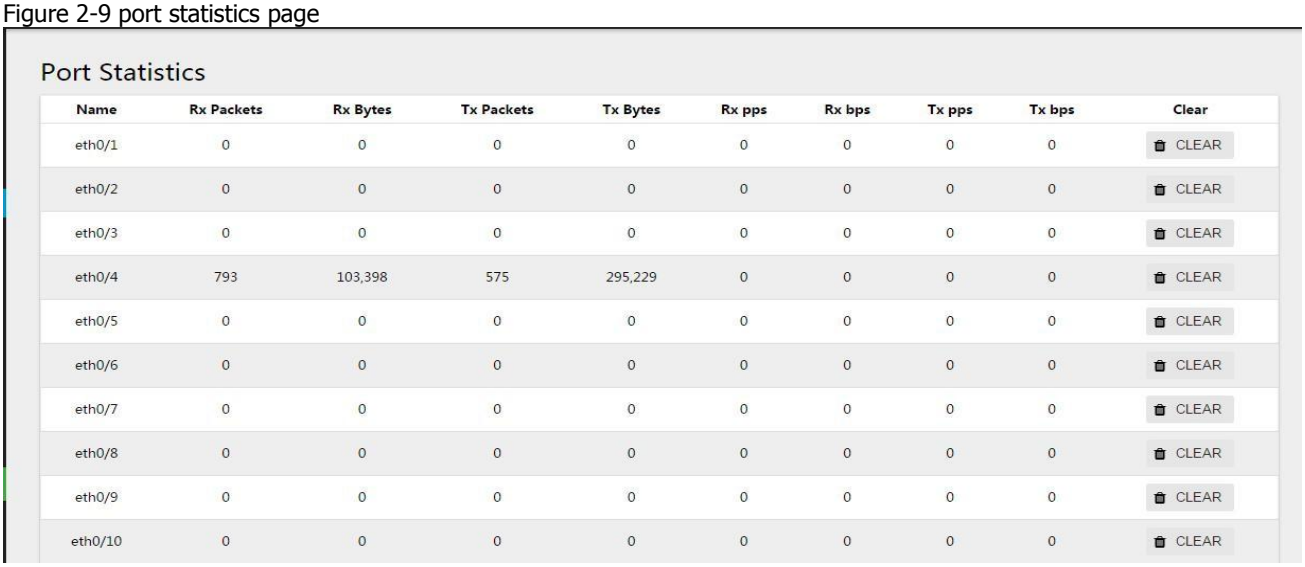


Table 2-4 port statistical parameter description

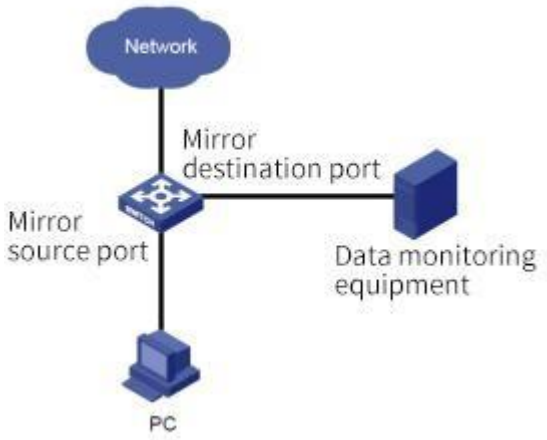
Configuration Items	Instructions
The name of the	Switch port
Receive a message	All messages received by the interface
Number of bytes received	The number of bytes of all messages received by the interface
Number of messages sent	All messages sent by the interface

Number of bytes sent	The number of bytes of all messages sent by an interface
Reception rate (PPS)	Interface receiving rate, unit PPS (bit per second bit/second)
Reception rate (BPS)	Packet Per Second Packet rate received by the interface, BPS (Packet Per Second)
Send rate (PPS)	Interface send rate, unit PPS (bit per second bit/second)
Sending rate (BPS)	Packet Per Second Packet Per Second Packet Packet
remove	Reset message

2.5 Port Mirroring

SPAN (Local Switched Port Analyzer) is the Local mirror function.The function of SPAN will copy the packet of the designated port to the destination port. In general, the destination port of SPAN will access data detection equipment. Users will use these devices to analyze the packet received by the destination port for network monitoring and troubleshooting, as shown in figure 2-10.
SPAN does not affect the message exchange between the source port and the destination port, but simply copies a copy of all incoming and outgoing messages from the source port to the destination port. Messages may be discarded when the mirror traffic of the source port exceeds the destination port bandwidth, such as when the 100Mbps destination port monitors the traffic of the 1000Mbps source port. SPAN is based on session management, configuring the source and destination ports of SPAN in the session.There can be only one destination port in a session, but multiple source ports can be configured simultaneously.

Figure 2-10 port mirroring



Configuration steps:

(1) select [interface] [port mirror] in the menu and enter the page shown in figure 2-11.

Figure 2-11 port mirroring interface

(2) click the "add" button to enter the page as shown in picture 2-12.

Figure 2-12 port mirroring configuration interface

(3) select the session, destination interface and source interface, and the specific parameters are described in table 2-5.
(4) click the "apply" button to complete the operation.

(5) click the "save" button in the menu to save the configuration.

Table 2-5 port mirroring parameters

Configuration Items	Instructions
The session	Select the group number of the port mirroring group to configure, and you can create a total of seven mirroring groups.
Purpose interface	Select mirror destination port, only one destination interface per session is allowed
The source interface	Selectmirrorsourceportstoallowmultiplesourceportstoexistsimultaneously

Configuration examples:

Case requirement: monitoring eth0/1 port and eth0/2 inbound/outbound messages using port eth0/3.

Step1:select[interface][portimage]in the menutoentertheportimageconfiguration interface.

Step 2: click the "add" button to enter the port image configuration interface.

(6) select the session, destination interface and source interface, and the specific parameters are described in table 2-5.
(7) click the "apply" button to complete the operation.

(8) click the "save" button in the menu to save the configuration.

Table 2-5 port mirroring parameters

Configuration Items	Instructions
The session	Select the group number of the port mirroring group to configure, and you can create a total of seven mirroring groups.
Purpose interface	Select mirror destination port, only one destination interface per session is allowed
The source interface	Selectmirrorsourceportstoallowmultiplesourceportstoexistsimultaneously

Configuration examples:

Case requirement: monitoring eth0/1 port and eth0/2 inbound/outbound messages using port eth0/3.
Step1:select[interface][portimage]in the menutoentertheportimageconfiguration interface

Step 3: click the "add" button to enter the port image configuration interface.
Step 4: click the "apply" button to complete the configuration and automatically return to the port mirroring interface. You can see the successfully created mirror group 1, as shown in figure 2-14.

Figure 2-14 port mirror display interface

Step 5: click the "save" button in the menu to save the configuration.

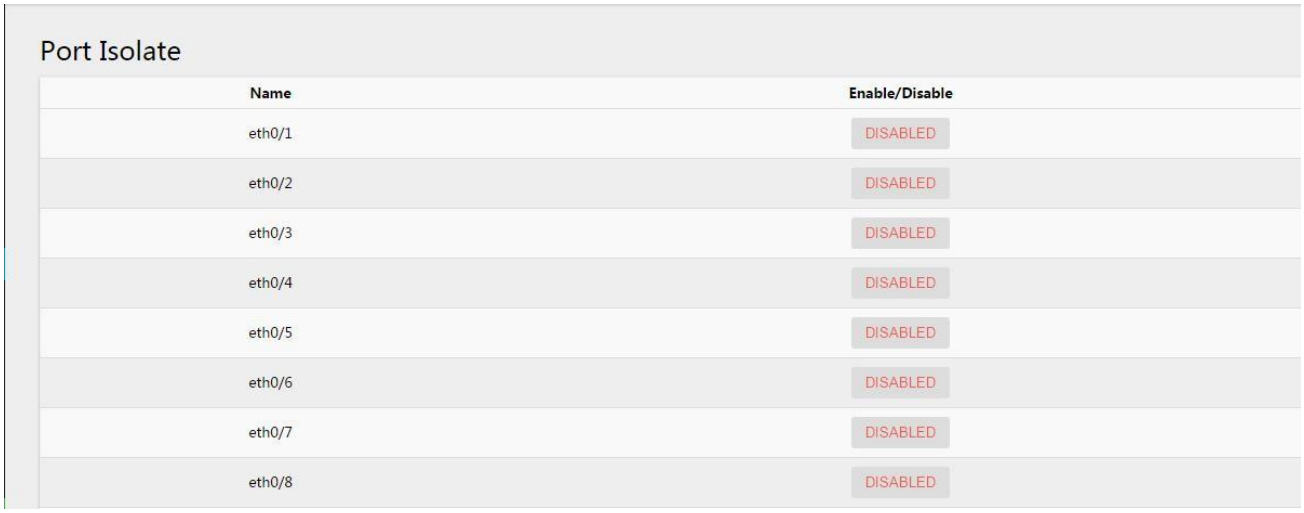
2.6 Port Isolation

In order to achieve layer isolation between messages, different ports can be added to different vlans, but limited VLAN resources will be wasted.The isolation between ports in the same VLAN can be realized by using the port isolation feature.The user only needs to add ports to the isolation group to realize the two-layer data isolation between ports in the isolation group. The function of port isolation provides users with a more secure and flexible networking scheme. The port isolation feature is independent of the VLAN to which the port belongs.For devices that do not support uplinking ports, two-way traffic interchanges between ports in isolation group and ports outside isolation group.
Configuration steps:

(1) select [interface] [port isolation] in the menu to enter the port isolation interface, as shown in figure 2-15.
(2) select the port to be isolated and click the "enable/disable" button.

(3) click the "save" button in the menu to save the configuration.

Figure 2-15 port isolation interface

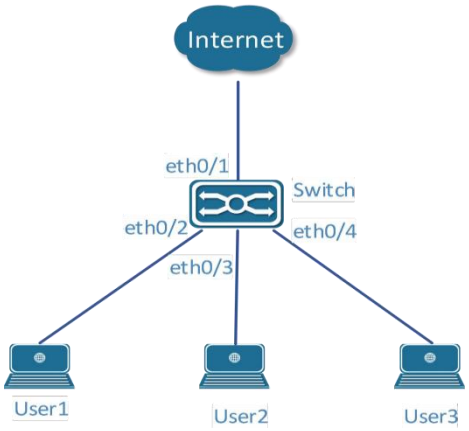


Configuration examples:

Networking requirements, as shown in figure 2-16:

- the cell User1, User2, and User3 are connected to the Switch ports eth0/2, eth0/3, and eth0/4, respectively.
- the device connects to the external network through the eth0/1 port.
- eth0/1, eth0/2, eth0/3 and eth0/4 belong to the same VLAN;Realize that cell users User1, User2 and User3 cannot communicate with each other, but can communicate with external network.

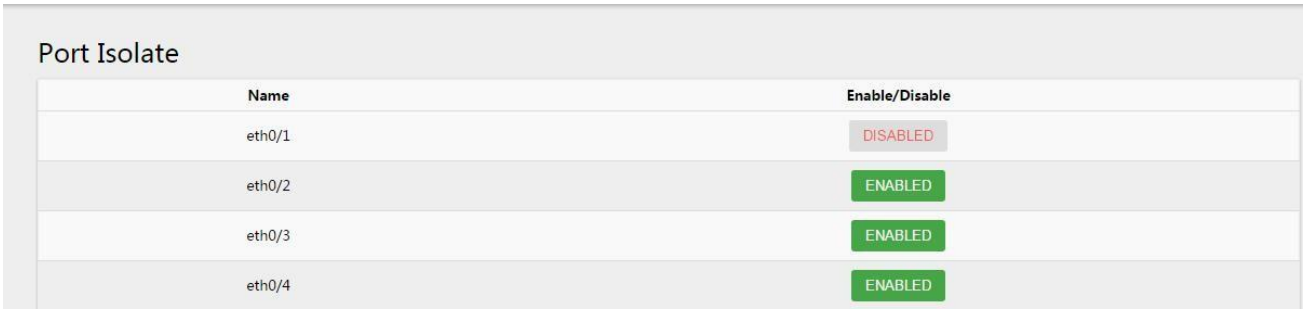
Figure 2-16 networking topology



Step 1: select [interface] -> [port isolation] in the menu to enter the port isolation interface.

Step 2: select eth0/2, eth0/3, eth0/4, and click the [disabled] button to enable port isolation, as shown in figure 2-17.

Figure 2-17 port isolation configuration interface



Step 3: click the "save" button in the menu to save the configuration.

2.7 Port Aggregation

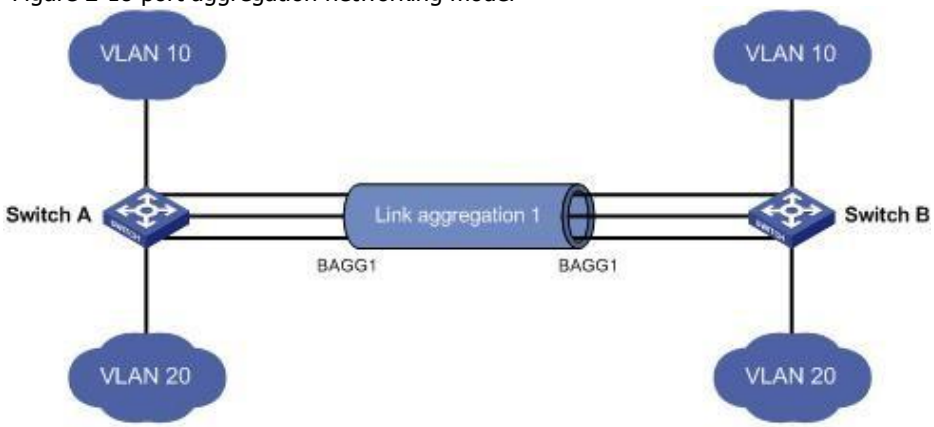
2.7.1 Overview

2.7.1.1 Polymerization Mouth

Binding multiple physical links together creates a logical link, which we call an aggregate port

(port-channel).This function conforms to ieee802.3ad standard. It can be used to extend link bandwidth and provide higher connection reliability. It is often used for port connection, as shown in figure 2-18.

Figure 2-18 port aggregation networking model



The polymerization port has the following characteristics:

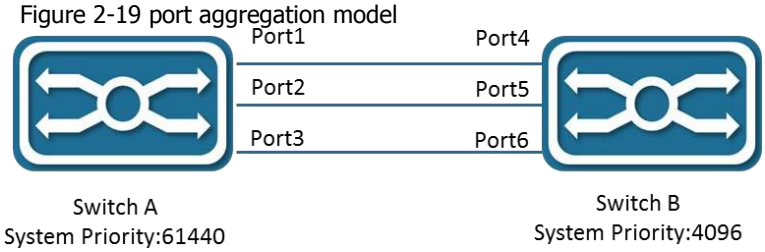
(1) high bandwidth, the total bandwidth of the aggregation port is the sum of the bandwidth of the physical member ports;
(2) support the traffic balancing strategy, according to which traffic can be allocated to each member link;

(3) support link backup. When a member link in the aggregation port is disconnected, the system will automatically allocate the traffic of the member link to other effective member links in the aggregation port.

2.7.1.2 LACP

Link Aggregation Control Protocol (LACP) based on IEEE802.3 AD standard is a Protocol for dynamic Link Aggregation.If the port is enabled by the LACP protocol, the port sends the LACPDU to announce its system priority, system MAC, port priority, port number, operation key, etc.After receiving the LACP message of the opposite end, the connected device compares the system priority of both ends according to the system ID in the message.At one end of the system ID higher priority, will be in accordance with the port ID, in order of priority from high to low set aggregation group within the port is in a state of aggregation, and issue the updated LACP packets, the terminal device after receiving the message, will set the corresponding port into the aggregation state, so that the two sides on the exit port or join aggregation group to achieve consistently.Only when both ports have completed the dynamic aggregation binding operation can the physical link forward the datagram.
After the LACP member port link is bound, periodic LACP message interactions are also conducted. When the LACP message is not received for a period of time, the packet receipt timeout is considered, the member port link is unbound, and the port is again in the non-forwarding state. There are two modes of timeout: long timeout mode and short timeout mode.In the long timeout mode, a packet is sent at an interval of 30 seconds. If the opposite packet is not received within 90 seconds, it will be in the packet receiving timeout.In the short timeout mode, a packet is sent at an interval of 1 second between ports, and if the opposite packet is not received within 3 seconds, it is in the packet receiving timeout.

Figure 2-19 port aggregation model



As shown in figure 2-19, switch A and switch B are connected through three ports.The system priority of switch A is 61440, and the system priority of switch B is 4096.Open the LACP port aggregation on the three directly connected ports of switch A and B, set the aggregation mode of the three ports as the active mode, and set the port priority of the three ports as the default priority 32768.
After receiving to end LACP message, switch B found their system ID is higher priority (switch B of A higher priority than switches) system, and in accordance with the order of the port ID priority (port under the condition of the same priority, according to the order of the port since the childhood) set port 4, 5, and 6 in the aggregation state.When switch A receives the updated LACP message from switch B, it finds that the system ID of the opposite end has A higher priority, and the ports are set to aggregate state, and ports 1, 2 and 3 are set to aggregate state.

2.7.2 Configure the Aggregation Port

Configuration steps:

(1) select [interface] [port aggregation] in the menu, enter the port aggregation configuration interface, and select load balancing algorithm in the global configuration interface, as shown in figure 2-20, and parameter description is shown in table 2-6.

Figure 2-20 global configuration interface for port aggregation

Table 2-7 global configuration parameter description

Configuration Items		Instructions	
Global configuration	Name	Load balancing algorithm	
	Value	DST - MAC	Equalize by destination MAC address.
		SRC - MAC	Equalize according to the source MAC address.
		SRC-DST-MAC	Balance by source MAC address and destination MAC.
		DST IP -	Equalize by destination IP address.
		SRT - IP	Balancing based on source IP addresses.
		SRC - DST - IP	Balance based on source IP address and destination IP address.
		DST - port	Equalize according to the L4 TCP/UDP destination port number.
		SRC - port	Equalize according to the L4 TCP/UDP source port number.
		SRC - DST - port	The L4 TCP/UDP source and destination port Numbers are balanced.
	Application		Click on the enable

(2) in the aggregation port member, configure the "ID" and "mode" of the corresponding port, and click "apply" to complete the configuration, as shown in FIG. 2-21 and table 2-8 of parameter description.

Figure 2-21 aggregation port member configuration interface

Table 2-8 parameter description of aggregation member port configuration

Configuration Items		Instructions	
Aggregate member port	Name	Corresponding port number	
	ID	The ID of the aggregation port member	
	Model	Manual	Set to manual mode
		The Active	This port initializes the LACP aggregation operation
		Passive	The port will not initiate the LACP aggregation operation actively, but passively participate in the LACP calculation after receiving the neighbor's LACP packet.
	Application	Click on the enable	
	Remove	Click clear the physical port	

After the configuration is completed, the aggregation port ID and member port information that have been successfully created will be displayed in the interface of the aggregation port, as shown in figure 2-22, and the parameter description table 2-9.

Figure 2-22 aggregation interface display

Table 2-9 parameters of polymerization port

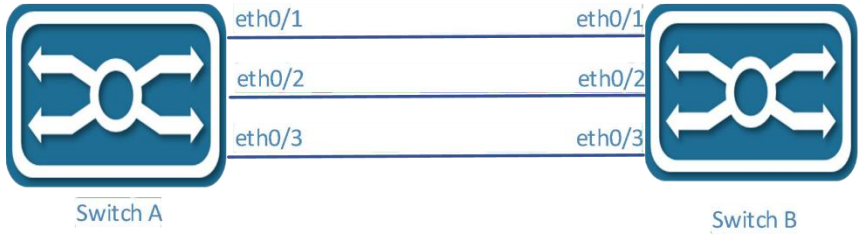
Configuration Items		Instructions
The aggregation mouth	ID	The ID of the aggregation port.
	Name	Name of polymerization port
	Members	The specific aggregator member name.

2.7.3 Configuration Examples

1. Networking requirements

- Switch A and Switch B connect to each other through their layer 2 Ethernet ports eth0/1 through eth/0/3, as shown in figure 2-23.
- Switch A and Switch B are connected by three physical links.On Switch A and Switch B, ports are configured as port aggregation groups, so that the outgoing/incoming load is Shared among member ports.

Figure 2-23 port aggregation example



2. Configuration steps

Load sharing can be achieved using both static and dynamic aggregation groups. The configuration methods for both groups are described below.

(1) method 1: configure static aggregation groups

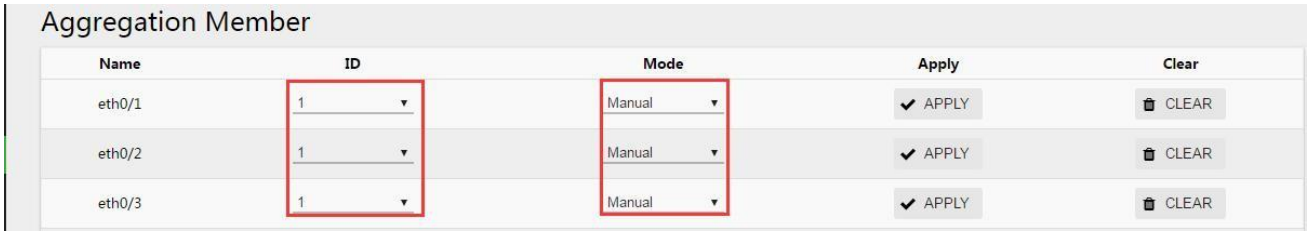
Step 1: select [interface] [port aggregation] in the menu to enter the port aggregation configuration interface.

Step 2: in the global configuration item, select "load balancing algorithm" as src-ip, and click "apply" button to save the configuration, as shown in figure 2-24.

Figure 2-24 global configuration

Step 3: from the aggregation port member, select eth0/1, ID is "1", mode select "Manual", and click "apply" to save the configuration.

Figure 2-25 aggregation member port static configuration



After configuration, you can see the successful aggregation port 1 created in the aggregation port, as shown in figure 2-26.

Figure 2-26. Create a successful static aggregation port

Step 4: click the "save" button in the menu to save the current configuration.

(2) method 2: configure dynamic aggregation groups

Step 1: select [interface] [port aggregation] in the menu to enter the port aggregation configuration interface.

Step 2: in the global configuration item, select "load balancing algorithm" as src-ip, and click "apply" button to save the configuration, as shown in figure XXX.

Figure 2-27 global configuration

Step 3: from the aggregation port member, select eth0/1, ID is "1", mode select "Manual", click "apply" to save the configuration, and use the same operation to complete the configuration of eth0/2 and eth0/3 successively, as shown in figure XXX.

Figure 2-28 aggregate member port dynamic configuration

After configuration, you can see the successful aggregation port 1 created in the aggregation port, as shown in figure 2-29.

Figure 2-26. Create a successful dynamic aggregation port

Step 4: click the "save" button in the menu to save the current configuration.

2.8 Management of PoE

instructions

- Switches with PoE modules only support PoE features.
- Non-poe switches, PoE functions are displayed in Web pages, but no configuration is allowed.

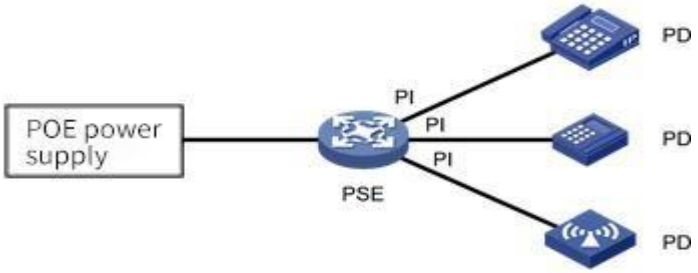
2.8.1 Introduction of PoE

The PoE (Power over Ethernet) refers to the remote Power supply of the equipment via the Ethernet port by connecting the twisted pair of wires to the external PD (Powered Device).

PoE system composition

The PoE system is shown in figure 2-27, including PoE Power supply, PSE (Power Sourcing Equipment), PI (Power Interface) and PD.

Figure 2-27 PoE system



1. The PoE power supply

PoE power supplies the entire PoE system.

2. The PSE

PSE is the device that directly powers PD.PSE comes in two flavors: Endpoint (Endpoint) and Midspan (Endpoint) : PSE integrates with the switch, and PSE and the switch are independent.PSE of our company adopts built-in methods. PSE supports main functions including finding and detecting PD, classifying PD, supplying power to it, power management, and detecting whether the connection with PD is disconnected, etc.

3. The PI

PI refers to Ethernet interfaces with PoE power supply capability, also known as PoE interfaces, including FE and GE interfaces.
PoE interface remote power supply has two modes:

Signal line power supply mode: PSE USES 3/5 type twisted pair (1, 2, 3, 6) to transmit data to PD and direct current at the same time. Idle line power supply mode: PSE USES 3/5 type twisted pair of wires (4, 5, 7, 8) that are not used for data transmission to transmit direct current to PD.

4. PD

PD is the device that receives PSE power, such as IP phone, wireless AP (Access Point), portable device charger, card reader, network camera and so on.
PD equipment can be connected to other power sources while receiving PoE power supply for power redundancy backup.

2.8.2 Configuration PoE

instructions

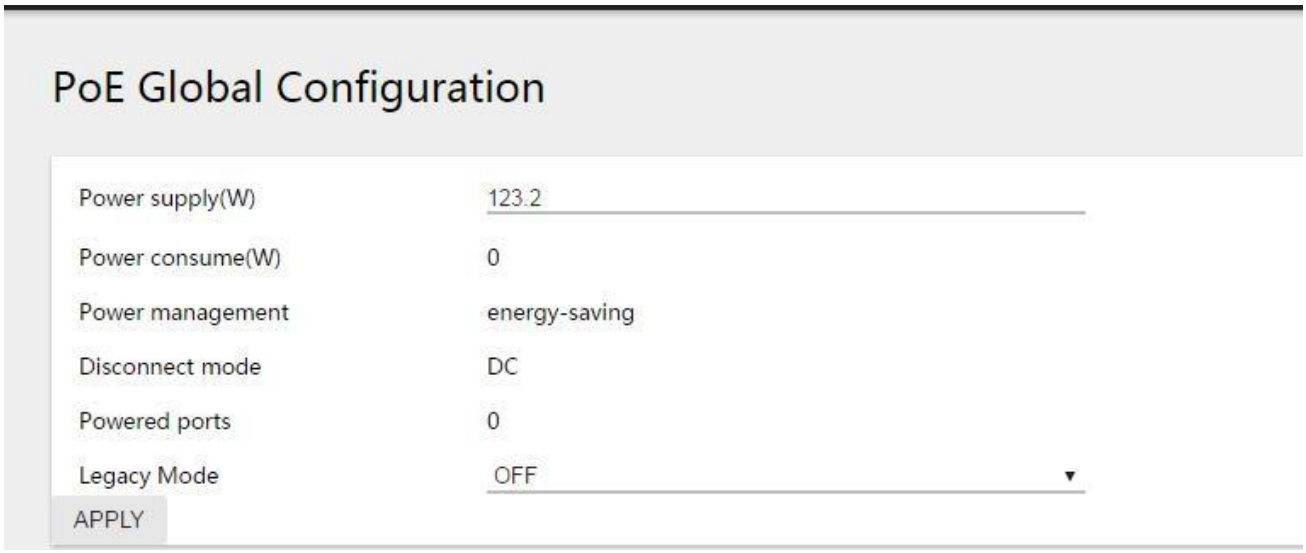
Before configuring PoE functions, make sure that the PoE power supply or PSE is in a normal operating state, otherwise you may not be able to configure or configure the PoE
The function does not work.

PoE configuration steps:

(1) select [interface] -> [PoE management] in the menu to enter the PoE management interface.

(2) set the maximum power in PoE global configuration, and click "apply" to complete the configuration, as shown in figure 2-28.

Figure 2-28 PoE global configuration



PoE global configuration parameters are described in table 2-10.

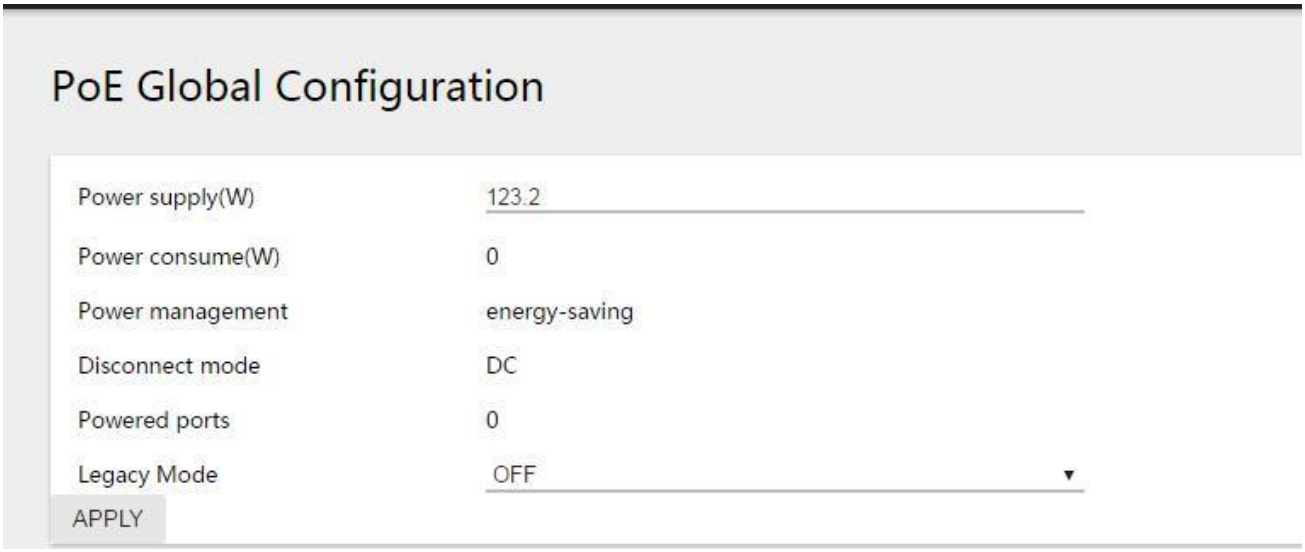
Table 2-10 PoE global configuration parameter descriptions

Configuration Items	Explanation
The most powerful	By default, the default power provided by the device is 15.4w * port number. For example, the maximum power provided by 8-port device is 123.2w. If the maximum power of PoE power supply is less than the maximum output powerof the equipment, the maximum output power of PoE power supply should be set to-10w (mainboard power consumption) in order to prevent the power of the equipment from exceeding the PoE power rating and causing overcurrent of PoE power supply.
Consumed power	Shows the total power consumed by the PoE.
Power supply management	The default is energy saving mode, and the power allocated for each port is calculated by the actual consumed power. PSE will allocate the excess power to other ports by default.
Port mode	The default is DC disconnect mode.
Number of power supply ports	Displays the number of ports currently powered.
Compatibility mode	ON/OFF, default to OFF. OFF: only standard PD devices are supported. The detected resistance is between 19k and 26.5k, and the detected capacitance is less than 150nF. ON: supports non-standard PD devices, which can supply power to some PD devices whose detected resistance and capacitance values exceed the standard values. 

	This function belongs to the global mode and is effective for all ports. It is necessary to confirm that the device with port access is PD product, otherwise it is easy to cause wrong power supply to the access device and cause damage to the device.

(3) select the port to be configured, click [edit] to enter the interface configuration interface, and select "enable/disable" the PoE function of this port, as shown in figure 2-29.

Figure 2-29 PoE interface configuration



(4) click the "apply" button to complete the operation and return to the PoE main interface, as shown in figure 2-30.

Figure 2-30 PoE interface configuration main interface

(5) click the "save" button in the menu to save the configuration. The PoE port status parameters are described in table 2-11.

Table 2-11 PoE parameter description

Configuration Items	Instructions
Enable/disable	Set enable or disable PoE power on ports
State	PoE current power supply state, OFF power supply shutdown state, ON power supply state.
Why	-sheldon: the port is Short of power.
Current	Current operating current of the device.
Power	The power consumed by the current device.

instructions

- The default power supply priority of the system is: the priority decreases with the increase of port number
- When the external power supply of the equipment is insufficient, the PoE interface with high power supply priority shall

be given priority to power supply.

- If PSE power is low, no matter the priority of newly connected PD, it will not close the port that has been supplied, and no power will be supplied to newly connected PD.

3 Exchange

3.1 A VLAN

3.1.1 Overview

VLAN is short for Virtual Local Area Network, which is a logical Network divided on a physical Network. This network corresponds to the second layer of the ISO model.Vlans are not partitioned by the physical location of the network ports. A VLAN has the same properties as a normal physical network, except that there are no physical location restrictions. The second layer of unicast, broadcast, and multicast frames are forwarded and diffused within one VLAN without directly entering 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.

3.1.2 Link Type

Link connection types of ports can be divided into two types according to different processing methods of VLAN Tag by ports when forwarding messages:
Access:

Messages sent by the port do not carry VLAN Tag, which is generally used to connect with terminal devices that cannot recognize VLAN Tag, or when different VLAN members do not need to be distinguished.
Trunk:

For messages sent by the port, messages in the default VLAN do not carry Tag, while messages in other vlans must carry Tag.Usually used for interconnection between network transmission devices.
Hybrid:

Messages sent by the port can be set with Tag in some vlans and without Tag in some vlans as required. Hybrid type ports are used for both interconnection between network transport devices and direct connection to terminal devices.

3.1.3 Default VLAN (PVID)

In addition to the vlans that ports allow to pass, you can set the default VLAN for ports.By default, the default VLAN for all ports is VLAN 1, but the user can configure it as needed.

- the default VLAN for an Access port is the VLAN to which it belongs.
- Trunk ports and Hybrid ports allow multiple vlans to pass through and configure the default VLAN.
- when removing a VLAN, if the VLAN is the default VLAN of a port, the default VLAN of the port will revert to VLAN 1 for Access port; For Trunk or Hybrid ports, the default VLAN configuration for ports does not change, meaning they can use a VLAN that no longer exists as the default VLAN.

- It is recommended that the default VLAN for this end device port be the same as the default VLAN for the connected end device port.
- It is recommended to ensure that the default VLAN for the port is the VLAN that the port is allowed to pass through. If a port does not allow a VLAN to pass through, but the default VLAN of the port is that VLAN, the port discards the received message of the VLAN or the message without VLAN Tag.

1.7.1.1 Port Processing of Messages

After configuring the port connection type and the default VLAN, there are several different conditions for the port to receive and send messages, as shown in table 3-1.

Table 3-1 port mail message processing

Port Type	Processing of received messages		Processing of sending messages
	When a packet is received without Tag	When a message is received with Tag	
The Access	Adds the default VLAN to the message The Tag	• Receive this message when the VLAN is identical to the default VLAN • When the VLAN is different from the default VLAN, the newspaper is discarded	Remove Tag and send the text
Trunk	• VLAN columns allowed when the default VLAN is on the port When the table is in, it receives the message and adds the Tag of the default VLAN to the message • When the default VLAN is not in the list of vlans that the port allows to pass, the message is discarded	• The VLAN receives the message when it is in the list of vlans that the port allows to pass through • When the VLAN is not in the list of vlans that the port allows to pass, the message is discarded	• When the VLAN is the same as the default VLAN and in the list of vlans that ports allow to pass through, remove the Tag and send the text • When the VLAN is different from the default VLAN and the port is allowed to pass through the VLAN list, keep the original Tag and send the text
Hybrid			When the VLAN is in the list of vlans that the port allows to pass, the user can manually configure whether to remove the Tag or not by sending the message

3.1.4 Configuration VLAN

3.1.4.1 Introduction to VLAN Configuration

Configure the Access port-based VLAN

Table 3-2 VLAN configuration steps based on Access ports

Steps	Configuration Tasks	Instructions
1	Configure the connection type of the port	optional The connection type for the configured port is Access, and by default, the connection type for the port is Access
2	Create a VLAN	Optionally create one or more vlans
3	Configure the default VLAN for the port	Configure the default VLAN for Access ports

Configure a VLAN based on Trunk ports

Table 3-3 VLAN configuration steps based on Trunk ports

Steps	Configuration Tasks	Instructions	
1	Configure the connection type of the port	Will choose The connection type for the configured port is Trunk By default, the port's connection type is Access	By default, the Trunk port is Tagged VLAN (the default VLAN) is VLAN 1 prompt When a Trunk port's Untagged VLAN is changed, the Trunk port's Untagged VLAN will be automatically Tagged VLAN
2	Create a VLAN that needs to be added to this Trunk	Optionally create one or more vlans	
3	Configure the Trunk to which the VLAN belongs	Select the Trunk and add the VLAN	Will choose Trunk port has only one Untagged VLAN, which is its default VLAN.

Configure vlans based on Hybrid ports

Table 3-4 VLAN configuration steps based on Hybrid ports

Steps	Configuration Tasks	Instructions	
1	Configure the connection type of the port	Will choose Configure the port's connection type as Hybrid By default, the port's connection type is Access	Hybrid ports can have multiple Untagged vlans. So, configure the Hybrid port multiple times through these two steps Tagged VLAN will also be available By default, the Hybrid port's Untagged VLAN is VLAN 1
2	Create a VLAN that needs to be added to the Hybrid port	Optionally create one or more vlans	
3	Configure the Trunk to which the VLAN belongs	Select the Trunk and add the VLAN	The Hybrid port can have multiple Tagged vlans. Therefore, Tagged VLAN configured multiple times for Hybrid ports through these two steps will be valid at the same time

3.1.4.2 Configure Ports in the VLAN

The VLAN configuration interface is shown in figure 3-1, and the detailed description of each parameter is shown in table 3-5.

Figure 3-1 VLAN configuration interface

Table 3-5 VLAN configuration parameters

Configuration Items	Instructions
ID	Select the group number of the port mirroring group to configure, and you can create a total of seven mirroring groups.
The name of the	VLAN name, not configurable, default VLAN 1 is default, VLAN 2 is VLAN0002.
Tagged member port	A port member sends a VLAN message with a Tag Tag.
Tagged member port	A port member sends a VLAN message without a Tag Tag.
The editor	Select the VLAN ID to edit and click this button to enter the edit interface.
Add	Click this button to enter the VLAN add interface.
Delete	Select the VLAN ID to edit, and click this button to remove the VLAN.

Configuration steps:

(1) select [switch] -> [VLAN] in the menu to enter the VLAN configuration interface, as shown in figure 3-2.

Figure 3-2 VLAN display interface

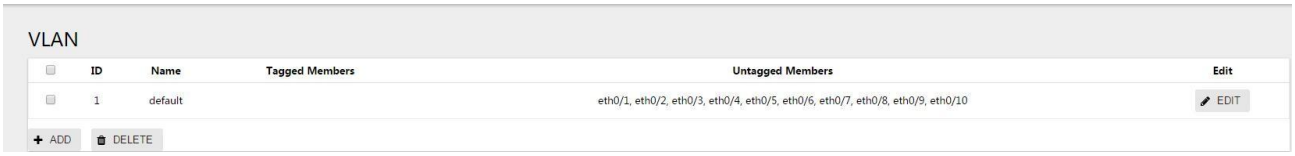


Figure 3-3 VLAN configuration interface

(2) click the "add" button to enter the page as shown in picture 3-3.

(3) configure the port members of VLAN, click the "apply" button to complete the operation.

(4) click the "save" button in the menu to save the configuration.

3.1.4.3 Configure the VLAN to Which the Port Belongs

The interface configuration interface is shown in figure 3-4, and the detailed description of each parameter is shown in table 3-6.

Figure 3-4 interface display interface

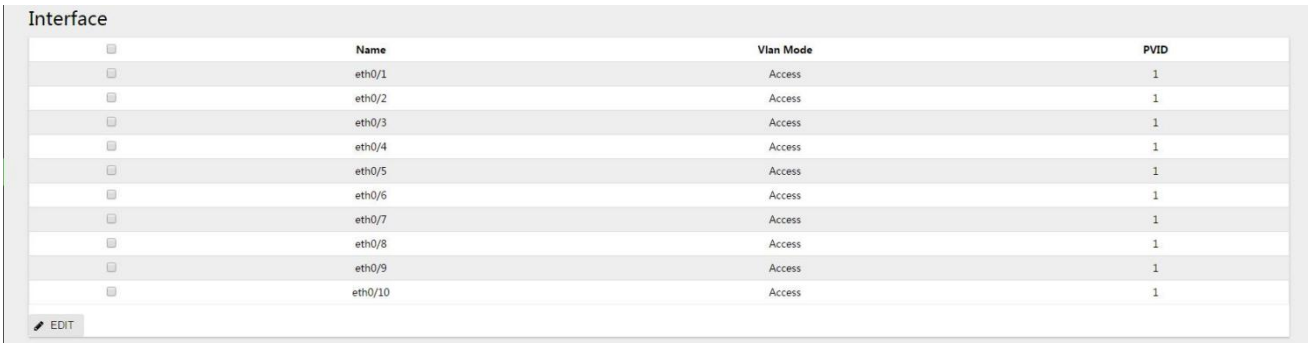


Table 3-6 interface configuration parameters

Configuration Items		Instructions
Name		Corresponding port name.
VLAN mode	The Access	Configure the port type to be an Access port.
	Trunk	Configure the port type to be Trunk.
	Hybrid	Configure the port type to be the Hybrid port.
PVID		PORT-BASE VLAN ID, suitable for Access PORT.
Native Vlan		Native vlans (Native vlans) are Native to the Trunk.
The editor		Select the port to edit and click this button to enter the edit interface.

Configuration steps:

(1) select [switch] -> [VLAN] in the menu to enter the interface configuration interface, as shown in figure 3-4.
(2) select the port to be configured and click the "edit" button to enter the interface configuration page.

(3) configure the VLAN mode of the port, PVID or Native VLAN. In general, it is recommended to configure the Native VLAN in the Trunk as 1. The configuration interface is shown in figure 3-6.

Figure 3-6 VLAN configuration interface

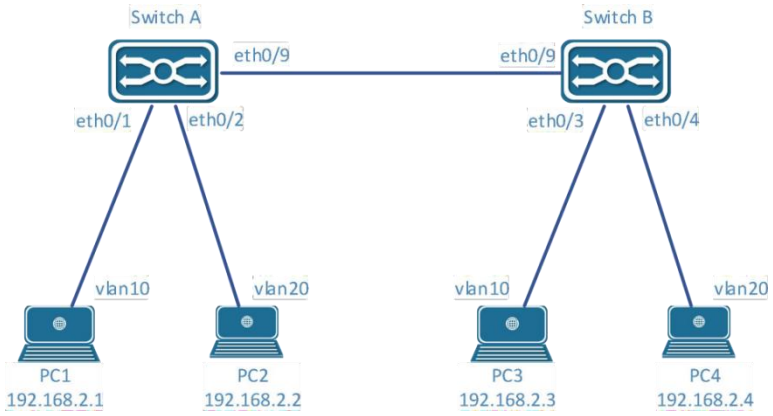
(4) click the "save" button in the menu to save the configuration.

3.1.5 VLAN Configuration Example

Configuration example:

Case requirements :Switch A and Switch B connect with each other through trunk. PCS of the same VLAN can exchange visits, and PCS of different vlans are forbidden to exchange visits. The network topology is shown in FIG. 3-7.

Figure 3-7 network topology diagram



Switch A configuration:

Step 1: configure eth0/9 as a Trunk and Native Vlan as a default of 1.

Select [VLAN] in the menu [switch] to enter the interface configuration interface.Select port eth0/9 and click the "edit" button to enter configuration mode, as shown in figure 3-8.Select Trunk for VLAN mode, Native VLAN default is 1.

Figure 3-8 interface configuration interface

Step 2: create VLAN 10,VLAN 20, and add VLAN 10 and VLAN 20 to Trunk eth0/9.

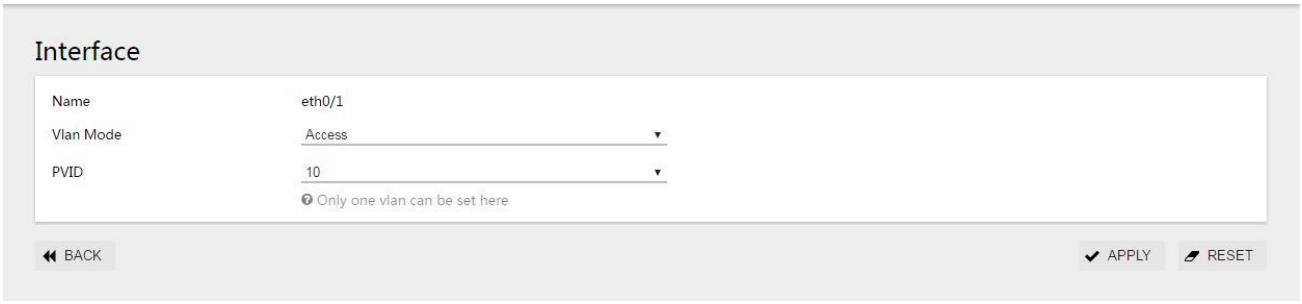
Under the Tagged member port, click "add" button to enter the VLAN editing interface, as shown in figure 3-9. Enter "10,20" in the dialog box, select port eth0/9 from Tagged member port, and click "apply" button to complete the configuration.

Figure 3-9 VLAN configuration interface

Step 3: configure port eth0/1 VLAN mode for Access and PVID 10.

Under the interface interface, select eth0/1 and click the "edit" button to enter the interface configuration interface, as shown in figure 3-10.VLAN mode is the default Access and PVID is configured at 10.Click the "apply" button to complete the configuration.

Figure 3-10 VLAN configuration interface



Step 4: configure port eth0/2 VLAN mode for Access and PVID 20.

In step 3, set eth0/2's VLAN mode to Access and PVID to 20.Click [apply] to complete the configuration, and the VLAN interface is shown in figure 3-11:

Figure 3-11 VLAN interface

Step 5: click the "save" button in the menu to save the configuration.

Switch B configuration:

Eth0/9 and eth0/10 are configured with the Switch A.Create VLAN 10 and VLAN 20 and complete the corresponding port configuration.After configuration, the VLAN interface is shown in figure 3-12.

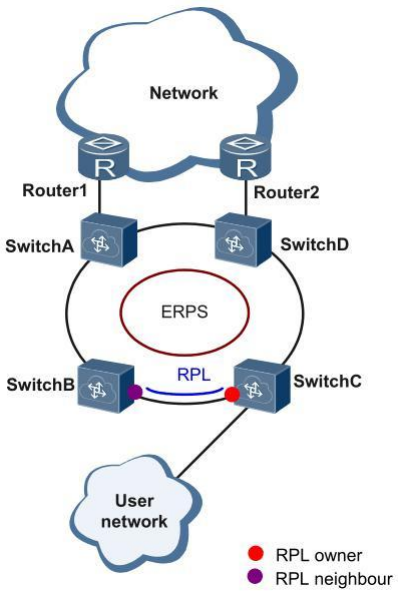
Figure 3-12 VLAN interface

3.2 ERPS

3.2.1 ERPS Function Overview

ERPS (Ethernet Ring Protection Switching protocol) is a network Protection protocol developed for the ITU, also known as g.8032.It is a link layer protocol for Ethernet ring networks. It can prevent broadcast storms caused by the data loop when the Ethernet is complete and quickly restore communication between the nodes of the Ethernet when one link is disconnected. At present, STP is another technology to solve the problem of two-layer network loop. STP is more mature, but its convergence time is longer (second level). ERPS is a link-layer protocol specially used in Ethernet ring networks. The two-layer convergence performance is up to 50ms, which has a faster convergence rate than STP.

Figure 3-13 typical ERPS networking



3.2.2 Introduction to ERPS Principle

ERPS is a standard ring network protocol dedicated to Ethernet link layer.Only two ports can join the same ERPS ring on each layer switching device.In an ERPS ring, to prevent a loop from appearing, you can start a loop breaking mechanism that blocks the RPL owner port and eliminates the loop.When link failure occurs in the ring network, the equipment running ERPS protocol can

quickly release blocking ports, perform link protection switching, and restore link communication between nodes in the ring network.This section mainly introduces the basic implementation principle of ERPS under single-ring networking in the form of example according to the process of link normal-> link fault-> link recovery (including protection switching operation).

3.2.2.1 Normal Links

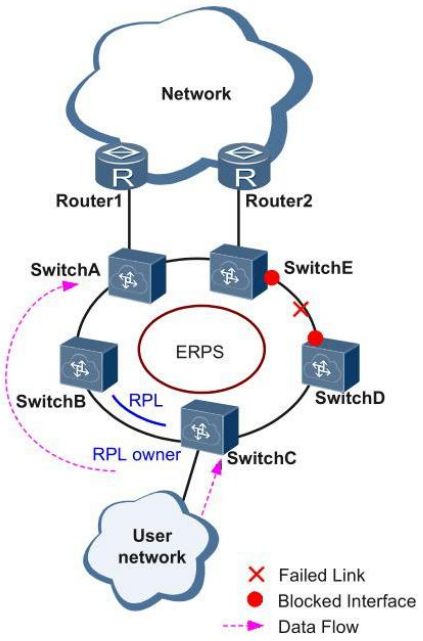
As shown in figure 3-14, all devices on the Switch A ~ Switch E circuit communicatenormally.

FIG. 3-14 normal ERPS link

To prevent loop generation, ERPS first blocks the RPL owner port, which is also blocked if the RPL neighbor port is configured, so that other ports can normally forward traffic.

3.2.2.2 Link Fault

As shown in figure 3-15, when the link between Switch D and Switch E fails, the ERPS protocol starts the protection switching mechanism, blocks the ports at both ends of the fault link, and then releases the RPL owner port. The two ports resume the receiving and sending of user traffic, thus ensuring the uninterrupted traffic.
Figure 3-15 ERPS link failure



3.2.2.3 Link Recovery

When the link returns to normal, ERPS rings are configured with a backcut mode by default, and the device that owns the RPL owner port re-blocks traffic on the RPL link, and the original fault link is reused to complete the transfer of user traffic.

3.2.2.4 ERPS Ring Types

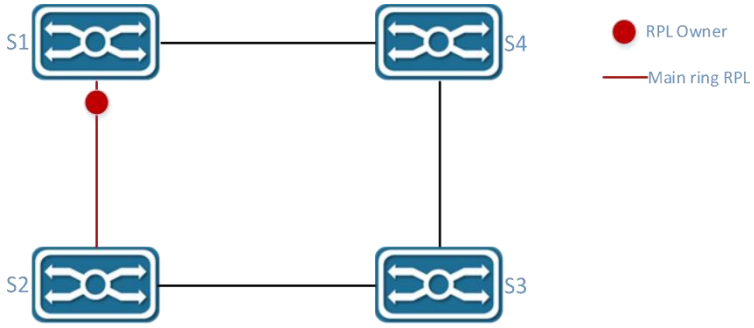
Single Ring:

For example, in figure 3-16, there is only one ring in the network topology; only one RPL Owner; only one RPL link;

All nodes need to have the same RAPS managed VLAN

- All devices in the ring need to support ERPS.
- Links between devices in the ring network must be directly connected, without intermediate equipment.

Figure 3-16 ERPS single-loop model

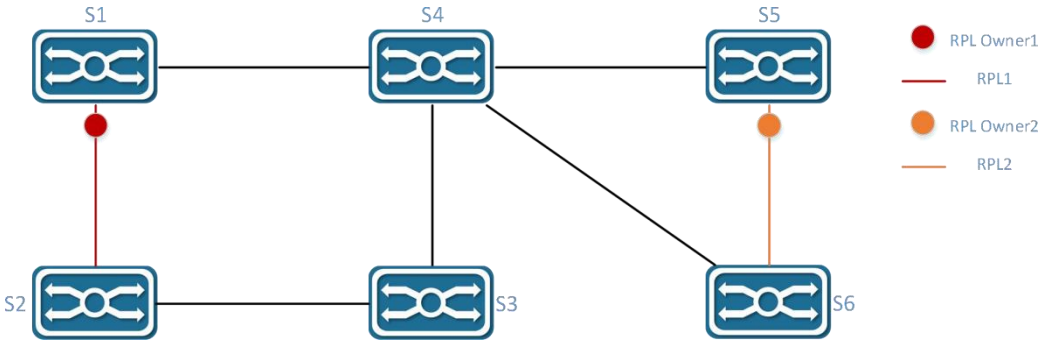


Tangent Ring:

An application scenario in which two or more rings sharing a single device in a network topology needs protection.For example, in figure 3-17, two rings in the network topology share one device.Each ring has one and only one blocking point, and each ring has one and only one RPL link.Different rings need to have different RAPS management VLANs.

- All devices in the ring need to support ERPS.
- Links between devices in the ring network must be directly connected, without intermediate equipment.

FIG. 3-17 ERPS tangential ring model

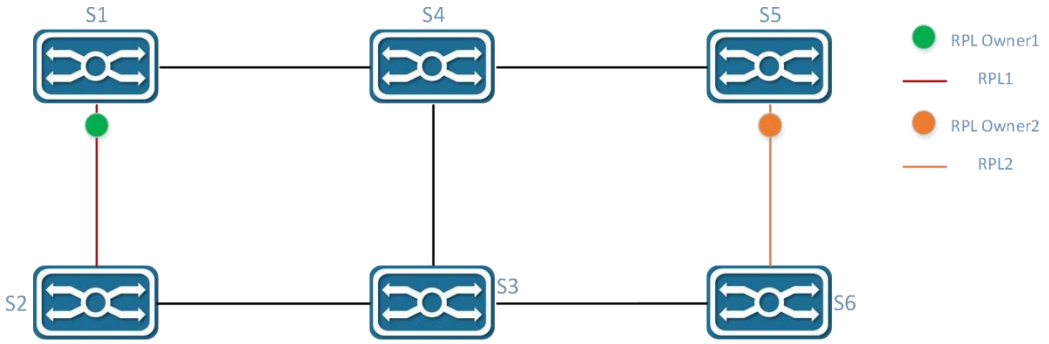


Intersecting Rngs:

In a network topology, two or more rings share a link (the two intersecting nodes must be directly connected, and no other nodes are allowed).Take figure 3-18 as an example, there are two rings in the network topology.Each ring has one RPL owner node and each ring has one RPL link.Different rings need to have different RAPS management VLANs.

- All devices in the ring need to support ERPS。
- Links between devices in the ring network must be directly connected, without intermediate equipment。

Figure 3-18 ERPS intersecting ring model



3.2.3 ERPS configuration profile

note

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

3.2.3.1 ERPS Management Interface

Click [exchange] -> [ERPS] in the menu to enter the ERPS overview interface, as shown in figure 3-19, and the specific description of parameter information is shown in table 3-8.

Figure 3-19 ERPS overview interface

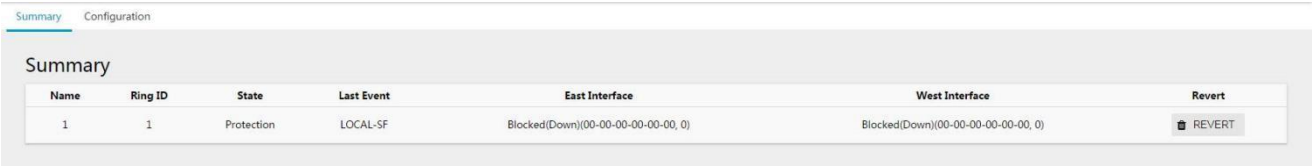


Table 3-7 description of ring configuration parameters

Configuration Item	instructions
Naming	The name of the ERPS ring
Ring Number	Number of ERPS rings
State	The current state of the ERPS ring, including: Idle: idle state, no fault, cutback already Pending: no fault Pending Pending backcut Protection: failure condition Protection
	Recent state machine events, including: RAPS-NR: remote fault recovery event RAPS-NR-RB: remote backcut event RAPS-SF: remote fault event

Previous Event	LOCAL-SF: LOCAL fault event LOCAL-CLEAR-SF: local fault recovery event WTR-EXP: local callback event
East interface	Eastward interface of ERPS ring
West Interface	Westward interface of ERPS ring
Cut Back	When the fault link resumes, you can choose to manually cut back immediately, otherwise the system will automatically cut back after 5 minutes

3.2.3.2 ERPS Ring Configuration

In the ERPS interface, click the "configure" button in the upper left corner to enter the ERPS ring configuration interface. Click the "add" button to add ERPS ring. After the configuration is completed, click the "apply" button, as shown in FIG. 3-20.

Figure 3-20 ERPS ring configuration

Table 3-8 configuration parameters

Configuration Items	instructions	
Ring number	ERPS ring ID, which can be any number.Each ERPS ring must have a unique ring number.	
East interface	Specifies that a port on the switch is an eastbound port	East port and west port are relatively defined, without strict distinction, that is, the loop can enter and exit at this point.
West interface	Specifies that a port on the switch is a westbound port	

After the configuration is completed, return to the ERPS ring configuration interface. Click the "delete" button after the ring entry to delete the ERPS ring, as shown in figure 3-21.

Figure 3-21 ERPS ring configuration

3.2.3.3 ERPS Instance Configuration

Click the "+ add" button of ERPS instance configuration to enter the interface. After the configuration is completed, click the "apply" button, as shown in figure 3-22. Specific parameters of the instance configuration are described in table 3-9.

Figure 3-22 ERPS instance configuration

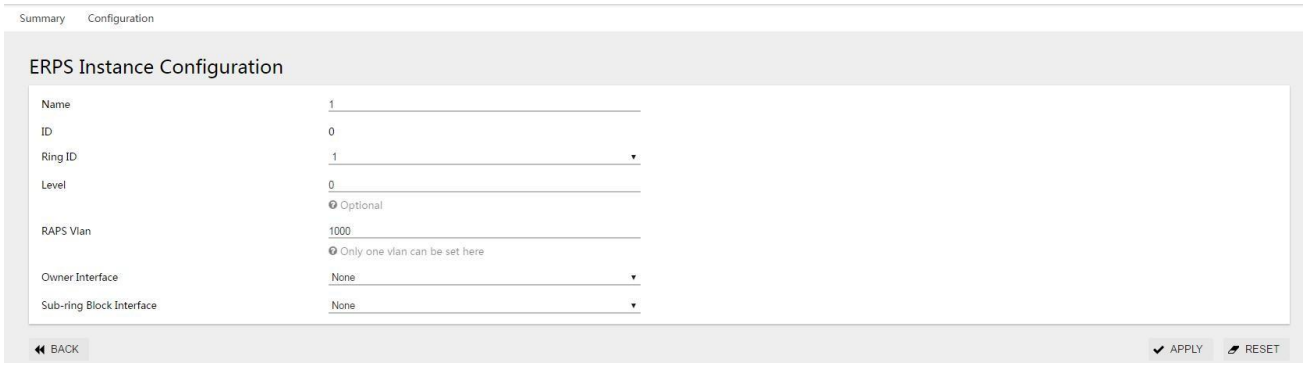


Table 3-9 RingConfiguration Parameters

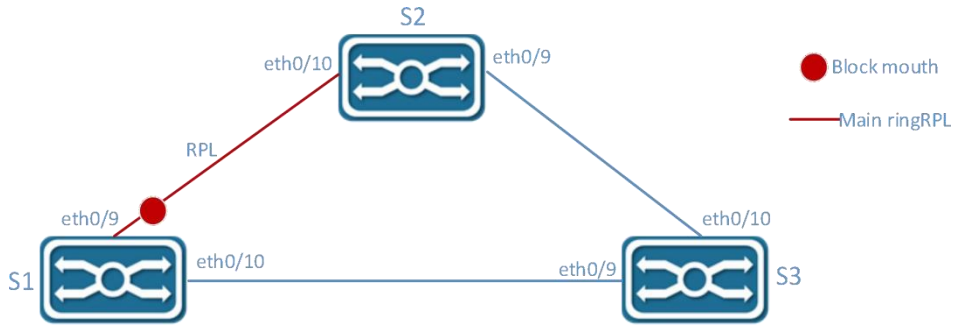
Configuration items	instructions
Naming	Instance names, string format, need to be unique, such as number "1", character "aa"
ID	Configure VLAN Instance for ERPS Instance protection; All vlans belong to Instance 0 by default; The default id is 0.
Ring Number	The associated ring ID must be the ring already created
Level	ERPS priority, default is 0
RAPS Management VLAN	Each switch in the same ring must be configured with the same RAPS management VLAN for transmitting ERPS protocol messages. A RAPS management VLAN can be a virtual VLAN, requiring a distinction from a data VLAN, without the need for actual creation.
Data VLAN	ERPS data vlans, setting up the vlans that are allowed to transfer in the ERPS ring.Must be an existing VLAN if Does not exist please add in VLAN configuration; Support VLAN Range class configuration, such as "1-3,5" for VLAN 1,2,3,5;
The Owner Interface	Main ring ERPS Owner node, can choose east interface or west interface as Owner node. Each ERPS ring has only one device configured as an RPL owner node that controls the end that needs to be blocked
Sub - Ring Blocking Mouth	Sub - ring blocking mouth, a sub - ring only a blocking mouth, you can choose east or west. This parameter needs to be configured only when the ring is tangential, and the sub-ring of the two devices whose rings are tangential must have a sub-ring blocking port.
Associated Instance	Only need to configure the sub-ring blocking port, set to the ring ID tangent to the current sub-ring

3.2.4 Examples of Single Ring Configuration

Case requirements:

A ring network with 3 switches, as shown in Figure 3-21, the default blocking port is configured to be the eth0/9 port of S1. When a failure occurs, the link can be restored in time to ensure that the network is available. The data VLAN is 1, 2, 3.

Figure 3-23 ERPS network topology

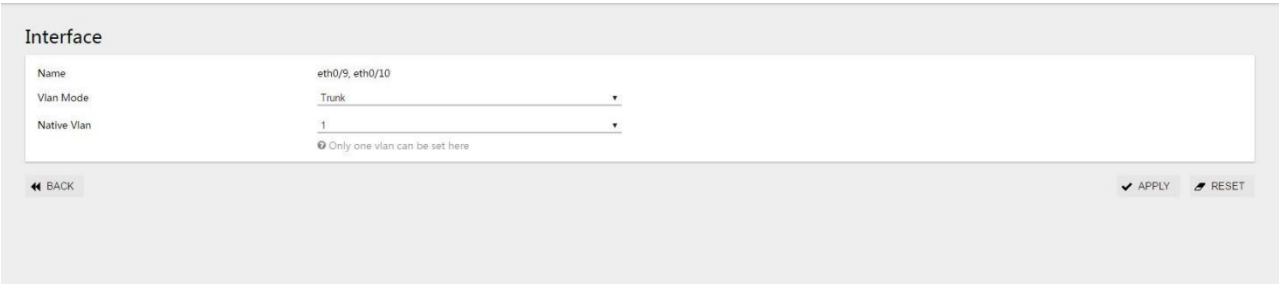


3.2.4.1 Configure Switch S1

Step 1: configure ports 9 and 10 for trunk ports and Native Vlan for default value 1.

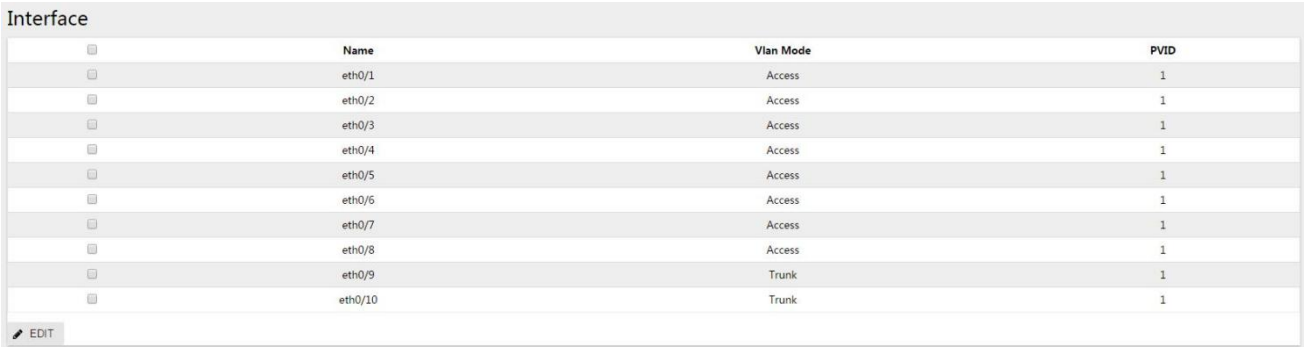
Select [VLAN] from the sub-item of [switch] in the menu to enter the interface configuration interface, select ports eth0/9 and eth0/10, and click the [edit] button to enter the configuration mode, as shown in figure 3-24.Select "Trunk" for VLAN mode, Native VLAN defaults to "1".

Figure 3-24 port configuration interface



Click the "apply" button, and the interface returned is shown in figure 3-25.

Figure 3-25 port status display interface



Step 2: create VLAN 2, 3, 4 and add VLAN 2, 3, 4 to Trunk ports eth0/9, eth0/10.

In the VLAN interface, as shown in Figure 3-26, click the [Add] button, enter "2-4" in the ID, and check eth0/9 and eth0/10 for the Tagged member port

Figure 3-36 create VLAN 2, 3, and 4

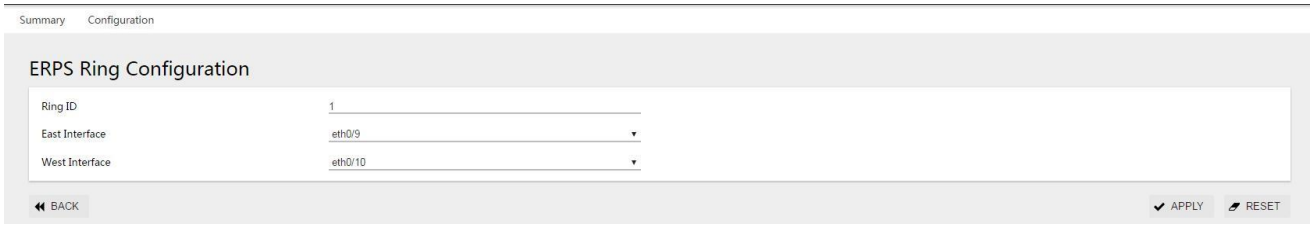
Click the "apply" button, and the interface returned is shown in figure 3-27.

Figure 3-27 port status display interface

Step 3: Create ERPS ring ID, set east-west interface.

Select [ERPS] in the menu [exchange] and enter the ERPS configuration interface. Click the button [+ add] to enter the ERPS ring configuration interface, as shown in figure 3-28.The ring number is set to "1", the east interface to "eth0/9", and the west interface to "eth0/10".

Figure 3-28 ERPS ring configuration interface

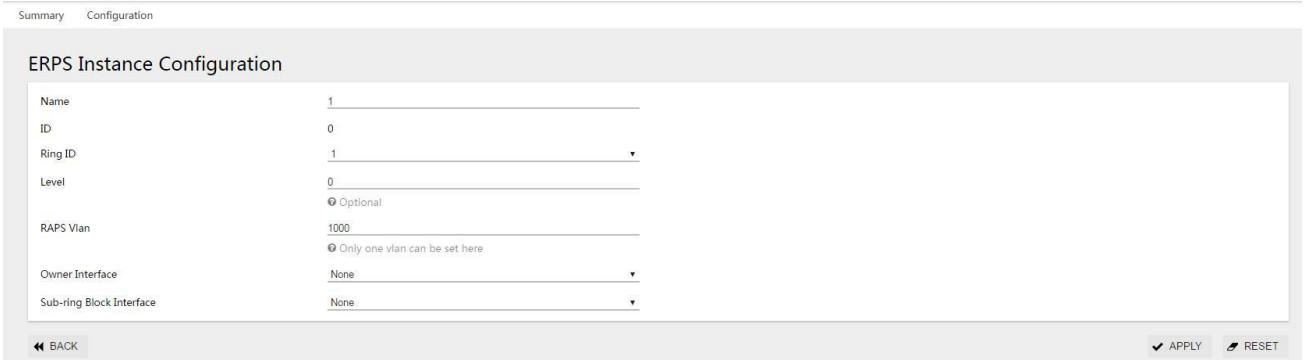


Click the "apply" button to return to the following page, as shown in picture 3-29.

Figure 3-29 ERPS ring configuration display interface

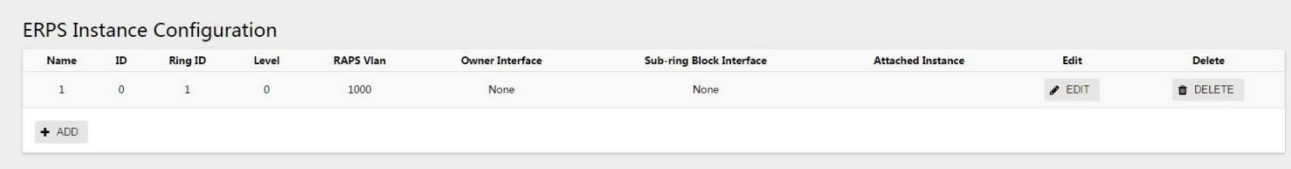
Step 4: create an ERPS instance and set the ring name, number, blocking port and other parameters.
In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface, as shown in figure 3-30.Name "1", ring number "1", level "0", RAPS management VLAN "1000", Owner interface "East", sub ring blocking port "None".

Figure 3-30 ERPS instance configuration interface



Click the "apply" button to return to the following page:

Figure 3-31 ERPS instance configuration display interface



Step 5: select the "save" button on the navigation bar and save the configuration.

instructions

- In the case of single ring, only one blocking point needs to be set, and the choice of blocking point is generally considered in the middle of the ring.

3.2.4.2 Configure Switch S2 and S3

Step 1: configure ports 9 and 10 for trunk and Native Vlan for default value 1.

Select [VLAN] in the menu [switch] to enter the interface configuration interface, select ports "eth0/9" and "eth0/10", click the "edit" button to enter the configuration mode, as shown in the figure.Select "Trunk" for VLAN mode, Native VLAN defaults to "1".

Step 2: Create VLAN 2, VLAN 3, and add VLAN 2 and VLAN 3 to Trunk ports eth0/9 and eth0/10.

In the VLAN interface, click the [Add] button, enter "2-3" in the ID, and check eth0/9 and eth0/10 for the tagged member ports.

Step 3: create the ERPS ring and set up the thing interface.

Select [ERPS] in the menu [exchange] and enter the ERPS configuration interface. Click the button [+ add] to enter the ERPS ring configuration interface, as shown in figure 3-27.The ring number is set to "1", the eastern interface to "eth0/9", and the western interface to "eth0/10".

Step 4: create an ERPS instance.

In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface, as shown in figure 3-32.Name "1", ring number "1", level "0", RAPS management VLAN "1000", Owner interface "None", sub ring blocking port "None".Figure 3-32 ERPS instance configuration display interface

instructions

Unlike S1, S2 and S3 are in the break point Owner interface =None.

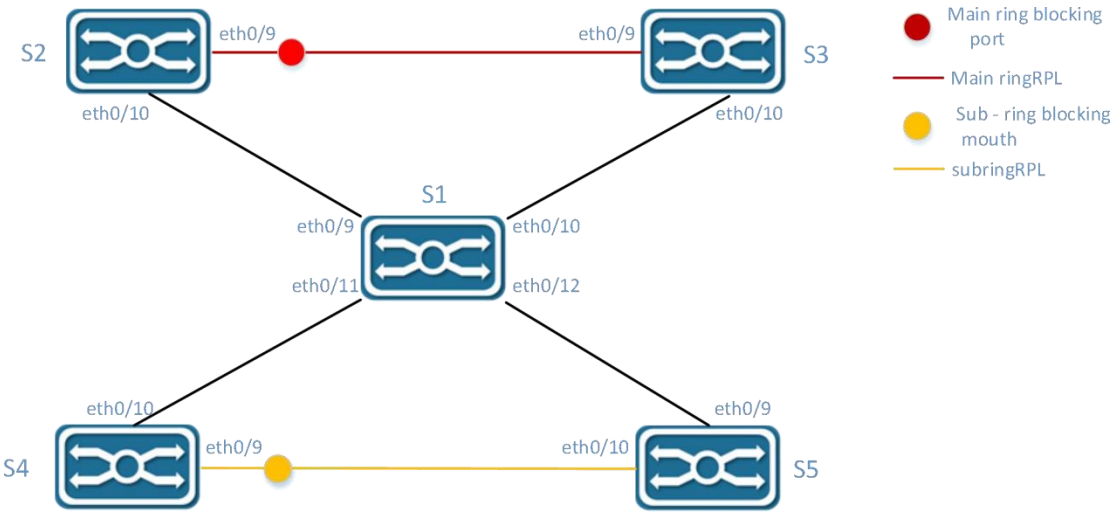
Step 5: select the "save" button on the navigation bar and save the configuration.

3.2.5 Examples of Tangential Ring Configuration

The topology diagram is shown in Figure 3-33. S1 is located in the central computer room and can be supervised and maintained by the administrator in real time. It has high reliability; S2-S5 is distributed in various deployment points. In order to improve the reliability of the network, avoid single The single-point failure risk of the link external connection, while avoiding the single-machine failure risk that may occur when the dual-link external single-machine

is connected, the dual-link external connection forms a ring network. The data VLANs are 1, 2, 3, and 4, and each ring network is required to converge quickly when a single point of failure occurs to avoid user network interruption.

Figure 3-33 network topology



3.2.5.1 Divide Main Ring and Sub-Ring

instructions

- The ring ID of the primary and subring must be different.
- The RAPS management VLANs within the primary and subring must be different.

There is no strict distinction between the main ring and the sub-ring. Generally once one of the main rings is assumed, and the other is a sub-ring.In this example, the ring composed of S1, S2 and S3 is defined as the main ring, the ring number is "1", the blocking port is "eth0/9" of S2, the RAPS management VLAN is "1000", the ring composed of S1, S4 and S5 is a sub-ring, the ring number is "2", the blocking port is "eth0/9" of S4, and the RAPS management VLAN is "1001", the specific parameters are shown in table 3-10.

Table 3-10 equipment parameters chart

parameter equipment	Ring number	RAPS VLAN	The Owner interface	Sub-ring blocking mouth	Associated instance
Switch S2	1	1000	Eth0/9	None	\
Switches S3	1	1000	None	None	\
Switch S1	1	1000	None	None	\
	2	1001	None	None	\
Switches S4	2	1001	Eth0/9	None	\
Switch the S5	2	1001	None	None	\

3.2.5.2 Configure Switch S1

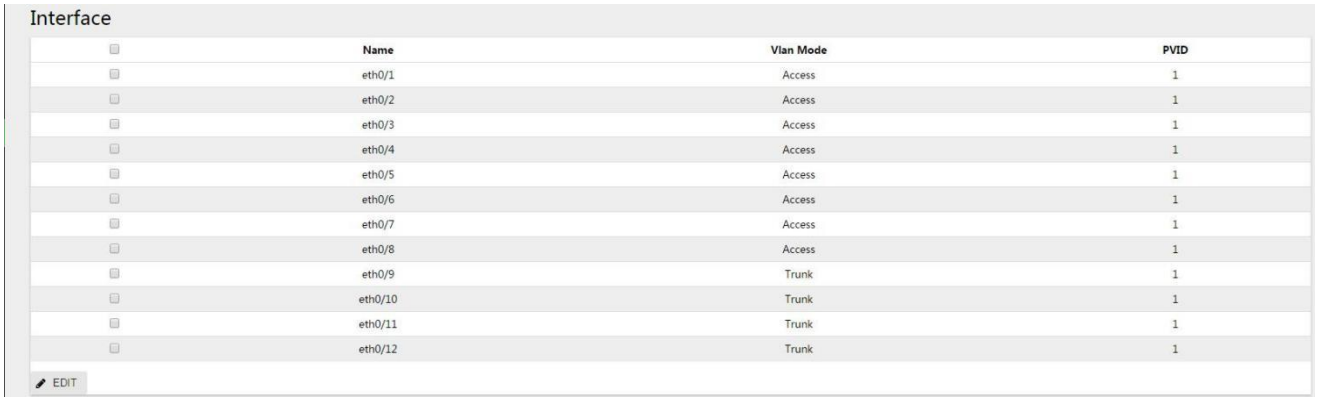
Step 1: configure ports 9, 10, 11, 12 as trunk ports and Native Vlan as default value 1.

Select [VLAN] from the sub-item of [switch] in the menu to enter the VLAN configuration interface. In the interface configuration item, select ports eth0/9, eth0/10, eth0/11, eth0/12, and click the edit button to enter the configuration mode, as shown in figure 3-34.Select "Trunk" for VLAN mode, Native VLAN defaults to "1".

Figure 3-34 port configuration interface

Click the "apply" button, and the interface interface returned is shown in figure 3-35.

Figure 3-35 port status display interface



Step 2: create VLAN 2, 3, 4 and add VLAN 2, 3, 4 to Trunk ports eth0/9, eth0/10, eth0/11,and eth0/12.

Tagged member ports are Tagged with eth0/9, eth0/10, eth0/11, and eth0/12.

Figure 3-36 create VLAN 2, 3, and 4

Click the "apply" button, and the interface returned is shown in figure 3-37.

Figure 3-37 port status display interface

Step 3: create the ERPS main ring and subring and set up the east-west interface.

(1) Create the main ring

Select [ERPS] in the menu [exchange] and enter the ERPS configuration interface. Click the button [+ add] to enter the ERPS ring configuration interface, as shown in figure 3-38.The ring number is set to "1", the eastern interface to "eth0/9", and the western interface to "eth0/10".

Step 3: create the ERPS main ring and subring and set up the east-west interface

(2) Create the main ring

Select [ERPS] in the menu [exchange] and enter the ERPS configuration interface. Click the button [+ add] to enter the ERPS ring configuration interface, as shown in figure 3-38.The ring number is set to "1", the eastern interface to "eth0/9", and the western interface to "eth0/10".

Figure 3-38 creates the ERPS main ring

(3) Create subrings

Select [ERPS] in the menu [exchange] and enter the ERPS configuration interface. Click the button [+ add] to enter the ERPS ring configuration interface, as shown in figure 3-39.The ring number is set to "2", the eastern interface to "eth0/11", and the western interface to "eth0/12".

Figure 3-39 creates an ERPS subring

Click the "apply" button to return to the following page:

Figure 3-40 ERPS ring configuration display interface

Step 4: create an ERPS instance

(1) Create ERPS instance 1

In the ERPS interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface, as shown in figure 3-41.Name "1", ring number "1", level "0", RAPS management VLAN "1000", Owner interface "None", sub ring blocking port "None".

Figure 3-41 ERPS instance configuration interface

(2) Create ERPS instance 2

In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface, as shown in figure 3-42.Name "2", ring number "2", level "0", RAPS management VLAN "1001", Owner interface "None", sub ring blocking port "None".

Figure 3-42 ERPS instance configuration interface

Click the "apply" button to return to the following page, as shown in picture 3-43:

Figure 3-43 ERPS instance configuration display interface

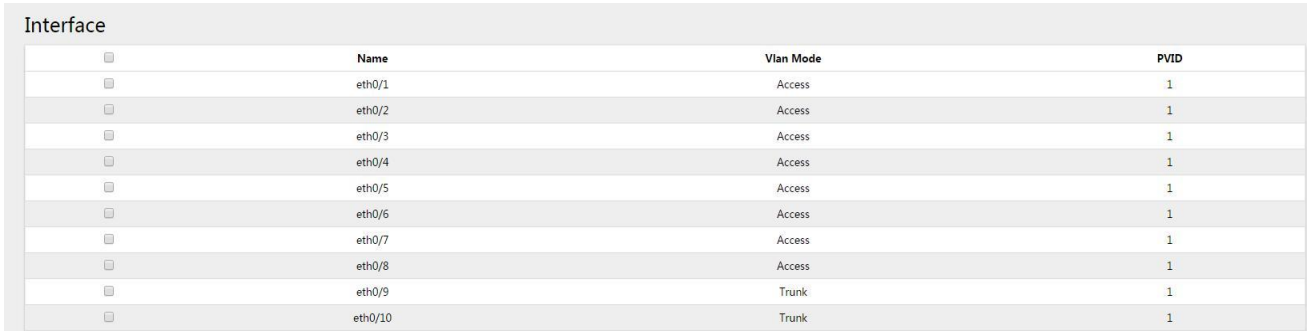
Step 5: select the "save" button on the navigation bar and save the configuration.

3.2.5.3 Configure switch S2

Step 1: configure ports 9 and 10 as trunk ports and Native Vlan as default value 1.

Select [VLAN] in the [Switch] sub-item of the navigation bar to enter the VLAN configuration interface. In the interface configuration item, select ports eth0/9, eth0/10, and click the [Edit] button to enter the configuration mode, as shown in the figure. Select "Trunk" for VLAN mode, and Native Vlan defaults to "1". Click the [Apply] button, and the returned interface interface is shown in Figure 3-44.

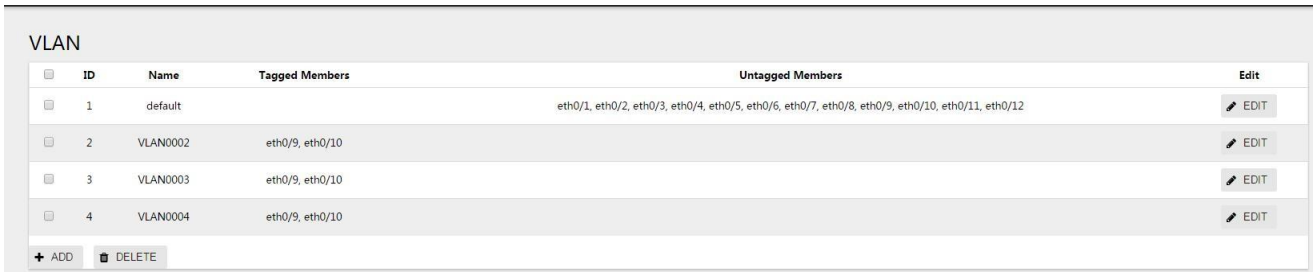
Figure 3-44 port status display interface



Step 2: create VLAN 2, VLAN 3, and VLAN 4, and add VLAN 2, 3, and 4 to Trunk eth0/9 and eth0/10.

Under the VLAN option, click the "add" button, enter "2-4" in the ID, Tagged member port, and tick eth0/9 and eth0/10.Click the "apply" button, and the interface returned is shown in figure 3-45.

Figure 3-45 port status display interface.



Step 3: Create the ERPS ring and set up the thing interface.

Select "ERPS" from the "switch" sub-item in the menu and enter the ERPS configuration interface. Click "+ add" button to enter the ERPS ring configuration interface.The ring number is set to "1", the eastern interface to "eth0/9", and the western interface to "eth0/10".Click the "apply" button, and the return page is shown in figure 3-46:

Figure 3-46 ERPS ring configuration display interface

Step 4: Create an ERPS instance and set up the blocking port.

In the ERPS configuration interface, select the instance configuration and click the "+ add" button to enter the ERPS instance configuration interface. The name is "1", ring number "1", level "0", RAPS management VLAN "1000", Owner interface "East", and sub ring blocking port is "None".Click the "apply" button to return to the page as shown in figure 3-47:

Figure 3-47 ERPS instance configuration display interface

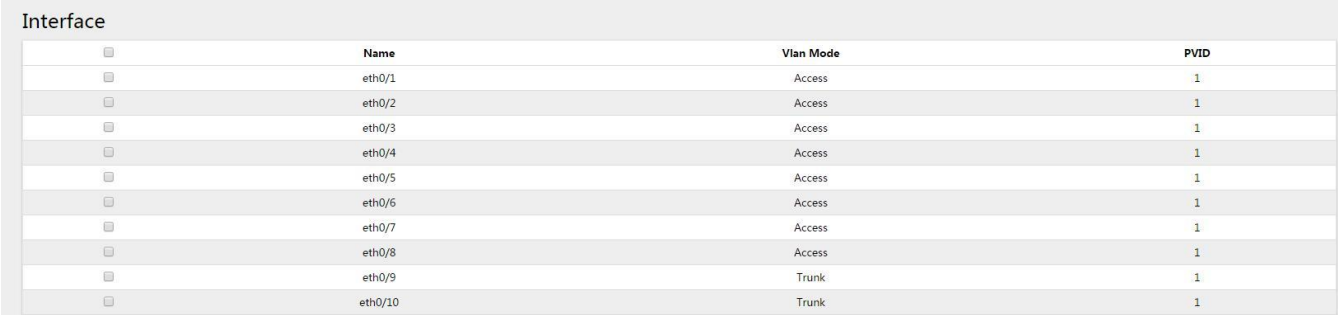
Step 5: select the "save" button on the navigation bar and save the configuration.

3.2.5.4 Configure Switch S3

Step 1: configure ports 9 and 10 as trunk ports and Native Vlan as default value 1.

Select [VLAN] from the sub-item of [switch] in the menu to enter the port configuration interface, select ports eth0/9 and eth0/10, and click the button of [edit] to enter the configuration mode.Select "Trunk" for VLAN mode, Native VLAN defaults to "1".Click the "apply" button, and the interface returned is shown in figure 3-48.

Figure 3-48 port status display interface



Step 2: create VLAN 2, VLAN 3, and VLAN 4, and add VLAN 2, 3, and 4 to Trunk eth0/9 and eth0/10.

Under the VLAN interface, click the "add" button, enter "2-4" in the ID, Tagged member port and tick eth0/9 and eth0/10.Click the "apply" button, and the interface interface returned is shown in figure3-49.

Figure 3-49 port status display interface

Step 3: create the ERPS ring and set up the east-west interface.

Select "ERPS" from the "switch" sub-item in the menu and enter the ERPS configuration interface. Click "+ add" button to enter the ERPS ring configuration interface.The ring number is set to "1", the eastern interface to "eth0/9", and the western interface to "eth0/10".Click the "apply" button to return to the page as shown in figure 3-50:

Figure 3-50 ERPS ring configuration display interface

Step 4: create an ERPS instance and set up the blocking port.

In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface.Set the name "1", ring number "1", level "0", RAPS management VLAN "1000", Owner interface "None", sub ring blocking port "None".Click the "apply" button to return to the page as shown in figure 3-51:

Figure 3-51 ERPS instance configuration display interface

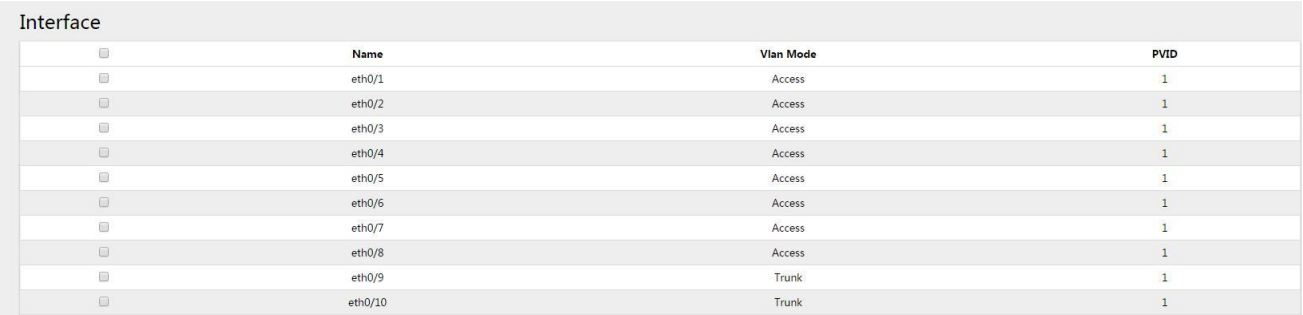
Step 5: select the "save" button on the navigation bar and save the configuration.

3.2.5.5 Configure Switch S4

Step 1: configure ports 9 and 10 as trunk ports and Native Vlan as default value 1.

Select [VLAN] from the sub-item of [switch] in the menu to enter the interface configuration interface, select ports eth0/9 and eth0/10, and click the button of [edit] to enter the configuration mode.Select "Trunk" for VLAN mode, Native VLAN defaults to "1".Click the "apply" button, and the interface returned is shown in figure 3-52.

Figure 3-52 port status display interface



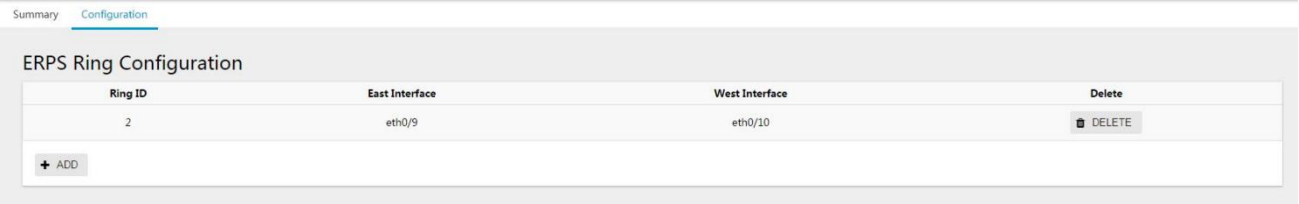
Step 2: create VLAN 2, VLAN 3, and VLAN 4, and add VLAN 2, 3, and 4 to Trunk eth0/9 and eth0/10. Under the VLAN interface, click the "add" button, enter "2-4" in the ID, Tagged member port and tick eth0/9 and eth0/10.Click the "apply" button, and the interface interface returned is shown in figure 3-53.

Figure 3-53 port status display interface

Step 3: create the ERPS ring and set up the east-west interface.

Select [ERPS] in the menu [exchange] and enter the ERPS configuration interface. Click the button [+ add] to enter the ERPS ring configuration interface, as shown in figure 3-54.The ring number is set to "2", the eastern interface to "eth0/9" and the western interface to "eth0/10".Click the "apply" button to return to the following page:

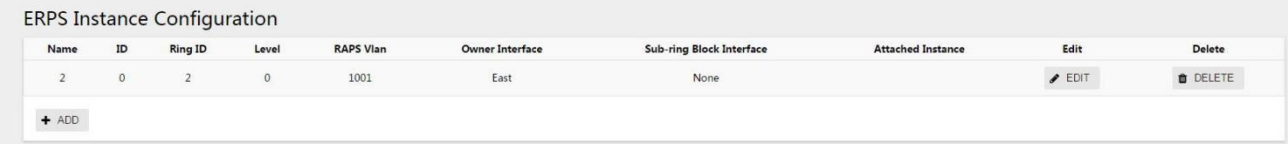
Figure 3-54 ERPS ring configuration display interface



Step 4: create an ERPS instance and set up the blocking port.

In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface, as shown in figure 3-55.Name "2", ring number "2", level "0", RAPS management VLAN "1001", Owner interface "East", sub ring blocking port "None".
Click the "apply" button to return to the following page:

Figure 3-55 ERPS instance configuration display interface



Step 5: select the "save" button on the navigation bar and save the configuration.

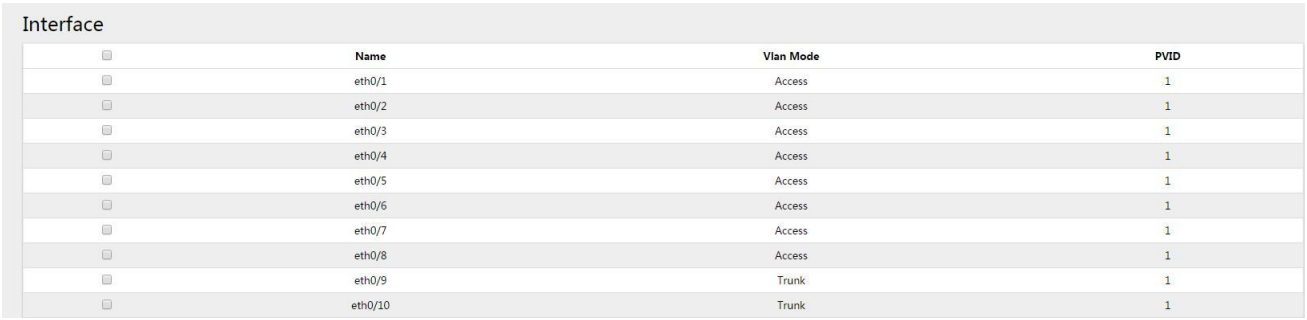
3.2.5.6 Configure Switch S5

Step 1: configure ports 9 and 10 as trunk ports and Native Vlan as default value 1.

Select [VLAN] in the menu [switch] to enter the interface configuration interface, select ports eth0/9 and eth0/10,

click the button [edit] to enter the configuration mode, as shown in the figure.Select "Trunk" for VLAN mode, Native VLAN defaults to "1".Click the "apply" button, and the interface returned is shown in figure 3-56.

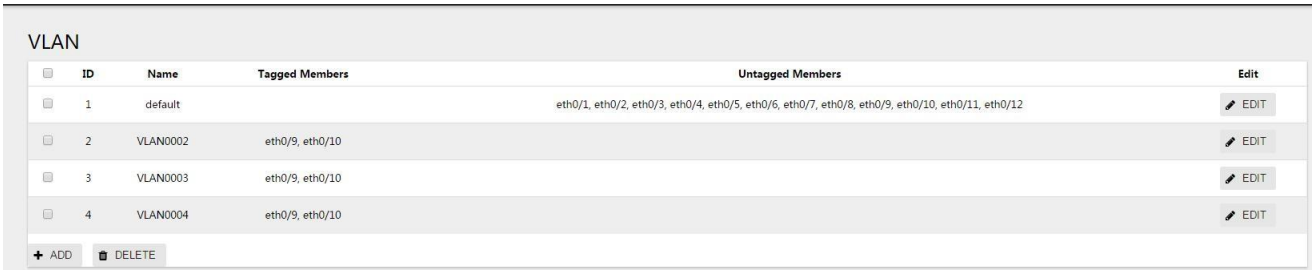
Figure 3-56 port status display interface



Step 2: create VLAN 2, VLAN 3, and VLAN 4, and add VLAN 2, 3, and 4 to Trunk eth0/9 and eth0/10.

Under the VLAN interface, click the "add" button, enter "2-4" in the ID, Tagged member port and tick eth0/9 and eth0/10.Click the "apply" button, and the interface returned is shown in figure 3-57.

Figure 3-57 port status display interface



Step 3: create the ERPS ring and set up the east-west interface.

Select [ERPS] in the menu [exchange] and enter the ERPS configuration interface. Click the button [+ add] to enter the ERPS ring configuration interface, as shown in figure 3-58.The ring number is set to "2", the eastern interface to "eth0/9" and the western interface to "eth0/10".Click the "apply" button to return to the following page:

Figure 3-58 ERPS ring configuration display interface

Step 4: create an ERPS instance and set up the blocking port.

In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface, as shown in figure 3-57.Name "2", ring number "2", level "0", RAPS management VLAN "1001", Owner interface "None", sub ring blocking port "None".
Click the "apply" button to return to the following page, as shown in picture 3-59:

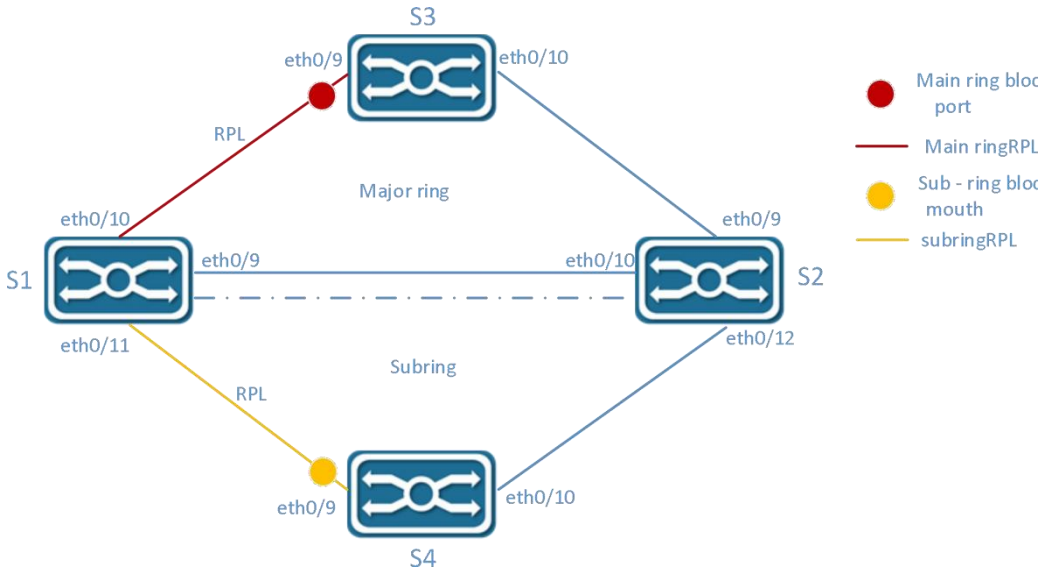
Figure 3-59 ERPS instance configuration display interface

Step 5: select the "save" button on the navigation bar and save the configuration.

3.2.6 Intersecting Ring Configuration Example

As shown in Figure 3-60, S1, S2, S3, and S4 form an intersecting ring, and the data vlan is 1, 2, 3, and 4. It is required that rapid convergence can be achieved when a single point of failure occurs in each ring; the network can at most have two failure points (different rings) without user disconnection, achieving optimal reliability.

Figure 3-60 ERPS intersecting ring



3.2.6.1 Divide Main Ring and Sub-Ring

instructions

- The ring ID of the primary and subring must be different.
- The RAPS management VLAN within the primary and subring must be different
- In the sub-ring, the port corresponding to the link where the main ring intersects with the sub-ring must be set as the blocking port, and the associated instance is set as the main ring.

There is no strict distinction between the main ring and the sub-ring. Generally one of the main rings is assumed, and the other is a sub-ring.In this example, the ring composed of S1, S2 and S3 is defined as the main ring, the ring number is "1", the blocking point is S3 eth0/9 port, and the RAPS management VLAN is "1000".The ring composed of S1, S2 and S4 is a sub-ring, the ring number is "2", the breaking point is eth0/9 port of S4, the RAPS management VLAN is "1001", and the intersecting link of the two rings is eth0/9 of S1 to eth0/10 of S2.Specific parameters are described in table 3-11.

Table 3-11 equipment parameters list

parameter equipment	Ring number	RAPS VLAN	The Owner interface	Sub-ring blocking mouth	Associated instance
Switch S1	1	1000	None	None	\
	2	1001	None	Eth0/9	1
Switch S2	1	1000	None	None	\
	2	1001	None	Eth0/10	1
Switches S3	1	1000	Eth0/9	None	\
Switches S4	2	1001	Eth0/9	None	\

3.2.6.2 Configure Switch S1

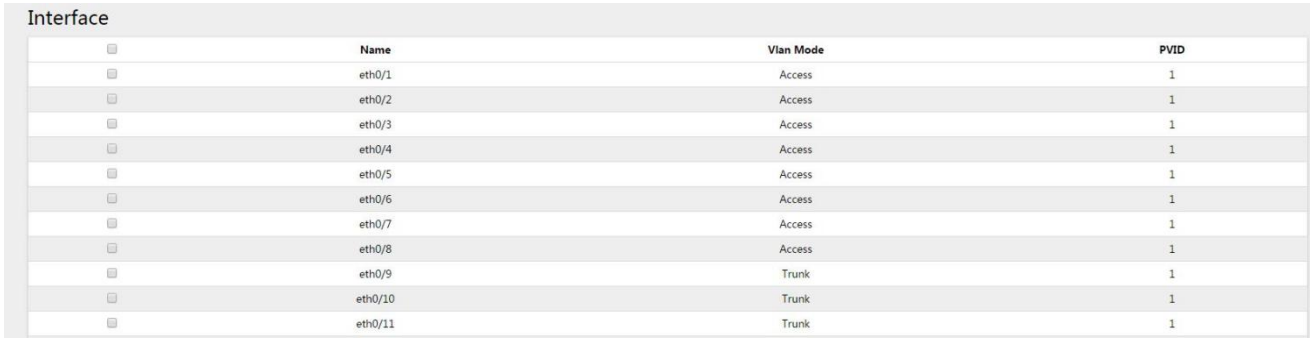
Step 1: Configure ports 9, 10 and 11 as trunk ports and Native Vlan as default value 1.

Select [VLAN] from the sub-item of [switch] in the menu to enter the VLAN configuration interface. Under the interface configuration option, check ports eth0/9, eth0/10 and eth0/11, and click the edit button to enter the configuration mode, as shown in figure 3-61.Select "Trunk" for VLAN mode, Native VLAN defaults to "1".

Figure 3-61 port configuration interface

Click the "apply" button, and the interface interface is shown in figure 3-62.

Figure 3-62 port status display interface



Step 2: Create VLAN 2, VLAN 3, and VLAN 4, and add VLAN 2, 3, and 4 to Trunk ports eth0/9, eth0/10, and eth0/11.
In the VLAN interface, click the [Add] button, enter "2-4" in the ID, and select eth0/9, eth0/10, and eth0/11 for the tagged member ports.

Figure 3-63 create VLAN 2, 3, and 4

Click the "apply" button, and the interface returned is shown in figure 3-64.

Figure 3-64 VLAN state display interface

Step 3: Create the ERPS main ring and subring and set up the thing interface.

(1) Create the main ring

Select [ERPS] in the menu [exchange] and enter the ERPS configuration interface. Click the button [+ add] to enter the ERPS ring configuration interface, as shown in figure 3-65.The ring number is set to "1", the eastern interface to "eth0/9", and the western interface to "eth0/10".

Figure 3-65 ERPS ring configuration interface

(2) Create subrings

Select "ERPS" from the "switch" sub-item in the menu and enter the ERPS configuration interface. Click "+ add" button to enter the ERPS ring configuration interface, as shown in figure 3-66.The ring number is set to "2", the eastern interface to "eth0/9", and the western interface to "eth0/11".Note that the eth0/9 (eastern interface) of the subring needs to be configured as a subring interrupter.

Figure 3-66 ERPS ring configuration interface

Click the "apply" button to return to the following page:

Figure 3-67 ERPS ring configuration display interface

Step 4: create an ERPS instance and set up the blocking port.

(1) create ERPS instance 1

In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface.

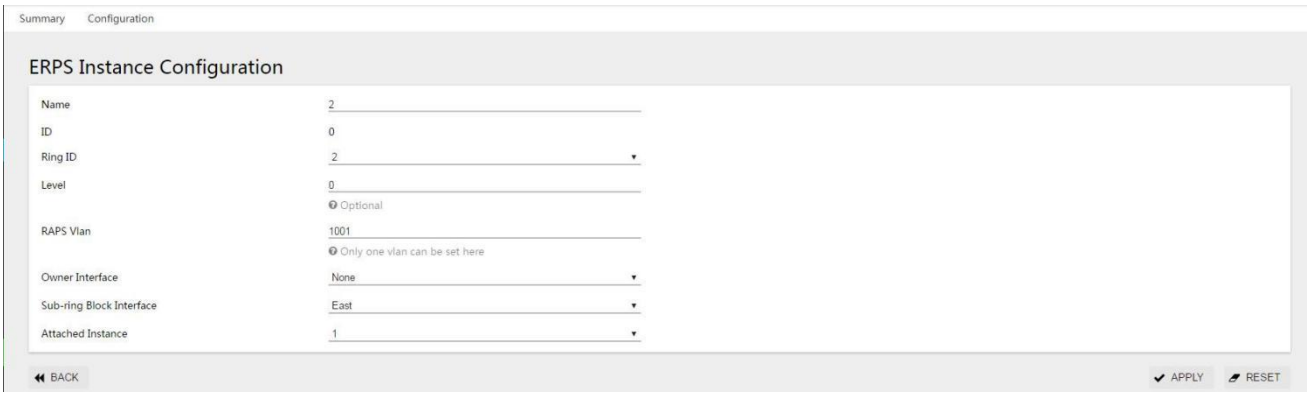
Figure 3-68 ERPS instance configuration interface

As shown in figure 3-68, name "1", ring number "1", level "0", RAPS management VLAN "1000", Owner interface "None", sub ring blocking port "None".

(2) Create ERPS instance 2

In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface, as shown in figure 3-69.Name "2", ring number "2", level "0", RAPS management VLAN "1001", Owner interface "None", sub ring blocking port "East", associated instance select "1".

Figure 3-69 ERPS instance configuration interface



Click the "apply" button to return to the following page:

Figure 3-70 ERPS instance configuration display interface

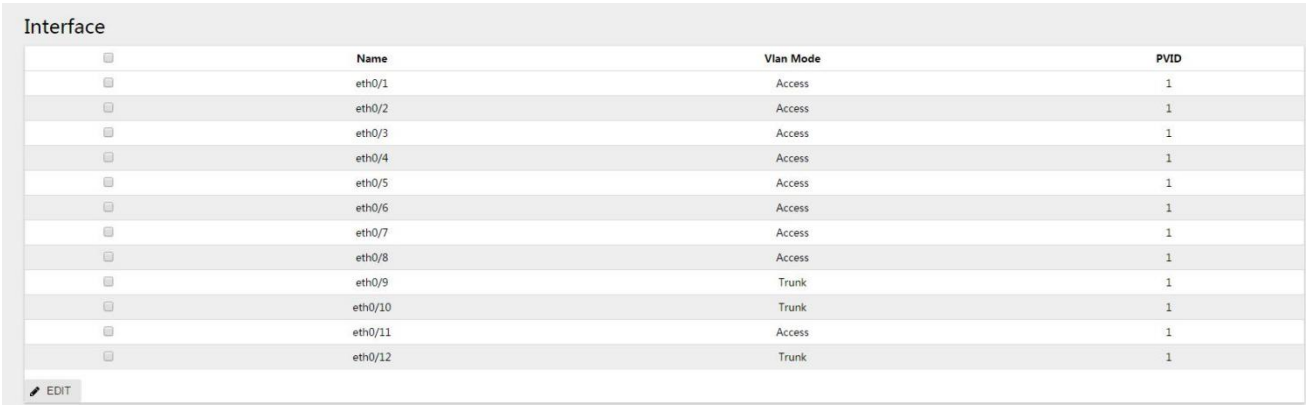
Step 5: select the "save" button on the navigation bar and save the configuration.

3.2.6.3 Configure Switch S2

Step 1: configure ports 9, 10 and 12 as Trunk ports and Native Vlan as default value 1.

Select [VLAN] from the sub-item of [switch] in the menu to enter the VLAN configuration interface. In the interface configuration options, select ports eth0/9, eth0/10, eth0/12, and click the edit button to enter the configuration mode.Select "Trunk" for VLAN mode, Native VLAN defaults to "1".Click the "apply" button, and the interface interface is shown in figure 3-71.

Figure 3-71 port status display interface



Step 2: create VLAN 2, VLAN 3, and VLAN 4, and add VLAN 2, 3, and 4 to Trunk eth0/9,eth0/10, and eth0/12.
Under the VLAN interface, click "add" button, enter "2-4" in ID, Tagged member port, tick eth0/9, eth0/10, eth0/12, and click "apply" button. The interface interface returned is shown in figure 3-72.

Figure 3-72 port status display interface

Step 3: create the main ring and sub-rings and set up the east-west interface.

(1) Create the main ring

Select [ERPS] from the [switch] subitem in the menu to enter the ERPS configuration interface. Click [+ add] button to enter the ERPS ring configuration interface. The ring number is set to "1", the eastern interface is set to "eth0/9", and the western interface is set to "eth0/10".

(2) Create subrings

Select [ERPS] in the menu [switch] and enter the ERPS configuration interface. Click [+ add] to enter the ERPS ring configuration interface. The ring number is set to "2", the eastern interface is set to "eth0/10", and the western interface is set to "eth0/12".Click the "apply" button to return to the following page:

Figure 3-73 ERPS ring configuration display interface

Step 4: create an ERPS instance and set up the blocking points.

(1) Create the main ring instance

In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface.Name "1", ring number "1", level "0", RAPS management VLAN "1000", Owner interface "None", sub ring blocking port "None".

(2) Create a sub-ring instance

In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface.Name "2", ring number "2", level "0", RAPS management VLAN "1001", Owner interface "None", sub ring blocking port "East", associated instance select "1".Click the "apply" button to return to the following page, as shown in figure 3-74:

Figure 3-74 ERPS instance configuration display interface

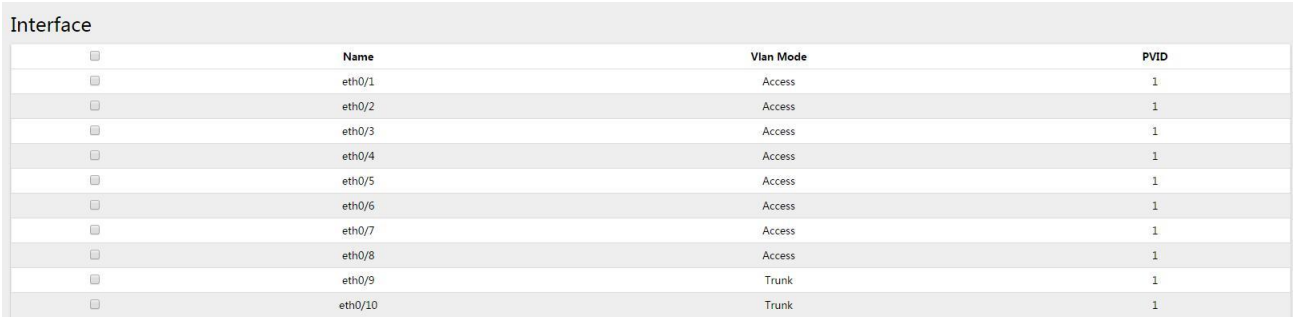
Step 5: select the "save" button on the navigation bar and save the configuration.

3.2.6.4 Configure Switch S3

Step 1: configure ports 9 and 10 as trunk ports and Native Vlan as default value 1.

Select [VLAN] from the [switch] sub-menu in the menu to enter the VLAN interface configuration interface. In the interface configuration options, select ports eth0/9 and eth0/10, and click the [edit] button to enter the configuration mode.Select "Trunk" for VLAN mode, Native VLAN defaults to "1".Click the "apply" button, and the interface interface returned is shown in figure 3-75.

Figure 3-75 VLAN state display interface



Step 2: create VLAN 2, VLAN 3, and VLAN 4, and add VLAN 2, 3, and 4 to Trunk eth0/9 and eth0/10. Under the VLAN interface, click the "add" button, enter "2-4" in the ID, Tagged member port and tick eth0/9 and eth0/10.Click the "apply" button, and the interface interface returned is shown in figure 3-76.

Figure 3-76 port status display interface

Step 3: create ERPS ring 1 and set up the thing interface.

Select "ERPS" from the "switch" sub-menu in the menu and enter the ERPS configuration interface. Click "+ add" button to enter the ERPS ring configuration interface, as shown in figure 3-77.The ring number is set to "1", the eastern interface to "eth0/9", and the western interface to "eth0/10".Click the "apply" button to return to the following page:

Figure 3-77 ERPS ring configuration display interface

Step 4: create an instance of ERPS ring 1

In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface, as shown in figure 3-78.Name "1", ring number "1", level "0", RAPS management VLAN "1000", Owner interface "East", sub ring blocking port "None".
Click the "apply" button to return to the following page:

Figure 3-78 ERPS instance configuration display interface

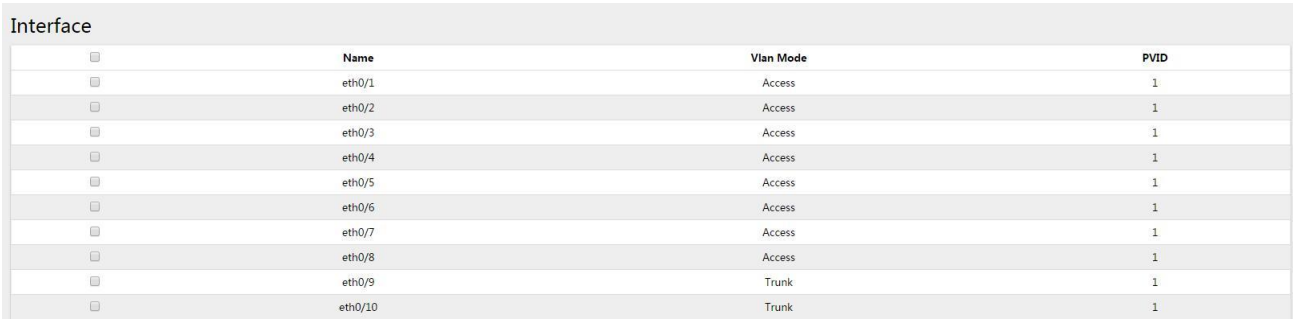
Step 5: select the "save" button on the navigation bar and save the configuration.

3.2.6.5 Configure Switch S4

Step 1: configure ports 9 and 10 as trunk ports and Native Vlan as default value 1.

Select [VLAN] from the submenu of [switch] in the menu to enter the VLAN interface. In the interface configuration option, select ports eth0/9 and eth0/10, and click the edit button to enter the configuration mode, as shown in the figure.Select "Trunk" for VLAN mode, Native VLAN defaults to "1".Click the "apply" button, and the interface returned is shown in figure 3-79.

Figure 3-79 interface status display interface



Step 2: create VLAN 2, VLAN 3, and VLAN 4, and add VLAN 2, 3, and 4 to Trunk eth0/9 and eth0/10. Under the VLAN interface, click the "add" button, enter "2-4" in the ID, Tagged member port and tick eth0/9 and eth0/10.Click the "apply" button, and the interface returned is shown in figure 3-80.

Figure 3-80 VLAN status display interface

Step 3: create ERPS ring 2 and set up the east-west interface.

Select [ERPS] in the menu [exchange] and enter the ERPS configuration interface. Click the button [+ add] to enter the ERPS ring configuration interface, as shown in figure 3-81.The ring number is set to "2", the eastern interface to "eth0/9" and the western interface to "eth0/10".Click the "apply" button to return to the following page:

Figure 3-81 ERPS ring configuration display interface

Step 4: create ERPS instance 2

In the ERPS configuration interface, select the instance configuration and click [+ add] button to enter the ERPS instance configuration interface, as shown in figure 3-82.Name "2", ring number "2", level "0", RAPS management VLAN "1001", Owner interface "East", sub ring blocking port "None".Click the "apply" button to return to the page as shown in figure 3-82:

Figure 3-82 ERPS instance configuration display interface

Step 5: select the "save" button on the navigation bar and save the configuration.

3.3 IGMP Snooping

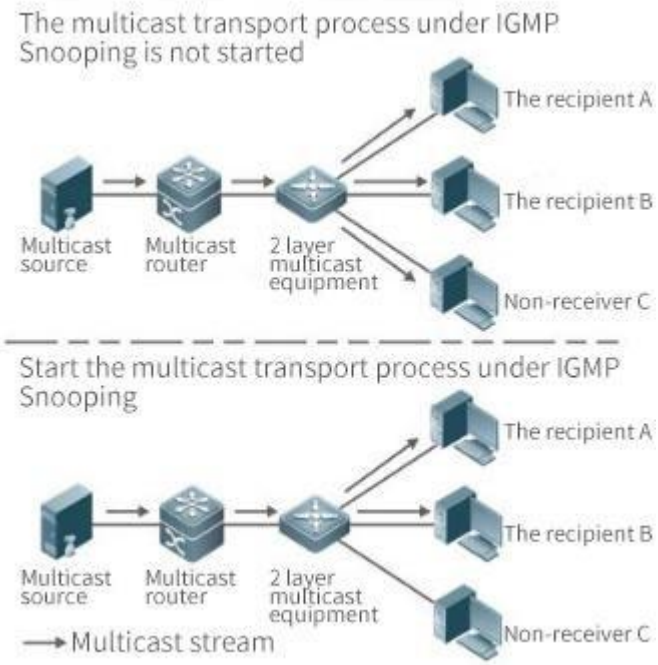
3.3.1 overview

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

The 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 receiver.

As shown in Figure 3-83, 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 member recipients..

Figure 3-83 how IGMP Snooping works



3.3.2 IGMP Snooping configuration

3.3.2.1 IGMP global configuration instructions

(1) select "IGMP Snooping" in the menu, and click the "configuration" TAB to enter the global configuration page of IGMP Snooping, as shown in figure 3-84.
(2) click the IGMP Snooping "disabled" button to enable the global IGMP Snooping function.

(3) click the "disabled" button of discarding unknown multicast to enable discarding unknown multicast function.

Figure 3-84 IGMP global configuration interface

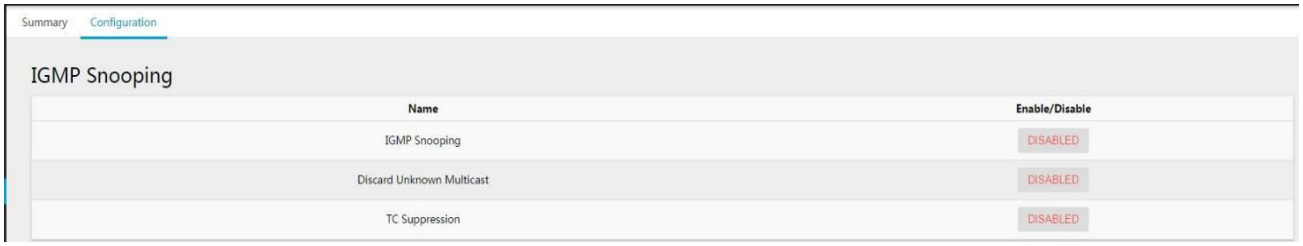


Table 3-11 global configuration parameter description

Configuration items		instructions
IGMP Snooping	IGMP Snooping	Turns on/off the IGMP Snooping function, which is turned off by default.
	Discard unknown multicast	Turn on/off discard unknown multicast function An unknown multicast data packet is defined as a forwarding item that does not exist in an IGMP Snooping forwarding those multicast data packets: • When enable discards the unknown multicast datagram function, the switch discards all received unknown groups Broadcast data message • Switch will be in the location of unknown multicast datagram when discarding unknown multicast datagram functionality is forbidden Belong to the VLAN broadcast within the paper
	Topological change suppression	Turn on/off topology change suppression

3.3.2.2 IGMP Routing Port Configuration Instructions

(1) select > [IGMP Snooping] in the menu, and click the "configuration" TAB to enter the IGMP routing port display page, as shown in figure 3-85.

Figure 3-85 IGMP routing port display interface

Table 3-12 IGMP routing port parameters

Configuration items		instructions
IGMP routing mouth	VID	The ID of the VLAN to which the multicast table entry belongs
	Interface	All member ports
	Delete	Delete the IGMP route

(2) click the "add" button to enter the interface of setting IGMP routing port, as shown in figure 3-86. Configure Vid and select the port to be applied.Click the "apply" button to complete the configuration.

Figure 3-86 IGMP routing interface configuration

3.2.2.3 IGMP Static Group Configuration Instructions

(1) Select [switch] -> [IGMP Snooping] in the menu, and enter the IGMP static group display page, as shown in figure 3-87.

Figure 3-87 IGMP static group display interface

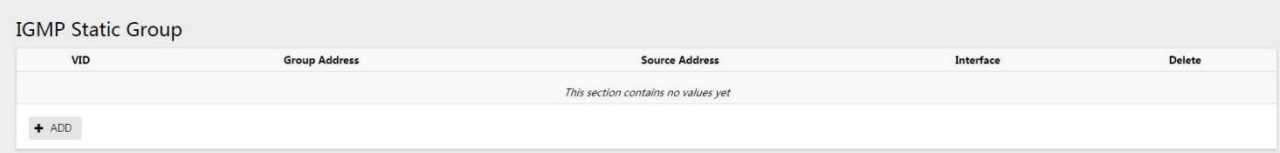


Table 3-13 IGMP static group parameter description

Configuration items		instructions
IGMP static group	VID	The ID of the VLAN to which the multicast table entrybelongs
	Group address	Multicast group address
	Source address	Multicast source address
	Interface	All member ports
	Delete	Delete the IGMP static group

(2) click the "add" button to enter the IGMP static group setting interface, as shown in figure 3-88.Configure vids, group addresses, source addresses, and interface names.Click the "apply" button to complete the configuration.

Figure 3-88 IGMP static group configuration interface

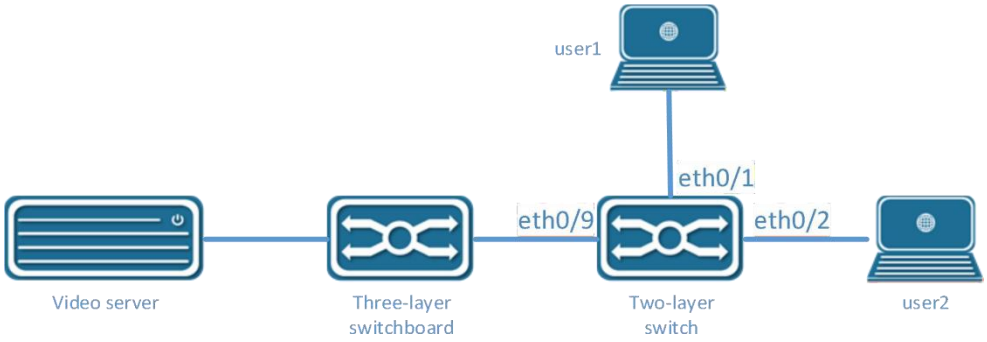
3.3.3 Examples of Configuration

Configuration example

Case requirements:

Video server uses 225.0.0.1 as the multicast source and applies multicast data stream to play video.Users click to play video as needed. Video message flow exists in the network only in the server-on-demand client channel, and no duplicate or invalid flow is allowed to maximize the utilization of network bandwidth.The network topology is shown in figure 3-89, in which the three-layer switch is used as the multicast routing device to directly connect the multicast source, enable the multicast routing forwarding function, and configure the multicast routing protocol (see the corresponding three-layer switch product configuration manual for details).The two-layer access switch is the user access device. The data VLAN is the default VLAN 1, the upper port is eth0/9, the lower port is eth0/1 and eth0/2 respectively.

Figure 3-89 IGMP network topology



Step 1: enable the IGMP Snooping function on Switch B.

Select "IGMP Snooping" from the "switch" sub-item in the menu, and enter the configuration screen. Click the "disable" button after "IGMP Snooping" to enable the IGMP Snooping function, as shown in figure 3-90.

Figure 3-90 IGMP enable configuration interface

Step 2: Enable the function of discarding unknown name multicasts on Switch B (optional)

Select "IGMP Snooping" in the "switch" subitem in the menu, enter the configuration interface, and click "disable" button after "discard unknown multicast" to enable the function of discarding unknown multicast, as shown in figure 3-91.

Figure 3-91 IGMP discarding unknown multicast configuration interface

Step 3: configure the IGMP routing port on Switch B (optional)

Select "IGMP Snooping" from the "switch" subitem in the menu, and enter the configuration interface. Click "add" button under "IGMP routing port" to enter the interface of routing port adding, as shown in figure 3-92.:

Figure 3-92 IGMP routing interface configuration

Click the "ok" button to return to the interface as shown in FIG. 3-93.

Figure 3-93 IGMP routing port display interface

Step 4: configure IGMP static groups under Switch B (optional)

Select "IGMP Snooping" from the "switch" subitem in the menu, and enter the configuration interface. Click the "add" button under "IGMP routing port" to enter the interface of routing port adding, as shown in figure xx.:

Figure 3-94 IGMP static group configuration interface

Click the "ok" button to return to the interface as shown in FIG. 3-95.

Figure 3-95 IGMP static group display interface

Step 5: select the "save" button on the navigation bar and save the configuration.

3.4 Spanning Tree

3.4.1 Overview

Spanning tree protocol is a two-layer management protocol, which eliminates the two-layer loop by selectively blocking redundant links in the network, and has the function of link backup.

SpanningTree protocols, like many others, are constantly being updated as the network evolves, from the original STP (SpanningTree Protocol) to the RSTP (Rapid SpanningTree Protocol) to the latest MSTP (Multiple SpanningTree Protocol).

With layer 2 Ethernet, there can only be one active path between the two lans, otherwise there will be a broadcast storm.However, in order to enhance the reliability of a LAN, it is necessary to establish redundant links, some of which must be in a backup state. If the network fails and another link fails, the redundant links must be promoted to active state.Controlling such a process manually is obviously a lot of hard work, and the STP protocol does it automatically.It enables a device in a LAN to do the following:

• discover and launch an optimal tree topology for the LAN.

• discover failures and then recover, automatically update the network topology so that the best tree structure possible is selected at all times.

3.4.2 Spanning Tree Configuration

The spanning tree module provides global configuration, MST configuration, instance, interface and other configurations of the spanning tree.The state and configuration interface are shown in figure 3-96~101, and the detailed parameters are shown in table 3-14~18:

Figure 3-96 spanning tree overview

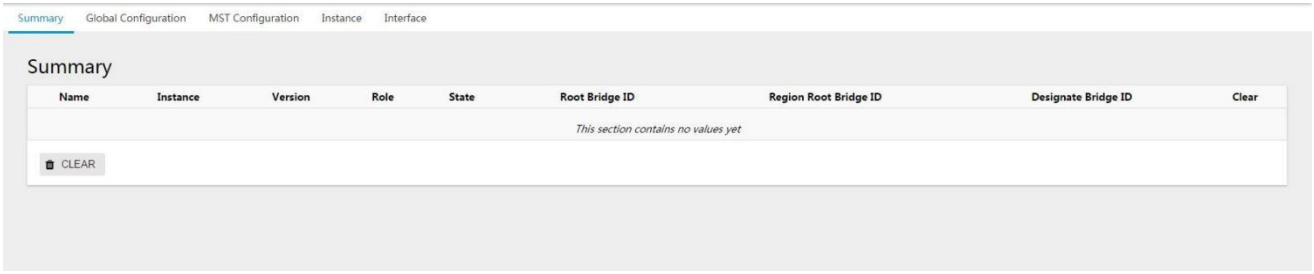


Table 3-14 overview parameter description of spanning tree

Configuration items		instructions
General Situation	Naming	The name of the interface
	The instance	Hardware instance ID
	Version	Interface spanning tree protocol version
	Role	Interface spanning tree roles, including Root: Root port, the interface connects to the direction of the Root bridge Designated: specifies the port that connects to the root port Alternate: Alternate port, Alternate root port Backup: Backup port Disable: interfaces Down or Disable the ports of the spanning tree protocol
	State	Interface spanning tree state, including: Forwarding: forward Discarding: discard Learning: Learning Listening: listen to
	The Root Bridge ID	The root bridge ID
	Region Root Bridge ID	Domain ID root bridge
	Designate Bridge ID	Specify the bridge ID
	Remove	Clear negotiated protocol version information

Figure 3-97 global configuration interface

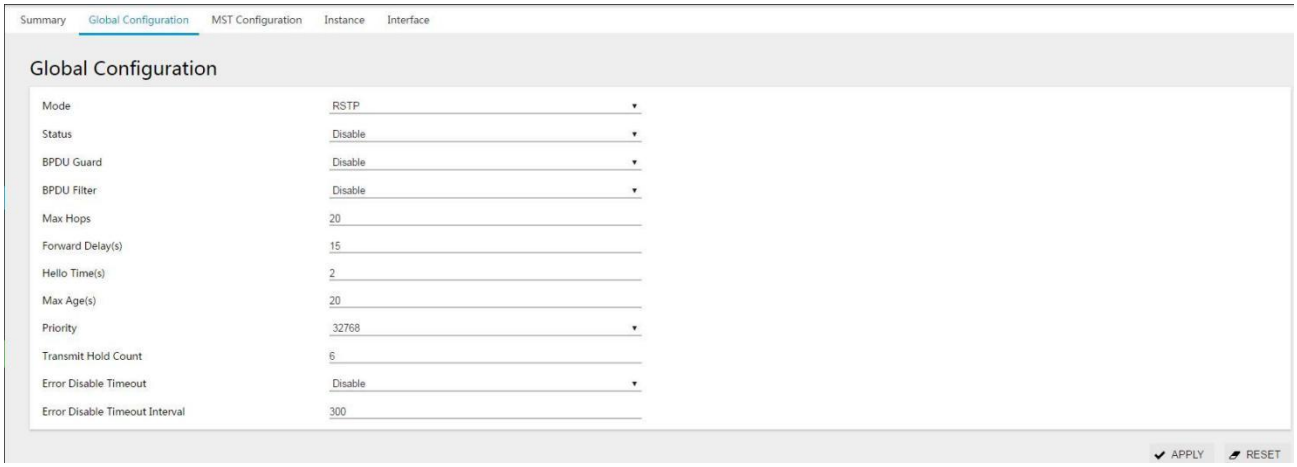


Table 3-15 global configuration parameter description

Configuration items		instructions
Global configuration	Mode	Set the working mode of STP, including STP, RSTP, and MSTP STP: in STP mode, each port of the device will send out STP BPDU messages RSTP: in the RSTP mode, each port of the device will send out RSTP BPDU messages. When it is found to be connected with the device running STP, the port will automatically migrate to the STP mode MSTP: in MSTP mode, each port of the device will send out MSTP BPDU messages. When it is found to be connected with the device running STP, the port will automatically migrate to STP mode
	State	Set whether to enable global STP functionality
	BPDU Protection	Set whether to enable global BPDU protection Enable BPDU protection function can prevent artificial forged configuration messages malicious attack devices, avoid network shock
	BPDU Filter	Turn on/off BPDU filtering
	The Largest Hop	Sets the maximum number of hops for the MST domain, which determines the size of the MST domain This parameter will only take effect in the domain if configured on the domain root, not on the non-domain root
	The Forward Delay	Set the delay time for device state migration
	Hello Time	Set the period of sending hello message to detect link fault
	Max Age	Sets the maximum length of time messages are held on the device
	priority	The bridge priority
	Forward Threshold	The maximum number of BPDU messages per second sent by the bridge
	Wrong port disable timeout	Configure the wrong port auto disable feature
	Error port disables timeout	Time to release the disabled port automatically triggered by wrong configuration

Figure 3-98 MST configuration interface

Table 3-16 MST configuration parameters

Configuration items		instructions
The MST Configuration	Domain name	Set the domain name for the MST domain By Default, the domain name for the MST domain is "Default"
	Revision level	Sets the revision level for the MST domain

Figure 3-99 instance configuration interface

Table 3-17 example configuration parameter description

Configuration Items		instructions
The Instance	ID	Instance ID
	VLAN list	All vlans associated with the instance, shown as a list
	Priority	The priority of the bridge in the current instance
	The editor	Click to edit the instance
	Delete	Click delete this instance

Figure 3-100 instance creation interface

Figure 3-101 interface status display interface

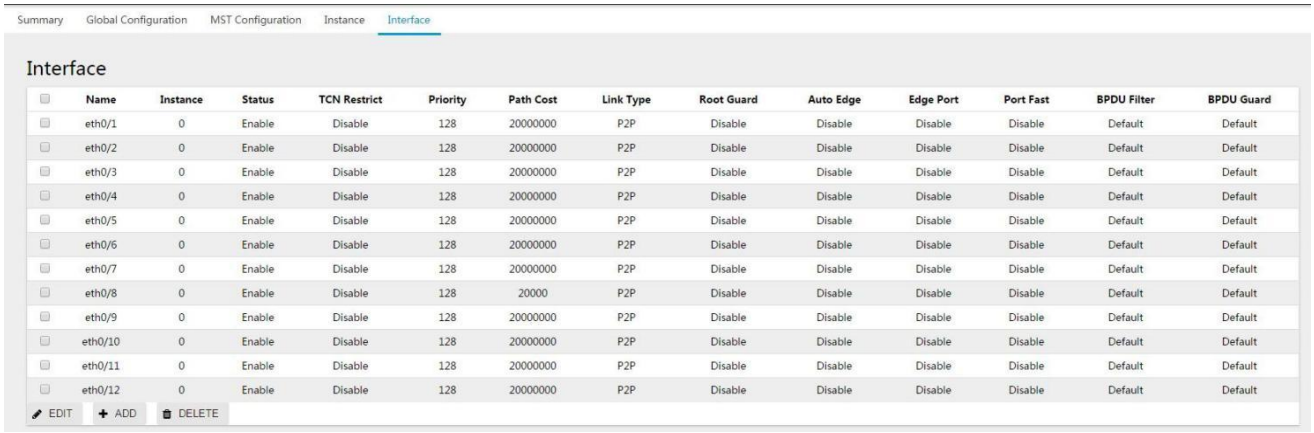
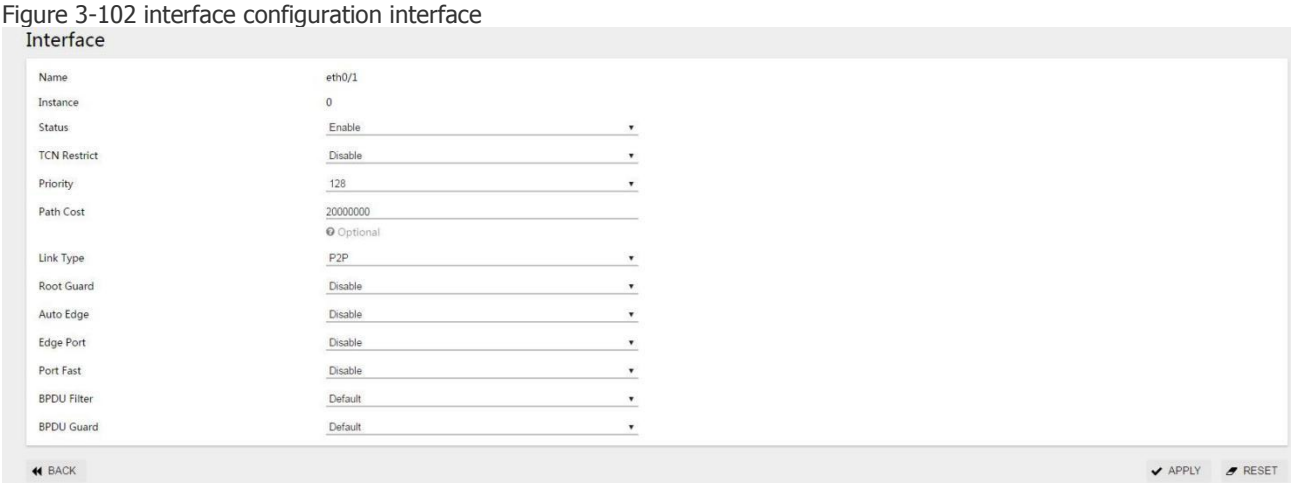


Table 3-18 interface parameter description

Configuration items		instructions
interface	The name of the	The name of the interface
	The instance	Interface associated instance ID
	state	Spanning tree switching state of the interface
	TCN message limit	Configure topology change notification message suppression
	priority	Configure interface priority
	Road king overhead	Configure interface path overhead
	Link type	Configure the interface link type
	Root protection	Configure the interface to enable root protection
	Automatic edge port	Configure the interface's ability to automatically identify edge ports
	Edge of the port	Configure the interface as an edge port
	Fast port	Configure the interface as a fast port
	BDPU filter	The configuration interface turns on BPDU filtering
	BDPU protection	The configuration interface turns on BPDU protection

Figure 3-102 interface configuration interface



3.4.3Configuration Examples

3.4.3.1Networking Requirements

MSTP is configured. Messages of different vlans in figure 3-103 are forwarded according to different spanning tree instances. The specific configuration is:

- All devices in the network belong to the same MST domain;

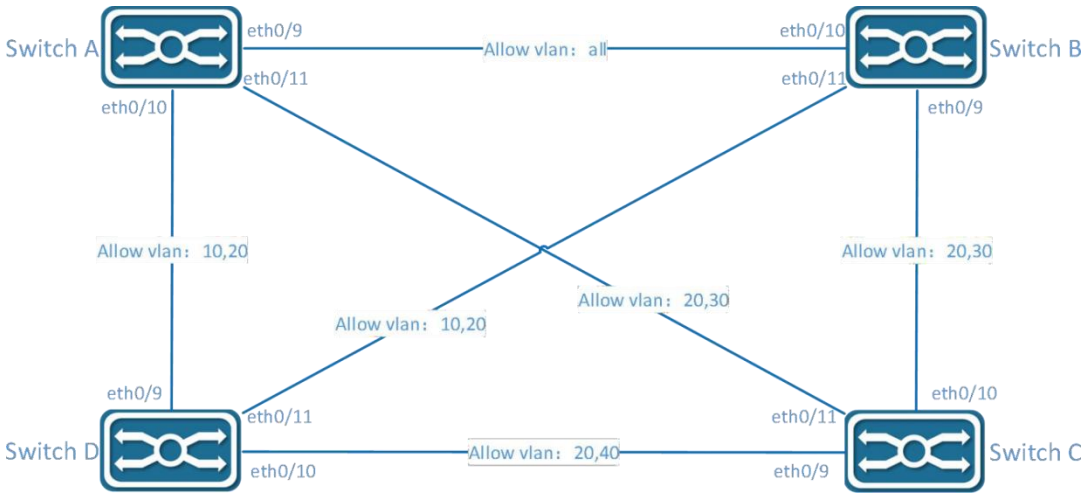
- VLAN 20 is forwarded along instance 0, VLAN 10's message is forwarded along instance 1, VLAN 30 is forwarded along instance 3, and VLAN 40 is forwarded along instance 4.

The parameter configuration of each device is shown in table 3-18:

Table 3-19 equipment parameters list

parameter equipment	VLAN	The instance	port
The Switch A	10	1	Eth9, eth0/10
	20	0	Eth9, eth0/10, eth0/11
	30	3	Eth9, eth0/11
	40	4	eth9
Switch B	10	1	Eth0/10, eth0/11
	20	0	Eth9, eth0/10, eth0/11
	30	3	Eth9, eth0/10
	40	4	eth10
The Switch C	10	1	
	20	0	Eth9, eth0/10, eth0/11
	30	3	Eth10, eth0/11
	40	4	eth9
The Switch D	10	1	Eth9, eth0/11
	20	0	Eth9, eth0/10, eth0/11
	30	3	
	40	4	eth10

Figure 3-103 MSTP network topology



instructions

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

3.4.3.2Configure Switch A

Step 1: select [switch] [VLAN] in the menu, in the port configuration interface, configure ports 9, 10, 11 as trunk ports, and Native Vlan as the default value 1.

Figure 3-104 VLAN mode configuration interface

Step 2: in the VLAN interface, click "add" button to create VLAN 10,20,30,40, as shown in figure 3-105.

Figure 3-105 VLAN creation interface

Click the "apply" button to return to the interface as shown in the figure. At this time, all ports will be added to the VLAN by default.

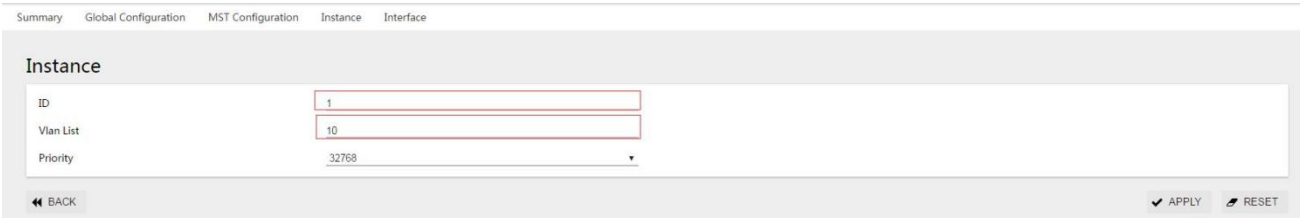
Figure 3-106 VLAN state display interface

Select VLAN 10 and click the "edit" button to enter the edit interface. Eth0/11 is deleted. Click "apply" to return to the following interface:

Figure 3-107 VLAN state display interface

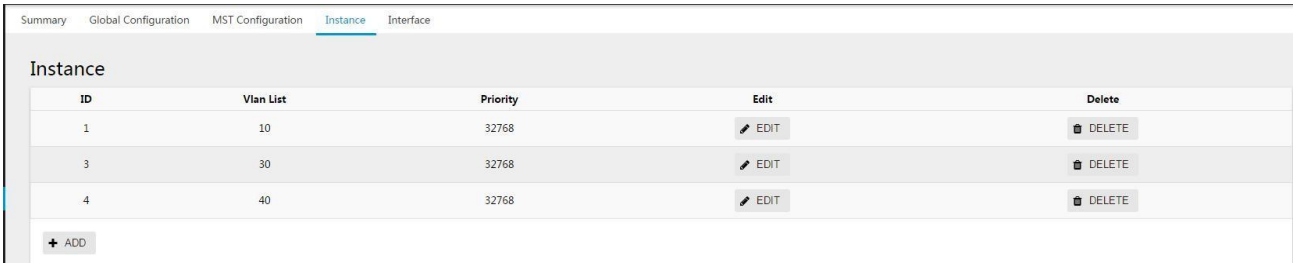
Step3: select the[exchange] [spanning tree], click the[instance]TAB, and click the[add] button, as shown in the figure below, ID is "1", VLAN list is "10", the default parameters are used for priority, and click the "apply" button to save the configuration.

Figure 3-108 spanning tree instance configuration interface



In the same way, create instances 3 and 4 with corresponding VLAN lists of 30 and 40, and create the successful instance list as shown in the figure.

Figure 3-109 spanning tree instance display interface



instructions

- Non associated VLAN is classified into instance 0 by default..

Step 4: in the current interface, click the "global configuration" TAB, select mode as "MSTP", state as "Enable", select default for other parameters, and click "apply" button to complete the configuration.

Figure 3-110 spanning tree global configuration interface

Step 5: select the "save" button on the navigation bar and save the configuration.

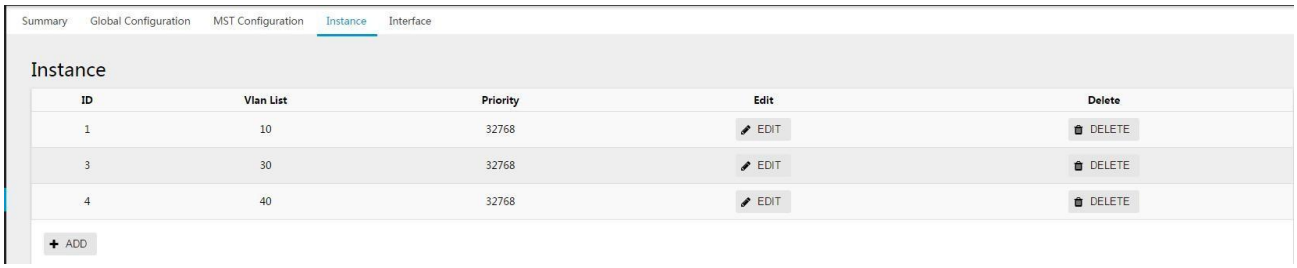
3.4.3.3configure Switch B

Step1: Refer to Swtich A, configure ports 9, 10, and 11 as trunk ports, and Native Vlan as the default value 1.
Step2: Create VLAN 10, 20, 30, 40, and add the corresponding ports to the VLAN, as shown in the figure.

Figure 3-111 VLAN status display interface

Step3: select the[exchange][spanning tree], click the [instance]TAB, and click the[add] button, as shown in the figure below, ID is "1", VLAN list is "10", the default parameters are used for priority, and click the "apply" button to save the configuration.

Figure 3-112 spanning tree instance display interface



Step 4: in the current interface, click the "global configuration" TAB, select mode as "MSTP", state as "Enable", select default for other parameters, and click "apply" button to complete the configuration.

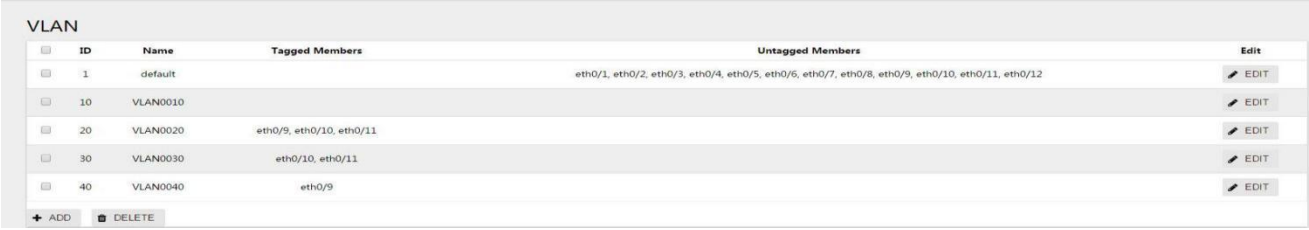
Figure 3-113 spanning tree global configuration interface

Step 5: select the "save" button on the navigation bar and save the configuration.

3.4.3.4 Configure Switch C

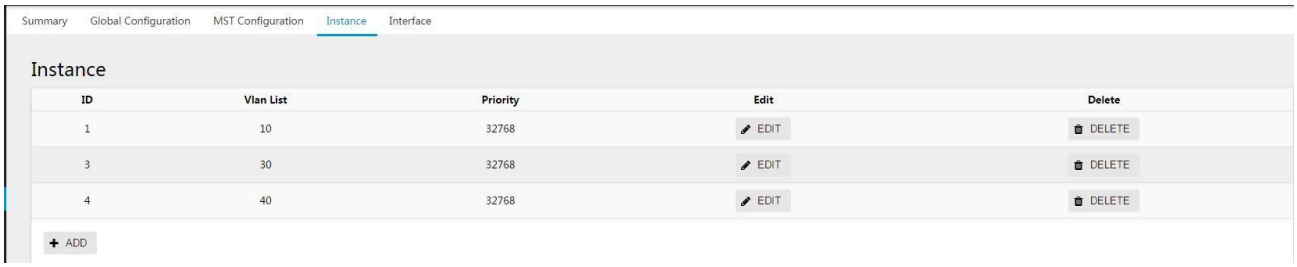
Step1: Refer to Swtich A to configure ports 9, 10, and 11 as trunk ports, and Native Vlan as the default value 1.
Step2: Create VLAN 10, 20, 30, 40, and add the corresponding ports to the VLAN, as shown in the figure.

Figure 3-114 VLAN state display interface



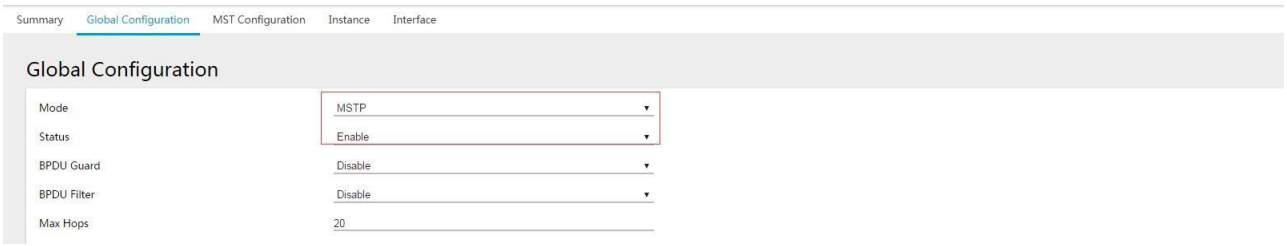
Step3: select the [exchange] [spanning tree], click the [instance] TAB, and click the [add] button, as shown in the figure below, ID is "1", VLAN list is "10", the default parameters are used for priority, and click the "apply" button to save the configuration.

Figure 3-115 spanning tree instance display interface



Step 4: in the current interface, click the "global configuration" TAB, select mode as "MSTP", state as "Enable", select default for other parameters, and click "apply" button to complete the configuration.

Figure 3-116 spanning tree global configuration interface



Step 5: select the "save" button on the navigation bar and save the configuration.

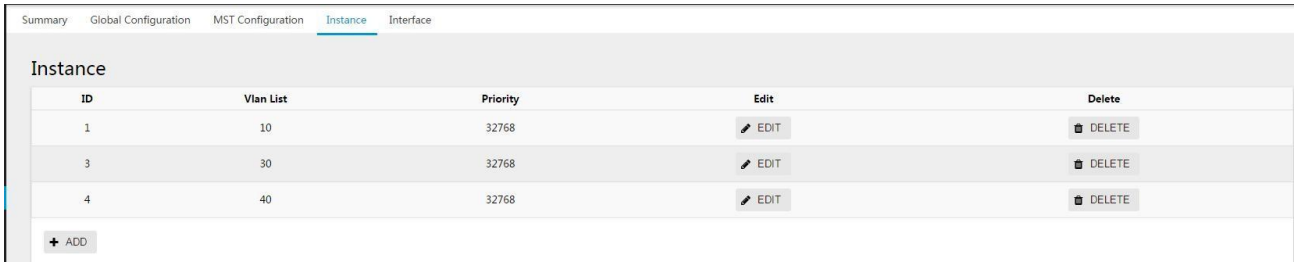
3.4.3.5Configure Switch D

Step1: Refer to Swtich A to configure ports 9, 10, and 11 as trunk ports and Native VLAN as default value 1.
Step2: Create VLAN 10, 20, 30, 40, and add the corresponding ports to the VLAN, as shown in the figure.

Figure 3-117 VLAN status display interface

Step3: select the [exchange] [spanning tree], click the [instance] TAB, and click the [add] button, as shown in the figure below, ID is "1", VLAN list is "10", the default parameters are used for priority, and click the "apply" button to save the configuration.

Figure 3-118 spanning tree instance display interface



Step 4: in the current interface, click the "global configuration" TAB, select mode as "MSTP", state as "Enable", select

default for other parameters, and click "apply" button to complete the configuration.

Figure 3-119 spanning tree global configuration interface

Step 5: select the "save" button on the navigation bar and save the configuration.

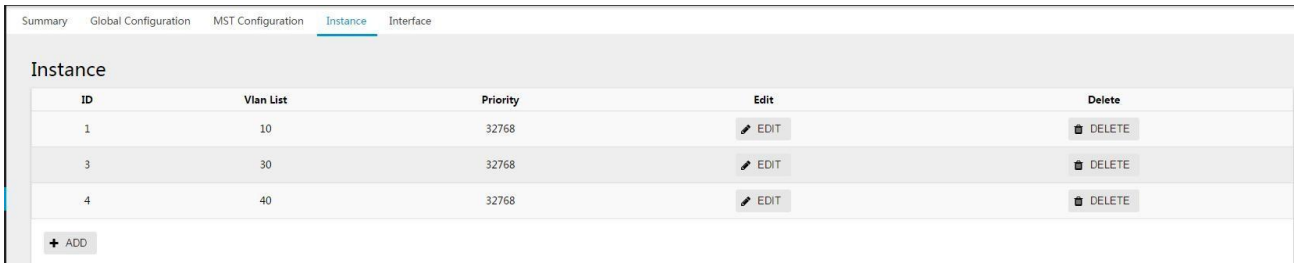
3.4.3.6Configure Switch D

Step 1: refer to Swtich A to configure ports 9, 10, and 11 as trunk ports and Native Vlan as default value 1.
Step 2: create VLAN 10,20,30,40 and add the corresponding ports to the VLAN, as shown in the figure.

Figure 3-117 VLAN status display interface

Step3:selectthe[exchange][spanningtree],clickthe[instance]TAB,andclickthe[add]button, as shown in the figure below, ID is "1", VLAN list is "10", the default parameters are used for priority, and click the "apply" button to save the configuration.

Figure 3-118 spanning tree instance display interface



Step 4: in the current interface, click the "global configuration" TAB, select mode as "MSTP", state as "Enable", select default for other parameters, and click "apply" button to complete the configuration.

Figure 3-119 spanning tree global configuration interface

Step 5: select the "save" button on the navigation bar and save the configuration.

3.5 MAC Management

3.5.1 Overview

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

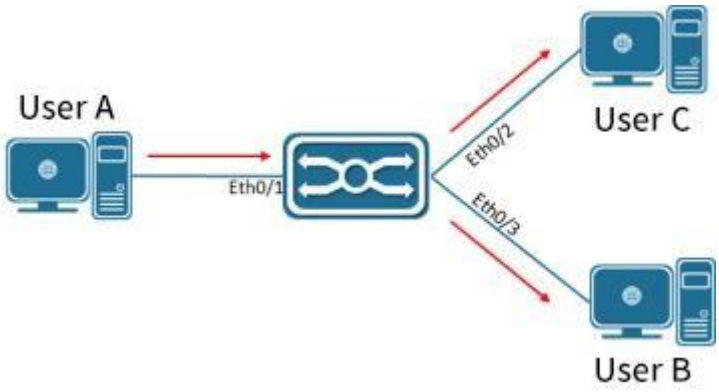
Well-known unicast: The Ethernet switch finds the entry corresponding to the destination MAC address and VLAN ID of the message in the MAC address table and the output port in the entry is unique, and the message is directly output from the port corresponding to the entry.

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

The MAC address of the Ethernet switch can be obtained dynamically or configured statically. Generally, it can be obtained dynamically. The following describes the working principle of dynamic MAC address learning by analyzing the interaction process between user A and user C.

As shown in Figure 3-120, user A sends a packet to port eth0/1 of the switch, and the Ethernet switch learns the MAC address of user A into the MAC address table. Since there is no source MAC address of user C in the address table, the Ethernet switch broadcasts the message to all ports belonging to VLAN 1 except eth0/1 connected to user A, including the ports of user B and user C At this time, user B can receive the packets sent by user A that do not belong to it.

Figure 3-120 unknown broadcast 1



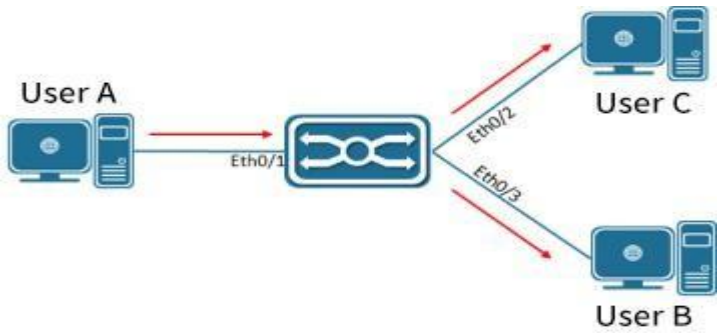
The current dynamic MAC address table information is shown in Table 3-20:

Table 3-20 Equipment Parameters List

The user	VLAN	The MAC address	Port
User A	1	000 e. C6C1 C8AB	Eth0/1

As shown in Figure 3-121, after user B receives the message, the response message is sent to user A through port eth0/2 of the Ethernet switch. At this time, the MAC address of user A already exists in the MAC address table of the Ethernet switch. The message is forwarded to port eth0/1 in unicast mode, and 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. Text.

Figure 3-121 unknown broadcast 2



The current dynamic MAC address table information is shown in Table 3-21:

Table 3-21 Equipment Parameters List

The user	VLAN	The MAC Address	Port
User A	1	000 e. C6C1 C8AB	Eth0/1
User C	1	000 e. C6C1 C8AD	Eth0/2

After an interaction process between user A and user C, the device has learned the source MAC addresses of user A and user C, and then the message interaction between user A and user C is forwarded in unicast mode, and then user B will no longer receive interactive messages between user A and user C.

3.5.2 Configure the MAC address

MAC address table entries are divided into: static MAC address table entries, dynamic MAC address table entries, and filtered MAC address table entries.
Static MAC address table entry: manually configured by the user, the table entry does not age.
Dynamic MAC address table entries: including those configured by the user and those learned by the device from the source MAC address. The table entries have an aging time.
Filtering MAC address entries: used to discard packets with specific MAC addresses (for example, for security reasons, a user can be blocked from receiving packets), it is manually configured by the user, and the entries do not age.
Select [switch] [MAC management] from the navigation bar and enter the MAC management interface, as shown in the figure below. All MAC management parameters are shown in table 3-22.

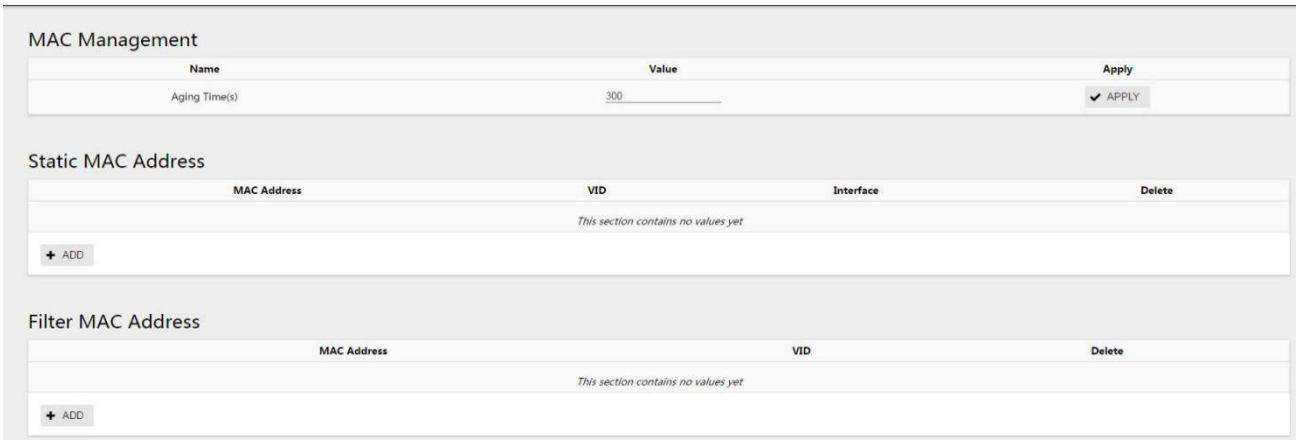


Table 3-22 MAC Address Management Parameters

Configuration Items		Instructions
Aging Time	Name	Aging time per second
	Value	<30,1000>, the default aging time is 300 seconds, the MAC address was aged by the system within 300 to 600 seconds of the last update
	Application	Click configure to take effect
Static Address	MAC Address	Static MAC address configuration in a format such as: 00-00-00-00-01
	VID	VLAN properties of MAC addresses
	Interface	Port properties of the MAC address
	Delete	Remove the static MAC address
Filter Address	MAC Address	Configure to filter MAC addresses in formats such as: 00-00-00-00-01
	VID	VLAN properties of MAC address
	Delete	Remove the filtered MAC address

3.5.3 MAC Address Configuration Example

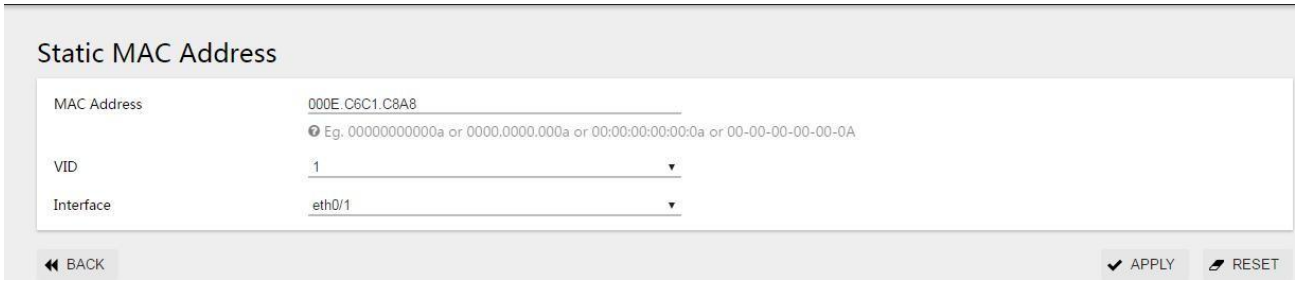
Configuration example:

Case requirements: All packets with destination MAC address 000E.C6C1.C8AB and VLAN 1 are forwarded from port eth0/1, and packets with MAC address 000E.C6C1.C8CC and VLAN 10 are filtered at the same time

Step 1: Create a static MAC address, MAC: 000E.C6C1.C8AB, VLAN 1, port eth0/1.

Select [Exchange] -> [MAC Management] in the menu to enter the MAC address configuration interface. In the static address item, click the [Add] button and configure the MAC address, VID and interface in sequence as shown in Figure 3-122.

Figure 3-122 Static Address Configuration

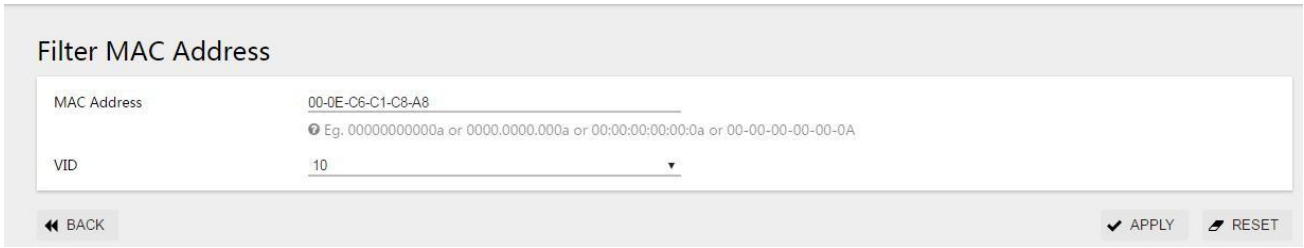


Click the [Apply] button to complete the configuration and return to the interface as shown in Figure 3-123.

Figure 3-123 Static Address Display

Step 2: Create filtering MAC address, MAC: 000E.C6C1.C8CC, VLAN10
in the menu, select [Exchange] -> [MAC Management], enter the MAC address configuration interface, in the filter address item, click the [Add] button, as shown in Figure 3-124, configure the MAC address, VID in turn.

Figure 3-124 Static Address Display



Click the [Apply] button to complete the configuration and return to the interface as shown in Figure 3-125.

Figure 3-125 Static Address Display

Step 3: Select the "save" button on the navigation bar and save the configuration.

3.6 QinQ

3.6.1 Overview

QinQ is the abbreviation of 802.1Q in 802.1Q. It is a Layer 2 tunneling protocol based on IEEE 802.1Q technology. It encapsulates the user's private network packet with an outer VLAN tag, so that it can carry two VLAN tags through the operator. The backbone network (also known as the public network) provides users with a relatively simple Layer 2 VPN tunnel technology, and it also makes it possible for operators to use one VLAN to provide services for user networks containing multiple VLANs.

3.6.1.1 QinQ's Background & Advantages

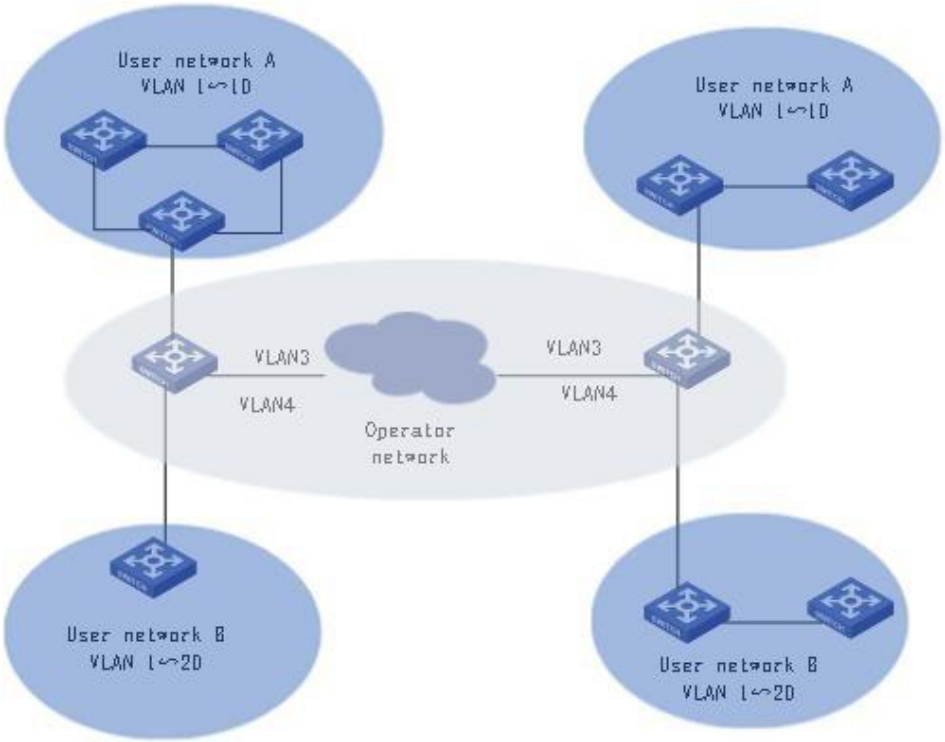
In the VLAN Tag field defined by IEEE 802.1Q, only 12 bits are used to represent the VLAN ID, and it can represent up to 4094 VLANs. However, in practical applications, especially in metropolitan area networks, a large number of VLANs are required to isolate users, and 4094 VLANs are far from meeting the demand. QinQ enables the entire network to provide a maximum of 4094×4094 VLANs, thereby meeting the demand for the number of VLANs in the metropolitan area network. It has the following advantages:

- Alleviate the problem of increasing shortage of VLAN ID resources on the public network.
- Users can plan their own private network VLAN ID, which will not cause conflicts with public network VLAN ID.
- Provides a simple and flexible Layer 2 VPN solution for small metropolitan area networks and enterprise networks.
- When the operator upgrades the network, the user network does not need to change the original configuration, so that the user network has a strong independence.

3.6.1.2 QinQ's Implementation Principles

In the transmission process of the public network, the device forwards the message only according to the outer VLAN tag, and learns the source MAC address entry of the message into the MAC address table of the VLAN where the outer VLAN tag is located, and the user's private network VLAN tag It will be transmitted as the data part of the message.

FIG. 3-126 QinQ Application Network Diagram



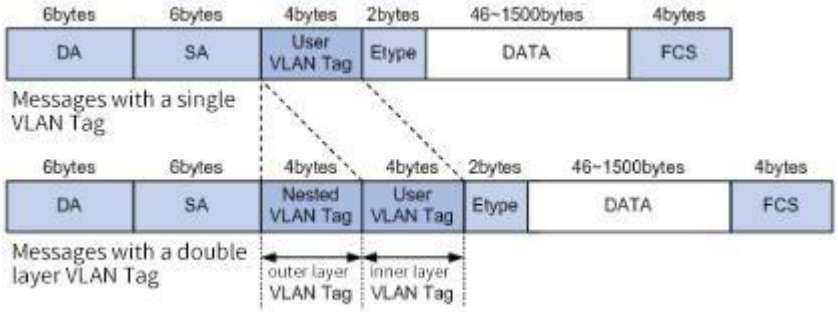
As shown in Figure 3-126, the private network VLANs of user networks A and B are VLAN 1 ~ 10 and VLAN 1 ~ 20 respectively. The VLAN assigned by the carrier to user networks A and B are VLAN 3 and VLAN 4 respectively. When packets with VLAN tags in user networks A and B enter the carrier network, the outside of the packets will be encapsulated with VLAN tags of VLAN 3 and VLAN 4 respectively. In this way, packets from different user networks are completely separated when transmitted in the operator's network. Even if the respective VLAN ranges of these user networks overlap, there will be no conflicts when transmitted in the operator's network.

3.6.1.3 QinQ's Packets Structure

As shown in Figure 3-127, QinQ packets carry double VLAN tags when they are transmitted on the carrier network:

- Inner VLAN Tag: VLAN Tag for the user's private network;
- Outer VLAN Tag: Public network VLAN tag assigned to users by the operator.

FIG. 3-127 QinQ's Packet Structure



3.6.1.4 QinQ's Implementation Mode

QinQ can be implemented in the following two ways:

1. Basic QinQ

Basic QinQ is implemented based on the port method. When the basic QinQ function is configured on the port, the device will tag the packet with the default VLAN tag of the port regardless of whether the packet received from the port has a VLAN tag:

- If the received packet is a packet with a VLAN tag, the packet becomes a packet with a double tag;
- If a packet without a VLAN tag is received, the packet becomes a packet with the default VLAN tag of the port.

2. Flexible QinQ

Flexible QinQ is implemented based on the combination of ports and VLANs. It extends the functions of QinQ and is a more flexible implementation of QinQ. Flexible QinQ In addition to realizing all basic QinQ functions, for packets received from the same port, different operations can be performed according to different VLANs, including:

- Add different outer VLAN tags to packets with different inner VLAN IDs.
- Mark the 802.1p priority of the outer VLAN according to the 802.1p priority of the inner VLAN of the packet.

Through the use of flexible QinQ technology, while being able to isolate operator networks and user networks, it can provide rich service features and more flexible networking capabilities.

3.6.2 QinQ Configuration

Read QinQ Overview

Select [Exchange]>[QinQ] in the menu to enter the page shown in Figure 3-128. The QinQ configuration can be displayed on the [Configuration] tab. The description of each parameter is shown in Table 3-23.

FIG. 3-128 QinQ Overview

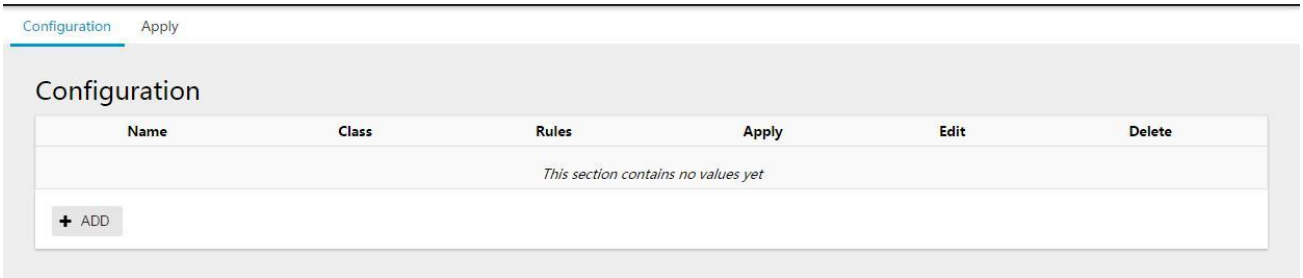


Table 3-23 QinQ Overview Parameter Instructions

Configuration items	Instructions
Name	QinQ rule name
Classification	QinQ category Stacking: multilayer tag Stacking pattern Mapping: tag replacement mode
List of rules	List of mapping rules
Application	QinQ on application information of mapping
Edit	Click the button to edit the rule
Delete	Click the button to remove the rule

Configuration QinQ

Step 1: Create VLAN VPN rule

On the current QinQ interface, click the [Add] button to enter the VLAN VPN rule creation interface, as shown in Figure 3-129. The description of each parameter of the VPN rule is shown in Table 3-23.

Figure 3-129 Creating VPN Rules

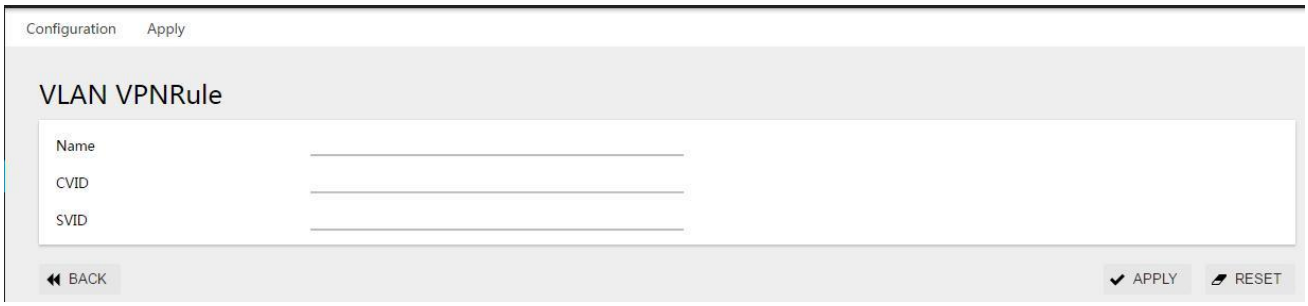


Table 3-23 QinQ Overview Parameter Instructions

Configuration Items	Instructions
Name	QinQ rule name
CVID	Client VLAN ids
SVID	Server side VLAN ID

After configuring "Name", "CVID", and "SVID", click the [Apply] button to return to the following interface, as shown in Figure 3-130, and you can see a list of successfully created rules.

Figure 3-130 Create Successful Rule List

Step 2: Configure the port's QinQ type

In the current interface, click the [Application] tab in the upper left corner to enter the port application configuration interface, as shown in Figure 3-131. Configure the QinQ type of the corresponding port and click the [Apply] button to

complete the configuration.

Figure 3-131 Configure the Type of QinQ Port

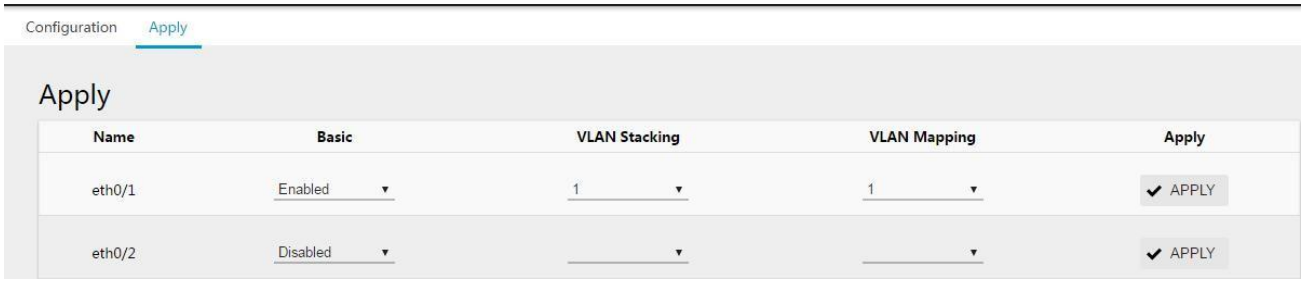
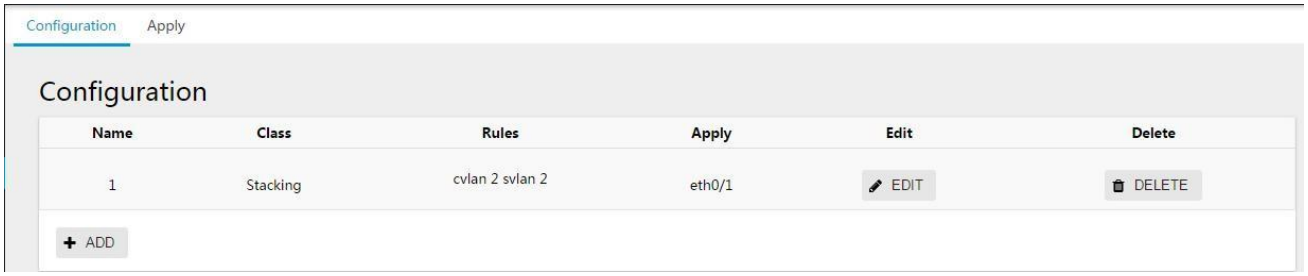


Table 3-24 QinQ Parameter Instructions

Configuration Items	Instructions
Name	The name of the interface
Basic	QinQ on the basis of rule application state
VLAN Stacking	QinQ read on several levels of rules application state
VLAN Mapping	QinQ is a replacement state of rule application

After configuration, click the upper left corner [profile] TAB bar, click the [profile] button, you can see the successful creation of QinQ rules. See figure 3-132. After the configuration is complete, click the [Summary] tab in the upper left corner and click the [Summary] button to see the successfully created QinQ rules. As shown in Figure 3-132.

Figure 3-132 Configure the Type of QinQ Port



3.6.3 QinQ Configuration Example

Configuration Example

Case requirement 1: implement layer 2 VPN service based on port

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

- On the public network, enterprise A and enterprise B belong to different VLANs, and they communicate through their own public network VLAN.
- The VLANs in enterprise A and enterprise B are transparent to the public network, and user VLANs in enterprise A and enterprise B can be reused without conflict.
- The tunnel encapsulates a layer of Native VLAN VLAN Tag for user data packets. In the public network, user data packets are transmitted in Native VLAN, which does not affect the use of VLANs in different enterprise user networks, and implements a simple Layer 2 VPN.

FIG. 3-133 QinQ Network Topology 1

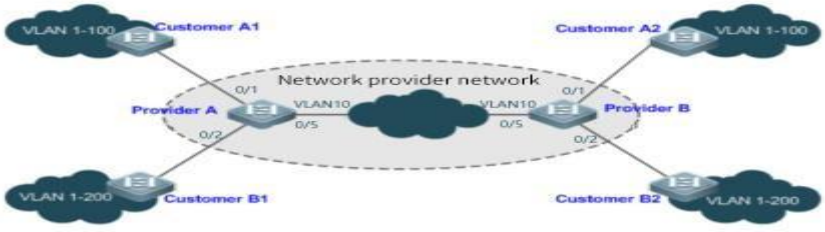


Illustration:

- Customer A1 and Customer A2, Customer B1 and Customer B2 are the edge devices of the network where Enterprise User A and Enterprise User B are located. Provider A and Provider B are service provider network edge devices, and enterprise A and enterprise B provide business edge devices connected to the public network.
- The office network VLAN range used by enterprise A is VLAN 1-100.
- The office network VLAN range used by enterprise B is VLAN 1-200.

Provider A and Provider B are completely symmetrical, and the configuration is exactly the same:

Step 1: Configure the port mode of ports eth0/1, eth0/2 and eth0/5 as Trunk port

in the menu, select [Switch]> [VLAN]> [Interface] to enter the interface configuration interface, select ports eth0/1, eth0/2, eth0/5, and click the [Edit] button to enter the configuration mode, as shown in Figure 3- 133 shown. Select "Trunk" for VLAN mode, and Native Vlan defaults to "1".

Figure 3-133 Configure Port VLAN Mode

Step 2: Create VLAN 2-200, and check eth0/1, eth0/2 and eth0/5 for the tagged member ports.

Select [Switch]> [VLAN] in the menu, click the [Add] button to enter the VLAN configuration interface, enter "2-100" in the ID text box, and select eth0/1, eth0/2, eth0/5 for the Tagged member port, click [Apply] button to complete the configuration.

Figure 3-134 Create VLAN

Step 3: Create VLAN 2-200, and check eth0/2 and eth0/5 for the tagged member ports.

Select [Switch]> [VLAN] in the menu to enter the VLAN configuration interface, enter "101-200" in the ID text box, check eth0/2, eth0/5 for the tagged member port, and click the [Apply] button to complete the configuration.

Figure 3-135 Create VLAN

Step 4: Configure the port mode of ports eth0/1, eth0/2 and eth0/5 as Trunk port.

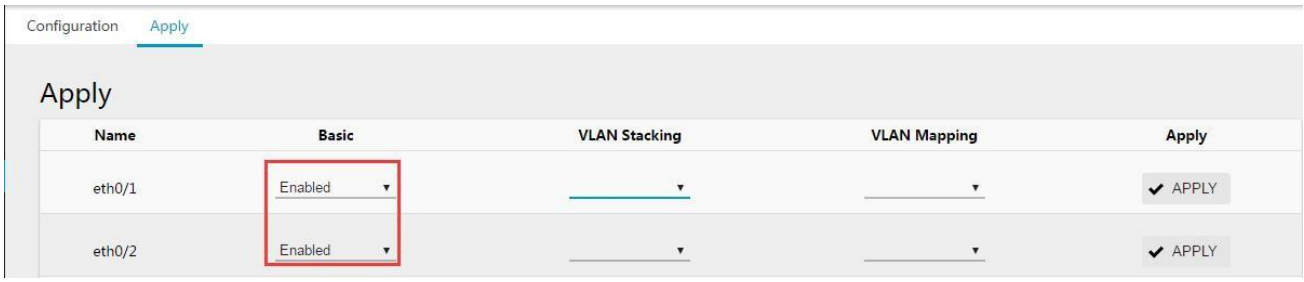
Select [Switch]> [VLAN]> [Interface] in the menu to enter the interface configuration interface, select ports eth0/1, eth0/2, and click the [Edit] button to enter the configuration mode, as shown in Figure 3-136. Select "Trunk" for VLAN mode, and "10" for Native VLAN.

Figure 3-136 Configure Port VLAN Mode

Step 5: Configure the port mode of ports eth0/1, eth0/2 and eth0/5 as Trunk port.

Select [Exchange]> [QinQ] in the menu to enter the QinQ configuration interface. Click the [Application] tab in the upper left corner, configure the "basic" of ports eth0/1 and eth/2 to Enabled, as shown in Figure 3-137, click the [Apply] button to complete the configuration.

Figure 3-137 Configure the Type of QinQ Port



Step 6: Select the [Save] button on the navigation bar to save the configuration.

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

Basic QinQ can only encapsulate user data packets with a native VLAN outer tag, that is, the outer tag encapsulation depends on the native VLAN of the tunnel port. Flexible QinQ provides flexible encapsulation of external tags (i.e. C-Tags) of service providers (ISPs) according to the tags (i.e. C-Tags) of user messages.

S-Tag), in order to more flexibly implement VPN transparent transmission and business flow QOS strategy.

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

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

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

Figure 3-138 QinQ Network Topology 2

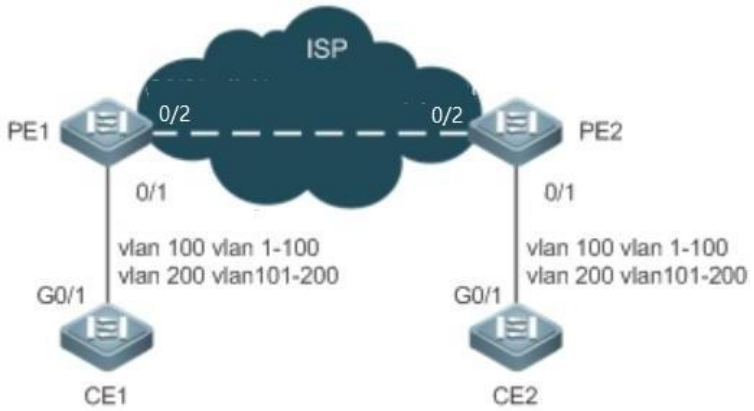


Illustration:

- CE1 and CE2 are edge devices connected to the user network, and PE1 and PE2 are edge devices of the provider service network.
- On CE1 and CE2 devices, VLAN 1-100 is the user's broadband Internet access service flow, and VLAN 101-200 is the user's IPTV service flow.
- PE1 and PE2 devices encapsulate different S-Tags for VLANs of different services to distinguish different service data. VLAN 1-100 encapsulates VLAN100, and VLAN101-200 encapsulates VLAN200.

The configurations of PE1 and PE2 are exactly the same:

Step 1: Create VLAN 2-200.

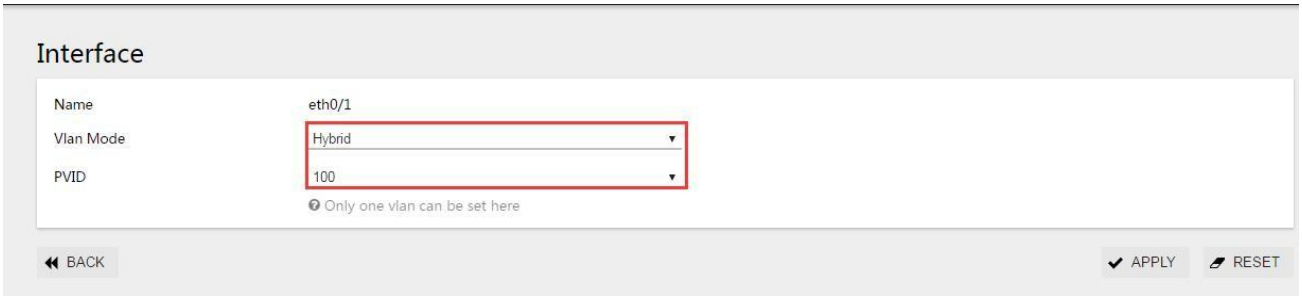
Select [Switch]>[VLAN] in the menu, click the [Add] button to enter the VLAN configuration interface, enter "2-200" in the ID text box and click the [Apply] button to complete the configuration.

Figure 3-139 Create a VLAN

Step 2: Configure the port mode of port eth0/1 as Hybrid port and PVID as "100".

in the menu, select [Switch]>[VLAN]>[Interface] to enter the interface configuration interface, select port eth0/1, and click the [Edit] button to enter the configuration mode, as shown in Figure 3-140. Select “Hybrid” for VLAN mode, and “100” for PVID.

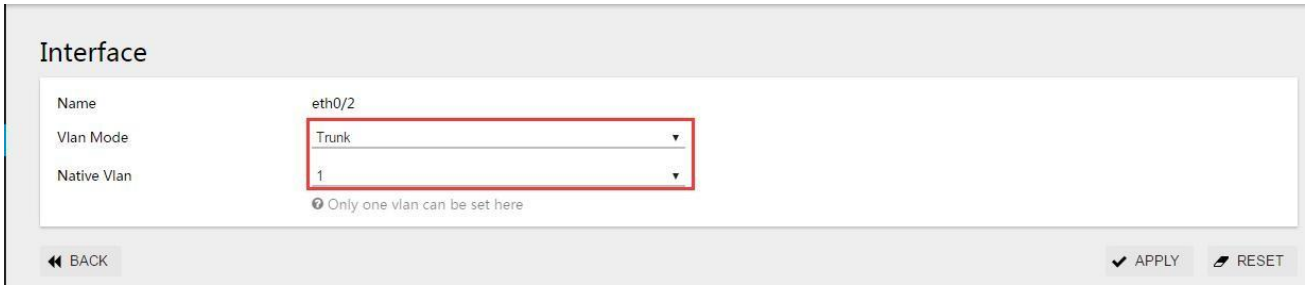
Figure 3-140 Configure Port VLAN Mode for Hybrid



Step 3: Configure the port mode of port eth0/2 as Trunk port and Native Vlan as "1".

in the menu, select [Switch]> [VLAN]> [Interface] to enter the interface configuration interface, select port eth0/2, and click the [Edit] button to enter the configuration mode, as shown in Figure 3-141. Select "Trunk" for VLAN mode, and Native Vlan defaults to "1".

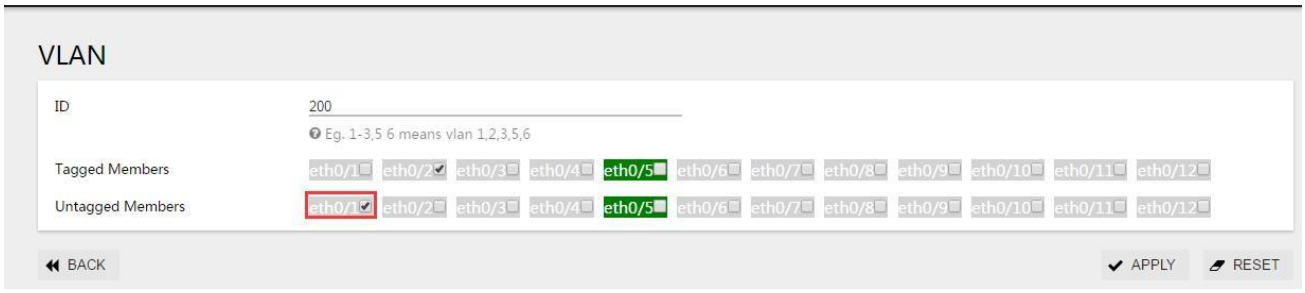
Figure 3-141 Configure Port VLAN Mode for Trunk



Step 4: Configure the tagged member port and untagged member port of VLAN200.

Select [Switch]>[VLAN] in the menu, click the [Add] button to enter the VLAN configuration interface, enter "200" in the ID text box, select eth0/2 for the tagged member port, and select eth0/1 for the untagged member port, Click the [Apply] button to complete the configuration.

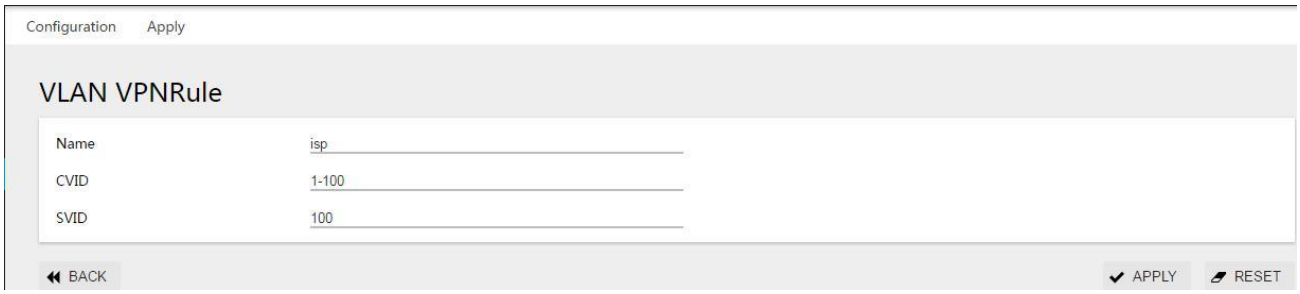
Figure 3-142 Configure Tagged and Untagged Member Ports



Step 5: Create VLAN VPN rules

in the menu, select [Exchange]> [QinQ], click the [Add] button to enter the VPN rule creation interface, enter the VLAN VPN rule creation interface, configure the name "isp", CVID "1-100", SVID "100", click Apply button to complete the configuration.

Figure 3-143 Create VLAN VPN Rules



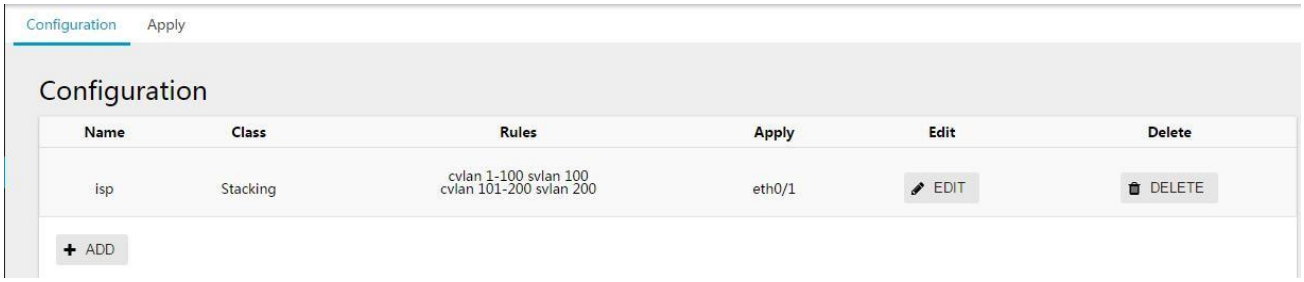
Step 5: Configure the Type of QinQ Port

In the current interface, click the "apply" TAB in the upper left corner to enter the interface of port application configuration, as shown in figure 3-144.Configure the "isp" in the VLAN Stacking drop-down option for the QinQ type of the corresponding port, click the apply button to complete the configuration.

Figure 3-144 Configure the Type of QinQ Port

The configured QinQ overview interface is shown in Figure 3-145.

Figure 3-145 QinQ Overview Interface



Step 6: Select the [Save] button on the navigation bar to save the configuration.

3.7 LLDP

3.7.1 overview

3.7.1.1 Background generated by LLDP

At present, the types of network devices are increasingly diverse and their configurations are complex. In order to enable devices from different manufacturers to discover and exchange their system and configuration information on the network, a standard information exchange platform is required.

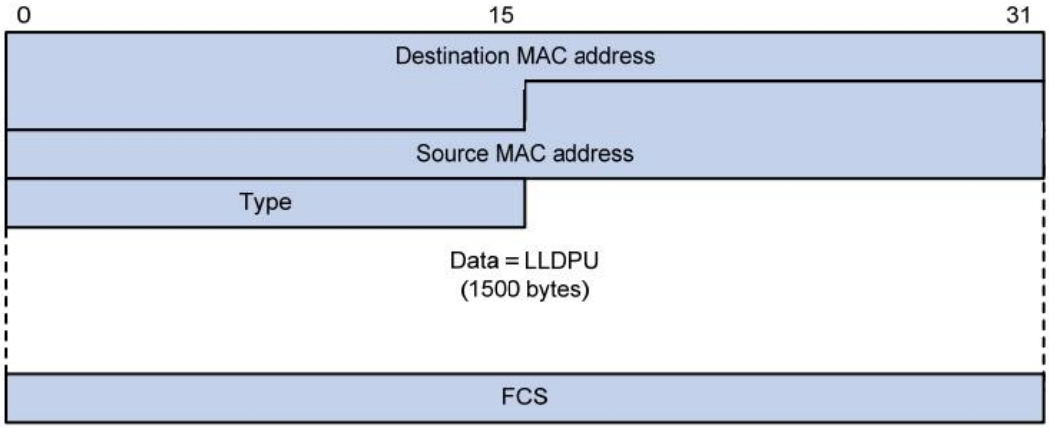
The Link Layer Discovery Protocol (LLDP) is developed in this context. It provides a standard Link Layer Discovery method. It can organize the main capabilities, management addresses, device ids, and interface ids of local devices into different TLVS (Type/Length/Value, Type/Length/Value) and encapsulate them in the Link Layer Discovery Protocol Data Unit (LLDPDU). The link layer discovery protocol data unit (LLDPDU) advertises the Information to the directly connected neighbor. After receiving the Information, the neighbor saves it in the form of a standard Management Information Base (MIB) for the network Management system to query and judge the communication status of the link.

3.7.1.2 Basic concept of LLDP

1. LLDP packets

LLDP packets encapsulated with LLDPDU are called LLDP packets. The encapsulation formats are Ethernet II and SNAP (Subnetwork Access Protocol).

Figure 3-146 LLDP packets encapsulated in Ethernet II format



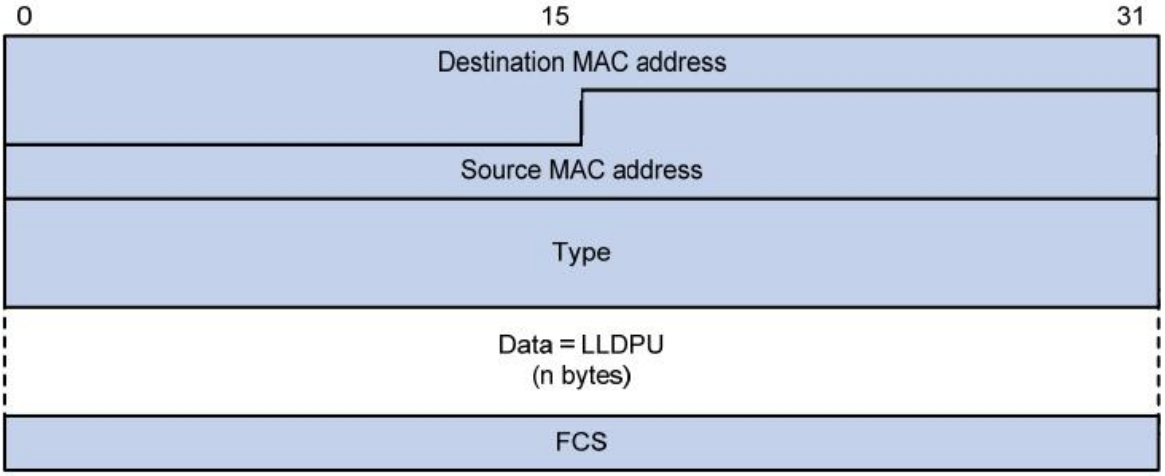
(1) LLDP packets encapsulated in Ethernet II format

As shown in Figure 3-146, an LLDP packet is encapsulated in Ethernet II format. The fields in the packet have the following meanings:

- Destination MAC Address: indicates the Destination MAC address, which is a fixed multicast MAC address 0x0180-C200-000E.
- Source MAC Address: indicates the Source MAC address, which is the port MAC address.
- Type: indicates the packet Type, which is 0x88CC.
- Data: indicates the Data content, which is LLDPDU.
- FCS: frame check sequence, used to verify packets.

(2) LLDP packets encapsulated in SNAP format

Figure 3-147 LLDP packets encapsulated in SNAP format



As shown in Figure 3-147, an LLDP packet is encapsulated in SNAP format. The fields in the packet have the following meanings:

- Destination MAC Address: indicates the Destination MAC address, which is a fixed multicast MAC address 0x0180-C200-000E.
- Source MAC Address: indicates the Source MAC address, which is the port MAC address or the device bridge MAC address. (If a port address is available, the port MAC address is used; otherwise, the device bridge MAC address is used.)
- Type: indicates the packet Type, which is 0xAAA-0300-0000-88cc.
- Data: indicates the Data content, which is LLDPDU.
- FCS: frame check sequence, used to verify packets.

2. LLDPDU

An LLDPDU is a data unit that encapsulates the data part of an LLDP packet.Before composing LLDPDU, the device encapsulates the local information into TLV format, and then combines several TLVS into an LLDPDU,

which is encapsulated in the data part of the LLDP packet for transmission.

Figure 3-148 LLDPDU encapsulation format

As shown in Figure 3-148, the four TLVS, the dark blue Chasis ID TLV, Port ID TLV, Time To Live TLV, and End of LLDPDU TLV, are required To be carried by each LLDPDU, while the remaining TLVS are optional.Each LLDPDU can carry up to 28 TLVS.

3. TLV

TLVS are the units that make up the LLDPDU, and each TLV represents a message.The TLVS that LLDP can encapsulate include basic TLVS,
802.1 Organization Defined TLV, 802.3 Organization Defined TLV, and LLDP-MED (Media Endpoint Discovery) TLV.
Basic TLVS are a set of TLVS for network device management. TLVS defined by 802.1 organization, TLVS defined by 802.3 organization, and TLVS defined by LLDP-MED are TLVS defined by standards organizations or other organizations to enhance the management of network devices. You can choose whether to send the TLV in LLDPDU based on actual needs.

(1) Basic the TLV

Among the basic TLVS, there are several TLVS that are required to implement LLDP functionality, that is, they must be published in LLDPDU, as shown in Table 3-25.

Table 3-25 Basic TLVS

The TLV name	instructions	Must publish or not
Chassis ID	The bridge MAC address of the sending device	is
Port ID	Identifies the port of the LLDPDU sender.If LLDPDU carries an LLDP-Med TLV, its The content is the MAC address of the port. If there is no port MAC, use the bridge MAC.Otherwise, its content is The name of the port	is
Time To Live	Time to Live The time this device information is alive on the neighbor device	is
End of LLDPDU	The end of LLDPDU identifier, which is the last TLV of LLDPDU	is
Port Description	Description of the port	no
System Name	Name of the device	no
System Description	Description of the system	no
System Capabilities	The main functions of the system and the function items that are enabled	no
Management Address	Manage the address, and the interface number and OID (Object Identifier) used to change the address.	no

(2) The 802.1 organization defines TLV

The IEEE 802.1 organization defines TLV as shown in Table 3-26.

Table 3-26 TLVS defined by the IEEE 802.1 organization

The TLV name	instructions

Port VLAN ID	PVID (Port VLAN ID) of a Port. Each LLDPDU carries more than one TLV of this type
Port And Protocol VLAN ID	Port and Protocol VLAN ID (PPVID) of a Port. One LLDPDU can carry multiple ports that are not connected to each other Duplicate TLVS of this type
VLAN Name	VLAN name of the VLAN to which the port belongs. One LLDPDU can carry multiple mutually exclusive TLVS of this type
Protocol Identity	Protocol Identity Supported by the port. An LLDPDU can carry multiple mutually exclusive TLVS of this type
DCBX	Data Center Bridging Exchange Protocol

(3) 802.3 Organizations define TLVS
The IEEE 802.3 organization defines TLV as shown in Table 3-27.

Table 3-27 TLVS defined by the IEEE 802.3 organization

The TLV name	instructions
MAC/PHY Configuration/Status	Rate and duplex status supported by the port, whether port rate auto negotiation is supported, whether auto negotiation is enabled, and the current rate and duplex status
Power Via MDI	Power supply capabilities of ports, including Power over Ethernet (PoE) types (PSE (Power Sourcing Equipment) or PD (Powered Device)), remote Power supply mode of PoE port, whether PSE Power is supported, Whether the PSE power supply is enabled and the power supply mode is controllable
Link Aggregation	Whether the port supports link aggregation and whether link aggregation is enabled
Maximum Frame Size	The Maximum Transmission Unit (MTU) configured for the port is the Maximum frame size supported by the port. Large transmission unit)
Power Stateful Control	The power status control of a port includes the power type used by the PSE/PD and the power supply/receiving priority And the power supplied/received

Our products currently do not support TLV for PoE related parts.

note

(3) LLDP-MED TLV

Lldp-med TLV provides many advanced applications for VoIP (Voice over IP), including basic configuration, network policy configuration, address information, directory management, etc. It meets the requirements of different manufacturers of Voice devices in terms of cost effectiveness, easy deployment, and easy management. It also solves the problem of deploying voice devices in Ethernet, and provides convenience for the manufacturers, sellers and users of voice devices.The contents of LLDP-MED TLV are shown in Table 3-28.

Table 3-28 LLDP - MED the TLV

The TLV name	instructions
LLDP-MED Capabilities	Type of LLDP-MED TLV supported by the network device
Network Policy	VLAN type, VLAN ID, Layer 2 and layer 3 and specific application of the port on the network device or terminal device Type, related priority, etc

Extended Power-via-MDI	Extended Power supply capabilities for network devices or end devices that extend the Power Via MDI TLV
Hardware Revision	Hardware version of the terminal device
Firmware Revision	Firmware version of the terminal device
Software Revision	Software version of the terminal device
Serial Number	Serial number of the terminal device
Manufacturer Name	Manufacturer name of the terminal device
Model Name	The module name of the terminal device
Asset ID	The asset identifier of the terminal device for directory management and asset tracking
Location Identification	Location identification information for network devices to be used by end devices in location-based applications

note

Our products do not support VoIP related TLV.

(4) Management address

The management address is the address used by the network management system to identify and manage network devices.The management address can clearly identify a device, which facilitates the drawing of network topology and facilitates network management.The Management Address is encapsulated in the Management Address TLV of LLDP packets and advertised.

3.7.1.3 LLDP Working Mechanism

1. LLDP working mode

LLDP works in the following four modes:

- TxRx: Both sends and receives LLDP packets.
- Tx: sends LLDP packets but does not receive LLDP packets.
- Rx: receives but does not send LLDP packets.
- Disable: neither sends nor receives LLDP packets.

When the LLDP working mode of a port changes, the port initializes the protocol state machine.To avoid constant port initialization due to frequent changes in the port's working mode, you can configure the port initialization delay time. When the port's working mode changes, the port initialization is delayed for a certain period of time.

2. LLDP packet sending mechanism

When a port works in TxRx or Tx mode, the device periodically sends LLDP packets to neighboring devices.If the local configuration of the device changes, the device immediately sends LLDP packets to notify the neighbor of the change of local information.To prevent a large number of LLDP packets from being sent due to frequent changes in local information, you need to delay the sending of each LLDP packet for a period of time before sending the next one. When the working mode of the device changes from Disable/Rx to TxRx/Tx or a new neighbor device is discovered

(that is, a new LLDP packet is received and information about the device that sends the LLDP packet is not saved locally), the device automatically enables the fast sending mechanism. That is, the interval for sending LLDP packets is shortened to one second. And continuously sends a specified number of LLDP packets and then returns to the normal sending interval.

3. LLDP packet receiving mechanism

When the port works in TxRx or Rx mode, the device checks the validity of the LLDP packet and the TLV it carries. After the check, the device saves the neighbor information To the local PC and then uses TTL (Time To Live,) in the Time To Live TLV. Time to Live) to set the aging time of the neighbor information on the local device. If the value is zero, the neighbor information is aged out immediately.

3.7.2 configuration LLDP

3.7.2.1 LLDP Configuration Task Overview

steps	Configuration tasks	instructions
1	Configure the global LLDP function	Enable the global LLDP function and set global LLDP parameters The global LLDP function is disabled by default and is mandatory
2	Configure the port LLDP parameters	Configure parameters related to the port LLDP function, including LLDP management status, Chassis Subtype, Port ID Subtype, Management Address Subtype, and the TLV allowed to advertise Type, optional
3	View port information	Optionally, view LLDP local information, neighbor information, statistics, and status information for a specified port
4	To view statistics	View global LLDP local information and statistics, optional
5	Check neighbor information	View global LLDP neighbor information, that is, LLDP information received from neighbors that neighbors group together Weave the TLV to send to the current device, which is optional

3.7.2.2 Configuring the global LLDP function

On the navigation bar, choose Switch > LLDP. The Global LLDP configuration page is displayed, as shown in Figure 3-149. Table 3-29 describes the parameters.→

Figure 3-149 LLDP Global configuration screen

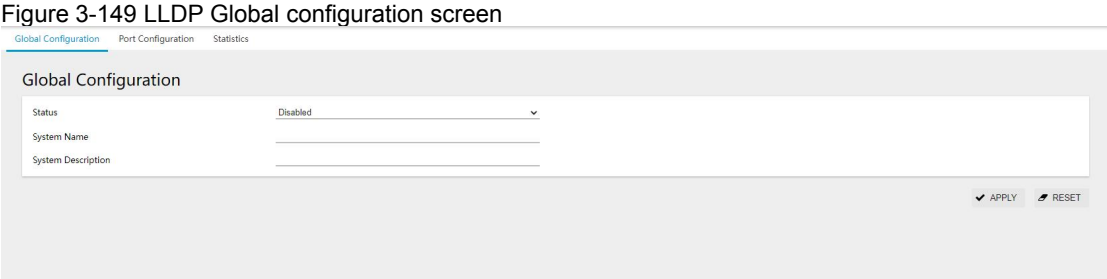


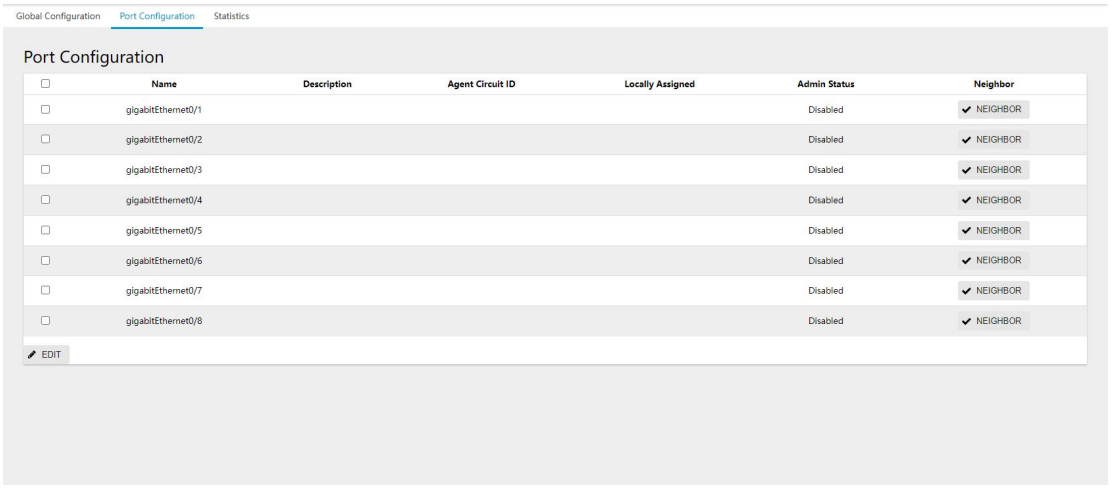
Table 3-29 LLDP Global configuration parameters

Configuration items	instructions
state	Disabled: Global enable Disabled Enabled: global enable
System name	The name of the device, which can be empty
System description	Description of the system, which can be empty

3.7.2.3 Configuring Port LLDP Parameters

Step 1: On the current screen, click the Ports TAB in the upper right corner to enter the LLDP Port configuration overview screen, as shown in Figure 3-150.

Figure 3-150 LLDP Port Configuration Overview



Step 2: Select the port to be configured and click Edit to enter the port configuration page, as shown in Figure 3-151. Table 3-30 lists the port configuration parameters.

Figure 3-151 LLDP port configuration page

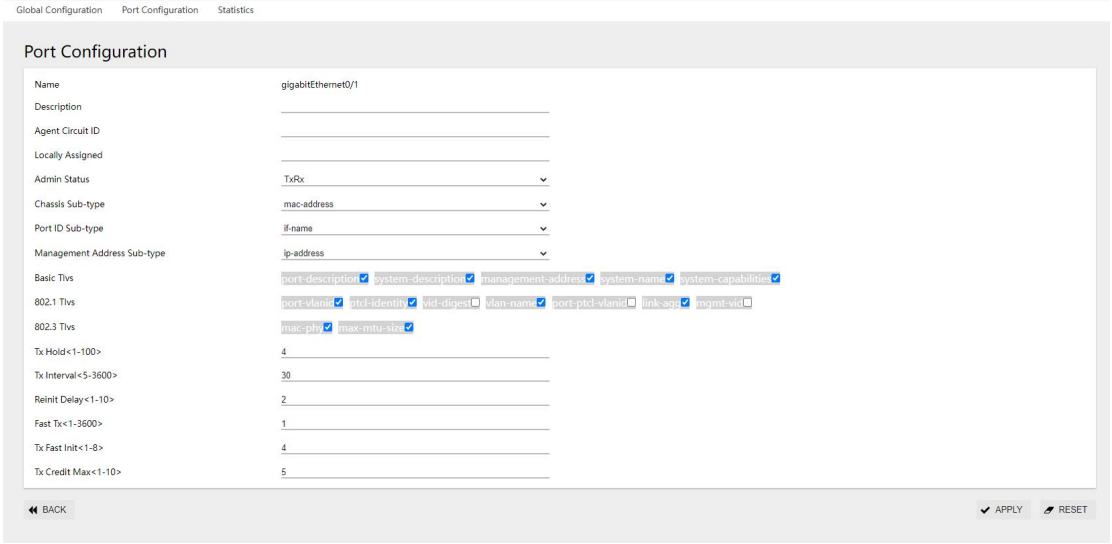


Table 3-30 LLDP port configuration parameters

Configuration items	instructions
describe	Displays the name of the LLDP port currently configured
Agent Circuit ID	Agent Circuit ID
Locally Assigned	Local configuration
Manage state	Disabled: Neither sends nor receives LLDPDU TxOnly: only sends LLDPDU but does not receive LLDPDU RxOnly: LLDPDU is received but not sent TxRx: Both sends and receives LLDPDU
Chassis Subtype	Mac-address: indicates a Mac address If-alias: indicates the interface alias If-name: indicates the interface name Ip-address: indicates the Ip address Territory-assigned: indicates the local configuration
Port ID Subtype	Mac-address: indicates the Mac address If-alias: indicates the interface alias If-name: indicates the interface name

	Ip-address: indicates the Ip address Agt-circuit-id: indicates the proxy circuit ID Locally-assigned: indicates the local configuration
Management Address Subtype	Mac-address: Mac address of the device Ip-address: indicates the device Ip address
Basic TIvs	Port-description: Port descriptor System-description: system descriptor Management-address: management address The system - the name: system name System-capabilities: system capabilities
802.1 TIvs	The port - vlanid: port vlanid PTCL - identity: protocol id Vid - digest: vid in this paper Vlan - name: name of vlan Port-ptcl-vlanid: specifies the vlanid of the port protocol Link-agg MGMT-VID: link aggregation management VID
802.3 TIvs	mac-phy:mac-phy Max-mtu-size: maximum MTU value
Tx hold	Transmission hold, the default value txFastInit is 4, which is used for packet TTL calculation;TTL=msgTxInterval * msgTxHold + 1
Tx interval	Transmission interval, the default value is 30 s; The administrator can change this value to anything between 5 and 3600.
Reinit delay	Represents the amount of delay between adminStatus changing to "Disabled" and trying to reinitialize. The default value for reinitDelay is 2 s.
Fast tx	Defines the time interval between the timer intervals between transmissions within a fast transmission cycle (i.e. txFast is not zero). The default value for msgFastTx is 1; Administrators can change this value to anything between 1 and 3600.
Tx fast init	This variable is used as the initial value of the txFast variable. This value determines the number of LLDPDU transmitted during the fast transmission cycle.
Tx credit max	Configure the maximum value of txCredit.The default value is 5. Administrators can change this value to anything in the range of 1 to 10.

3.7.2.4 Viewing statistics

On the current screen, click the Statistics TAB in the upper right corner to enter the LLDP statistics screen, as shown in Figure 3-152. Table 3-31 describes the parameters.

Figure 3-152 LLDP statistics page

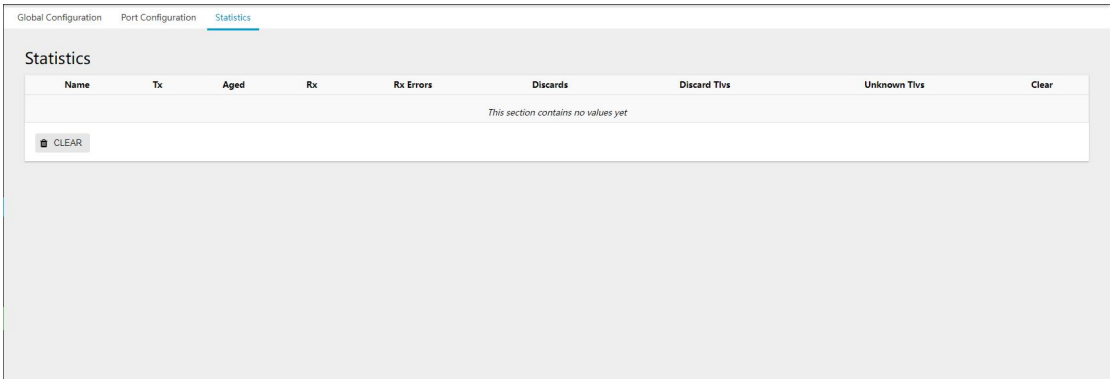


Table 3-31 LLDP port configuration parameters

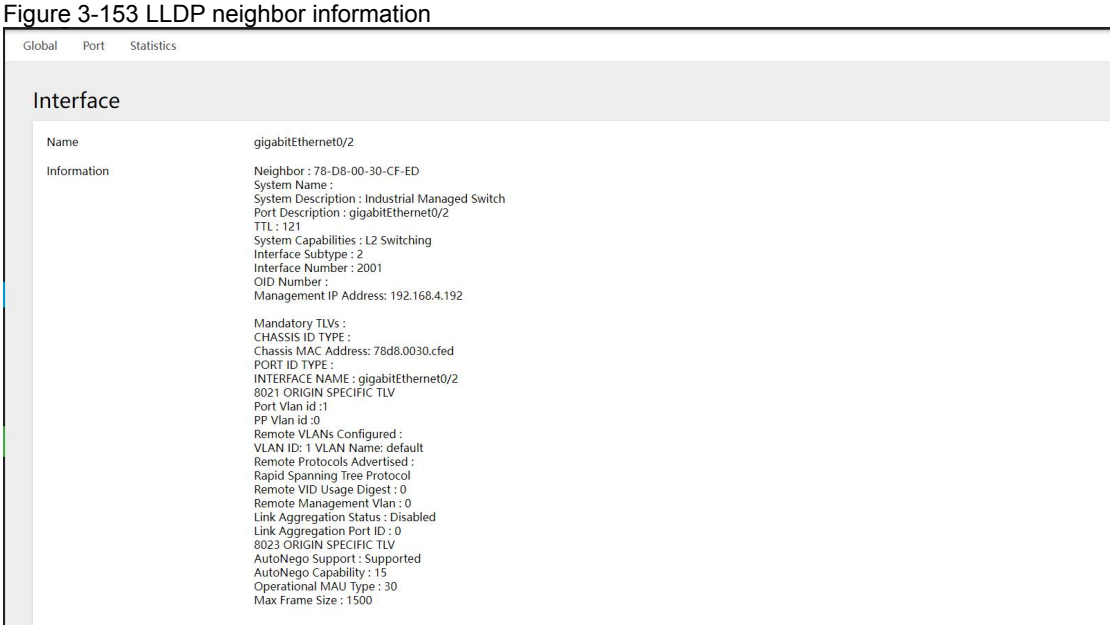
Configuration items	instructions
The name of the	Display interface name
Tx	Number of packets sent
Aged	Aged Packets
Rx	Number of received packets
Rx Errors	Number of receive errors
Discards	Number of discarded packets
Ddiscard TIvs	Discard the TIv number

Unknown TIvs	Unknown TLVS number
remove	Clear current count

3.7.2.5 Viewing Neighbor Information

On the Ports TAB page, click the Neighbor button of the corresponding port. The neighbor information page is displayed, as shown in Figure 3-153.

Figure 3-153 LLDP neighbor information



3.7.3 Configuration Examples

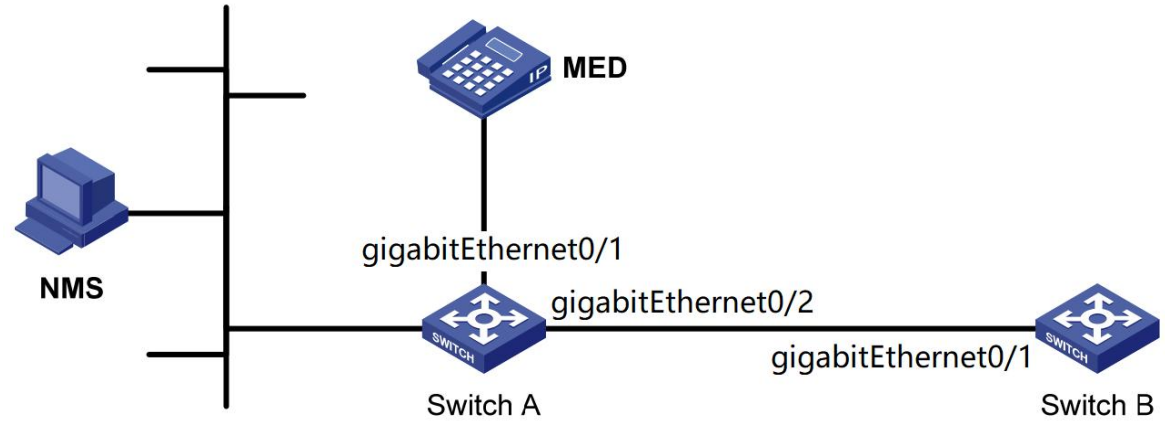
3.7.3.1 Networking Requirements

The Network Management System (NMS) is connected to Switch A through Ethernet
A is connected to the MED device through GigabitEthernet 0/0/1 and Switch B through GigabitEthernet 0/0/2.

• Configure the LLDP function on Switch A and Switch B so that the NMS can communicate between Switch A and MED

And the communication between the link between Switch A and Switch B.

Figure 3-154 Networking requirements



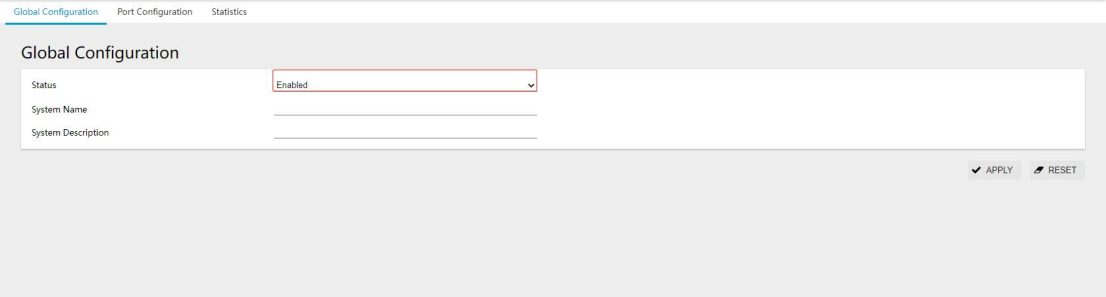
3.7.3.2 Configuration Procedure

Configure the Switch A

Step 1: Configure the global LLDP function.(In special cases, you can manually disable ports other than gigabitethernet0/0/1 and GigabitEthernet 0/0/2).

Click Switch [LLDP] on the navigation bar to enter the LLDP global configuration page.→Select "Enabled" and click "Apply" to turn on the LLDP global switch, as shown in Figure 3-155.

Figure 3-155 LLDP global configuration



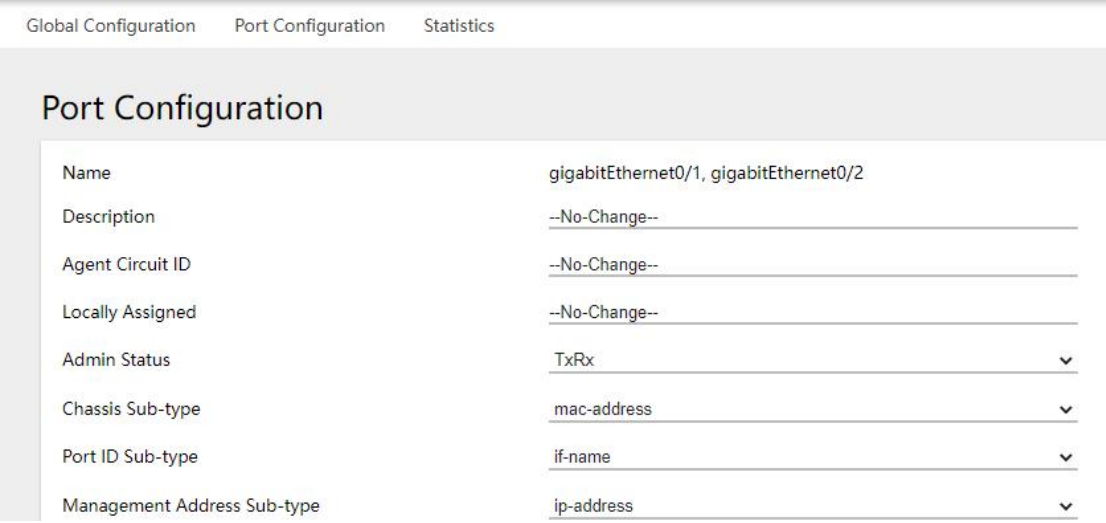
Step 2: Configure LLDP mode to Rx for ports GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2.
On the current interface, click the [Ports] TAB in the upper left corner to enter the LLDP port configuration interface. Select GigabitEthernet0/ and GigabitEthernet 0/0/2, and click the [Edit] button to enter the interface for configuring LLDP ports in detail, as shown in Figure 3-156. Select "RxOnly" for management status.
Step 3: Click the [Apply] button to complete the configuration.
Step 4: Click the "Save" button in the navigation bar to save the current configuration.

Configure the Switch B

Step 1: Enable LLDP globally

Step 2: Configure port GigabitEthernet 0/1 to TxOnly.
Step 3: Click Apply to complete the configuration.
Step 4: Click the "Save" button in the navigation bar to save the current configuration.

Figure 3-156 Configuring LLDP parameters for ports



4 Safety

4.1 ACL

4.1.1 ACL Overview

ACL (Access Control List, access control list) realizes the function of packet filtering by configuring matching rules and processing operations for packets.
It can effectively prevent illegal users from accessing the network, and at the same time can control the flow and save network resources. The packet matching rules defined by ACL can also be referenced by other functions that need to distinguish traffic, such as the definition of traffic classification rules in QoS.
ACL classifies data packets through a series of matching conditions. These conditions can be SMAC, DMAC, SIP, DIP, etc. of the data packet.
According to matching conditions, ACLs can be divided into the following types:
Standard IP-based ACL: Only formulate rules based on the source IP address of the data packet.
IP-based extended ACL: formulate rules based on the source IP address, destination IP address, ETYPE, and protocol of the data packet.
MAC-based ACL: Formulate rules based on the source MAC address and destination MAC address of the packet.
Nameable ACL: The rules are the same as the IP-based standard ACL and extended ACL.

4.1.2ACL Configuration

- A maximum of 128 rules can be configured under a single ACL-ID; due to hardware resource limitations, a single device supports a maximum of 500 rules.
- When the ACL has been applied to the port, if you need to add or delete rules, you need to remove the application from the port first.

The ACL module provides configurations based on ACL types, including IP, IP-Extend, MAC-Extend, IP-Named, and IP-Named-Extend. The ACL configuration interface is shown in Figure 4-1~5, and the description of each parameter is shown in Table 4-1~5.

Figure 4-1 ACL IP Configuration Interface

Table 4-1 ACL IP Parameter Description

Configuration Items		Instructions
ACL type	IP	ACLs of standard IP that match the source IP fields in IPv4 messages
Name		The number <1, 99> or <1300, 1999>
Type	Permit	Release the message hitting the rule
	Deny	Discard messages that hit the rule
Source Address		Source IP address, such as 192.168.64.1
Source Mask		The mask of the IP is reversed, such as matching the first 24 bits of the IP address, the mask is 255.255.255.0, and it needs to be configured as 00.00.00.255

Figure 4-2 ACL IP-Extend Configuration Interface

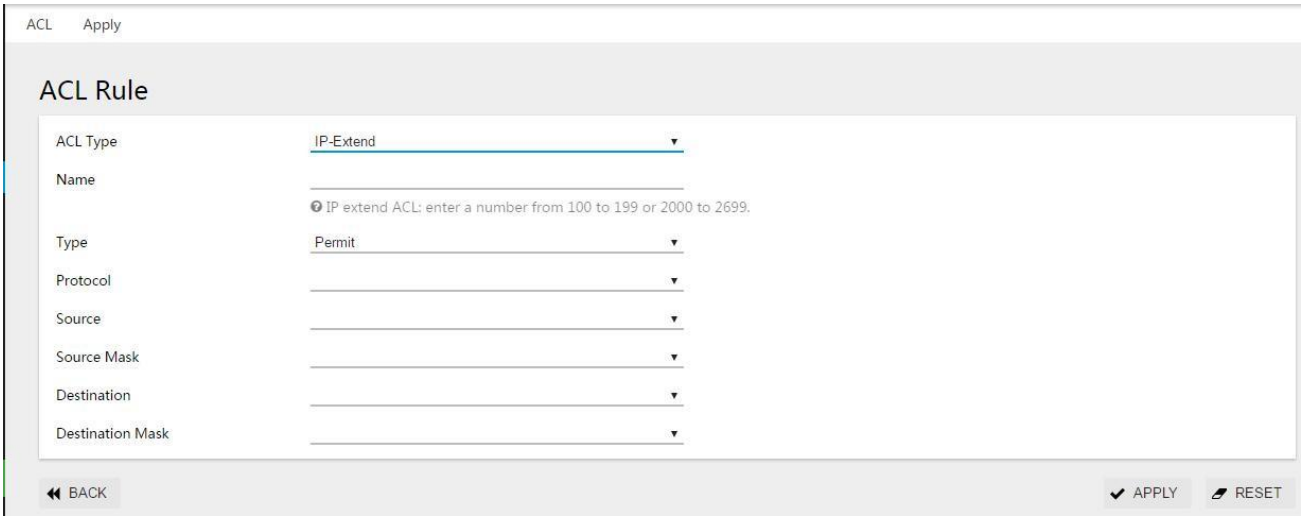


Table 4-2 IP-Extend Parameter Specification

Configuration Items		Instructions
ACL type	IP	Extend the ACL to match the protocol number, source IP address, and destination IP address of IPv4 messages
Name		The number <100, 199> or <2000, 2699>
Type	Permit	Release the message hitting the rule
	Deny	Discard messages that hit the rule
Agreement		Support common protocol message options, including tcp, udp, vrrp, igmp, gre, ipcomp, ospf, pim, rsvp, etc.

	Support all IPv4 packets Support IPv4 packets of custom protocol
Source Address	Source IP address, such as 192.168.64.1
Source Mask	The mask of the IP is reversed, such as matching the first 24 bits of the IP address, the mask is 255.255.255.0, here it needs to be configured as 00.00.00.255
Target Address	Destination IP address, such as 192.168.64.100
Target Mask	Homology mask

Figure 4-3 ACL Mac-Extend Configuration Interface

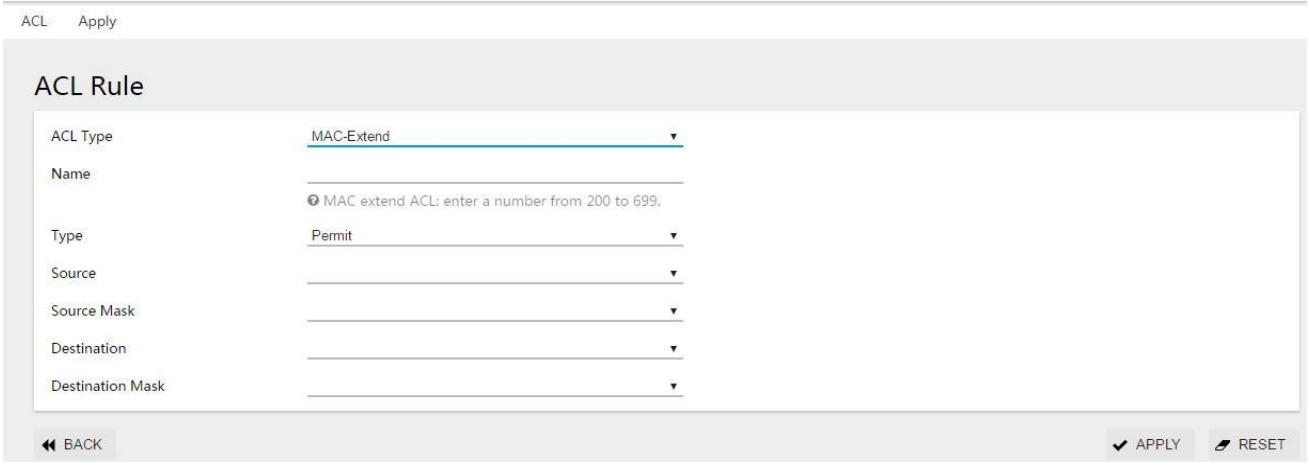


Table 4-3 ACL MAC-Extend Parameter Specification

Configuration Items		Instructions
ACL type	MAC -Extend	Extended MAC ACL to match the source and destination MAC addresses of the Layer 2
Name		The number < 200,699 >
Type	Permit	Release the message hitting the rule
	Deny	Discard messages that hit the rule
Source address		Source MAC address, such as 00. D0. F8.22.33.40
Source mask		The MAC address mask is inverted. If it matches the first 24 bits of the MAC address, the mask is ffff.ff00.0000, which needs to be configured as 0000.00ff.ffff
Target Address		Destination MAC address, such as 00. D0. F8.22.33.41
Target mask		Homology mask

Figure 4-4 ACL IP-Named Configuration Interface

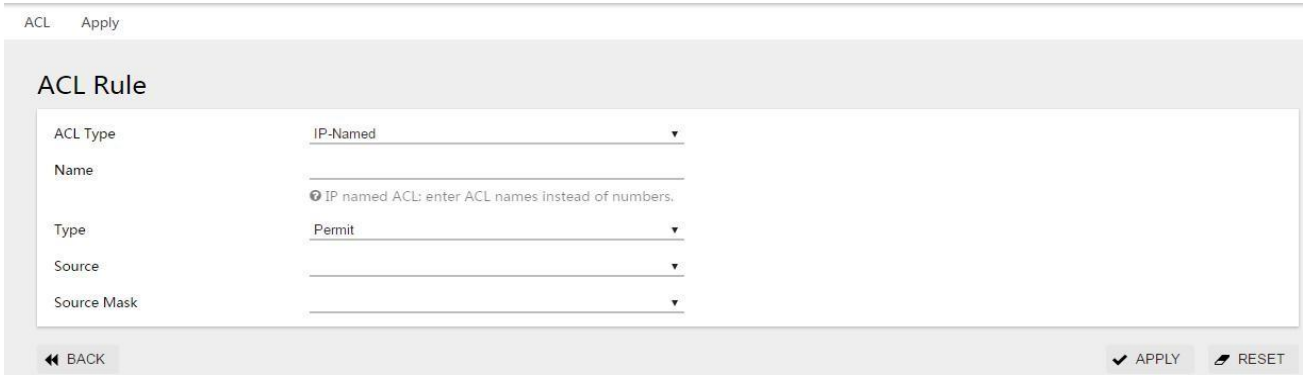


Table 4-4 ACL IP-Named Parameter Description

Configuration items		Instructions
ACL type	IP-Named	Standard ACL, support name naming, the first character must be a letter
Name		A string that begins with a letter
Type	Permit	Release the message hitting the rule
	Deny	Discard messages that hit the rule
Source Address		Source IP address, such as 192.168.64.1
Source Mask		The mask of the IP is reversed, such as matching the first 24 bits of the IP address, the mask is 255.255.255.0, and it needs to be configured as 00.00.00.255

Figure 4-5 ACL IP-Named-Extend Configuration Interface

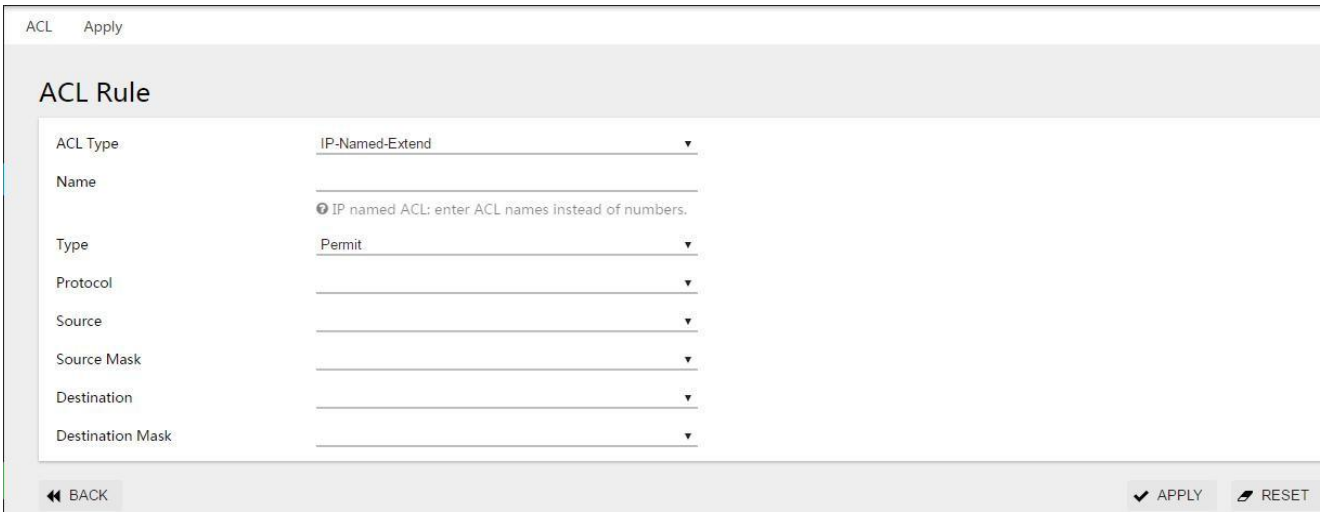


Table 4-5 ACL IP-Named-Extend Parameter Description

Configuration Items		Instructions
ACL type	IP-Named-Extend	Extend ACL, support name naming, the first character must be a letter
Name		A string that begins with a letter
Type	Permit	Release the message hitting the rule
	Deny	Discard messages that hit the rule
Agreement		Support common protocol message options, including TCP, udp, VRRP, igmp, gre, ipcomp, ospf, pim, RSVP, etc. Support all IPv4 messages Support IPv4 packets of custom protocol
Source Address		Source IP address, such as 192.168.64.1
Source Mask		The mask of the IP is reversed, such as matching the first 24 bits of the IP address, the mask is 255.255.255.0, and it needs to be configured as 00.00.00.255
Target Address		Destination IP address, such as 192.168.64.100
Target Mask		Homology mask

Operation steps:

(1) Select ACL in the menu [Security] to enter the ACL configuration interface.

(2) Select the ACL tab and click the [Add] button to enter the ACL rule interface.

(3) Fill in the parameters as required, and click the [Apply] button to save.

(4) Select the [Application] tab bar to enter the ACL application interface. Select the corresponding entry number in the corresponding port, and click the [Apply] button to make the configuration effective.

(5) Click the [Save] button in the menu to save the configuration.

4.1.3 Configuration Example

Configuration Example:

Case requirements: For ports eth0/1 and eth0/3, the source IP address range 192.168.0.1/24 network segment IPv4 packets are allowed, and all other IPv4 packets are discarded.

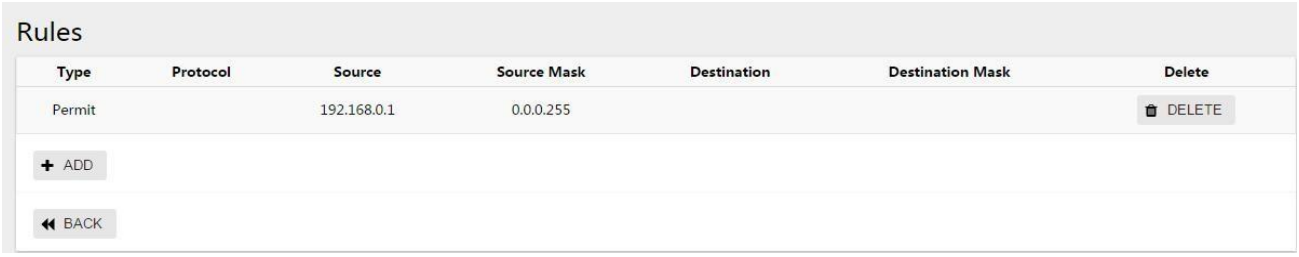
Step 1: Create standard IP ACL rule 1

Click [Security]→ACL in the menu to enter the ACL configuration interface. Click the [Add] button, as shown in Figure 4-1, ACL type "IP" name "1", type "permit", matching IP: "192.168.0.1", mask 255.255.255.0, inverted to "0.0. 0.255"

Figure 4-1 Create ACL Rules

Click the [Apply] button to automatically return to the main ACL configuration interface, as shown in Figure 4-2, you can see the successfully created ACL rules.

Figure 4-2 Create Successful ACL Rule



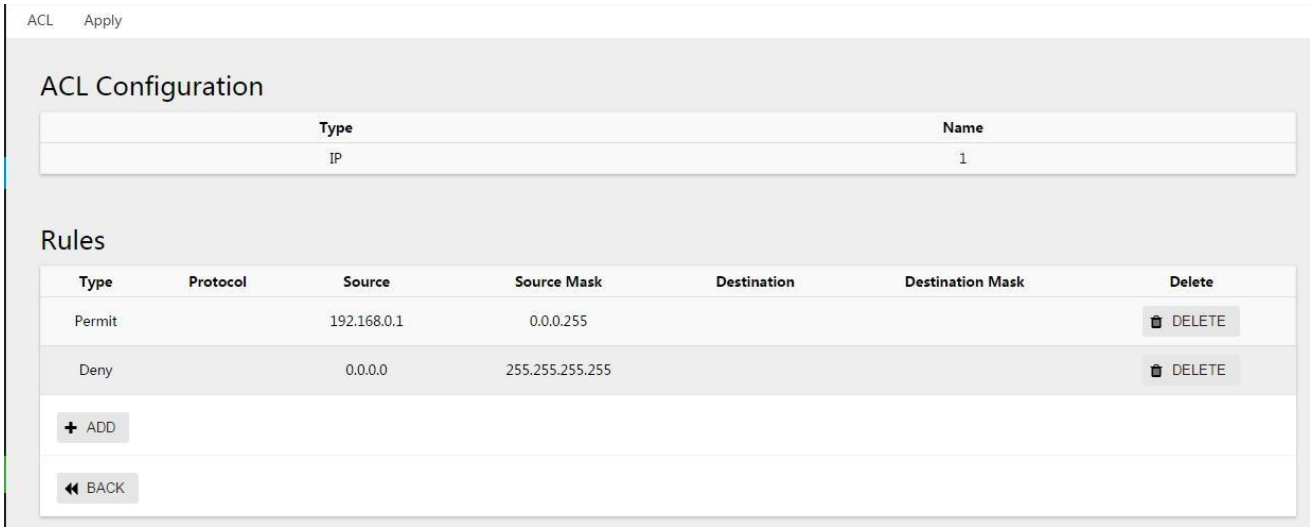
Step 2: Create standard IP ACL rule 2

Under the rule list, click the [Add] button to add a matching rule, as shown in Figure 4-3, type "deny", source IP "0.0.0.0", source mask "255.255.255.255". Click the [Apply] button to automatically return to the main ACL configuration interface, as shown in Figure 4-2, you can see the successfully created ACL rules.

Figure 4-3 Create ACL Rules

Click the [Apply] button to automatically return to the main ACL configuration interface, as shown in Figure 4-4, you can see the successfully created ACL rules.

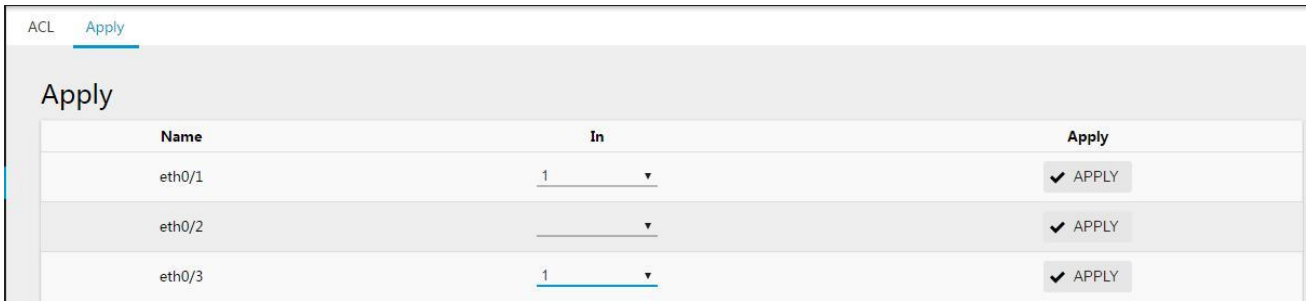
Figure 4-4 Create Successful ACL Rule



Step 3: Apply ACL rules to the port.

As shown in Figure 4-5, click [Apply] in the tab bar, select "1" for the ports eth0/1 and eth0/3 that need to enable ACL rules, and click the [Apply] button to make the rule effective.

Figure 4-5 Port Opening ACL Rules



Step 4: click the "save" button in the menu to save the configuration.

4.2 QoS

4.2.1 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.

A device that supports 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 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.

4.2.2 QoS Configuration

instructions

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

The QoS module provides QoS global configuration, port trust, CoS mapping, DSCP mapping, policy and other configurations. The configuration interface is shown in Figure 4-6~10, and the detailed parameter description is shown in Table 4-6~10:

Figure 4-6 QoS Profile Configuration Interface

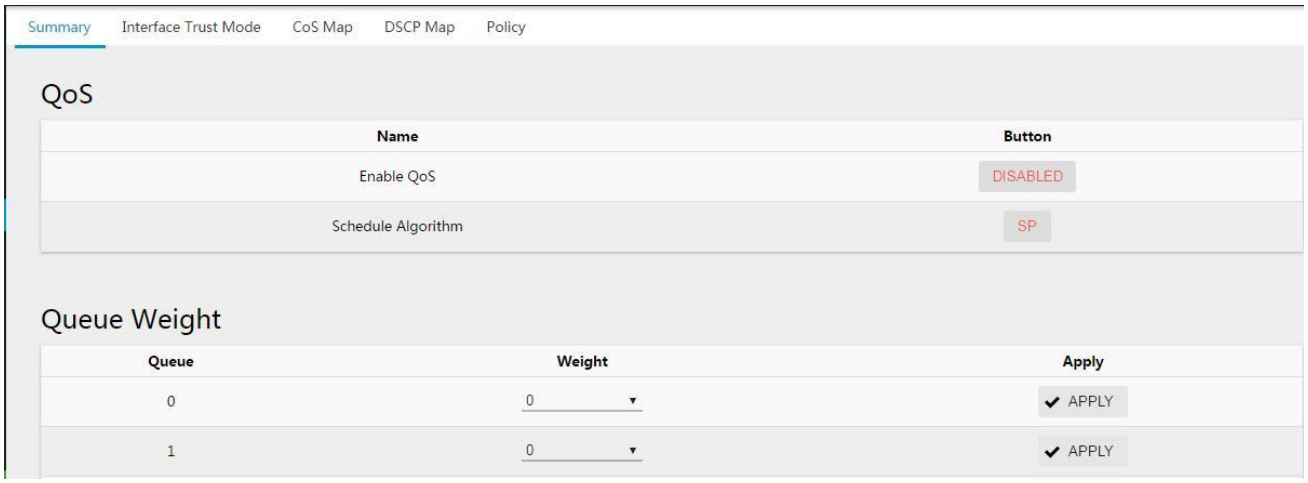


Table 4-6 QoS Overview Parameter Description

Configuration Items		Instructions		
General Description	QoS	Enable the QoS	Enable	Enable QOS. All QOS functions are not configured until enabled
			Disable	Disable QOS. When QOS is disabled, remove all QOS configurations
		Scheduling Algorithm	Sp	Absolute priority scheduling, the queue ID is large, the priority is high, the low priority queue is processed after the high priority queue is processed
			Wrr	The round-robin scheduling algorithm, according to the queue weight, schedules each queue in turn from the largest to the smallest queue ID.
	Queue Weight	Queue		< 0, 7 >
		Weight		<0, 32>, the larger the value, the higher the weight, and the greater the probability of priority processing of packets in this queue under channel congestion, 0 means infinity

Figure 4-7 QoS Port Trust Configuration Interface

Table 4-7 QoS Port Trust Parameters Description

Configuration Items		Instructions
Port Trust	Name	port
	Default CoS	<0, 7>, when the port is configured to be untrusted, or the message is configured to be trusted but the message does not meet the trust condition, the port default cos is used to mark the ingress message
	Trust	Support distrust, trust cos, trust dscp configuration. When in the no trust mode, the ingress phase modifies the cos field and dscp field of the message according to the port default cos; when the trust cos is configured, for the untagged message, the no trust mode is the same. For the tagged message, select the message with cos; When configuring trust dscp, for ip packets, select the packet with dscp, and for non-ip packets, it is the same as trust cos mode.
	Application	Click configure to take effect

Figure 4-8 QoS CoS Mapping Configuration Interface

Table 4-8 QoS CoS Mapping Parameters Description

Configuration Items			
CoS Mapping	CoS	\	< 0, 7 >
	Queue	\	<0, 7>, Cos-queue mapping relationship, based on the port-marked cos, modify the message egress queue, and it will take effect when the port is configured as no trust, trust cos or trust dscp and non-ip messages.
	DSCP	\	The cos-dscp mapping relationship takes effect when the configured port is no trust, trust cos or trust dscp and non-ip packets, modify the dscp value of packets
	Application	\	Click configure to take effect

Figure 4-9 QoS DSCP Configuration Interface

Table 4-9 QoS DSCP Parameter Description

Configuration Items		Instructions	
DSCP Mapping	DSCP	\	< 0, 63 >
	Queue	\	<0, 7>, dsp-queue mapping relationship, effective when the port is configured as trust dscp and ip packets are configured, modify the packet egress queue
	CoS	\	<0,7>, dscp-cos mapping relationship takes effect when the port is configured as trust DSCP and IP message is configured, and the message cos field is modified
	New DSCP Values	\	<0,63>, dscp-dscp mapping relationship, effective when the port is configured as trust DSCP and IP message, dscp-dscp mapping, followed by dscp-cos mapping
	Application	\	Click configure to take effect

Figure 4-10 QoS Policy Configuration Interface

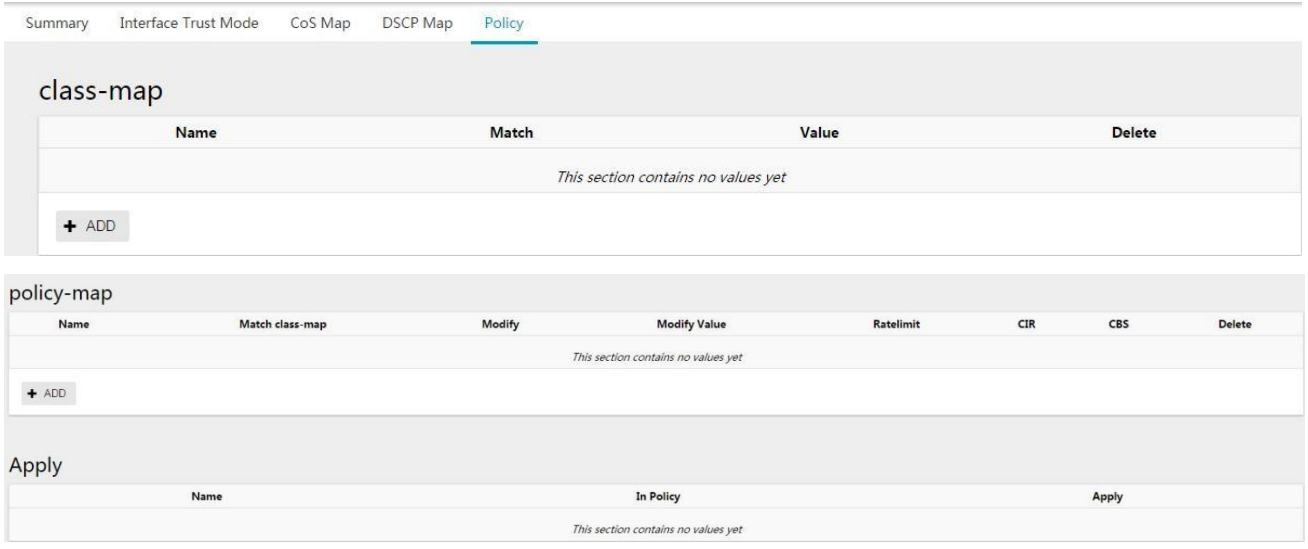


Figure 4-10 QoS Policy Parameters Description

Configuration Items		Instructions	
Policy	Class-map	Name	Create category, define category name
		Match	Define matching types and support associated ACLs; Support message matching of etype, dscp, cos, l4port, vlan field
		Value	The specific value corresponding to the flow matching type
		Delete	Delete category
	Policy-map	Name	Create policy, define policy name
		Match	class-map Select the class-map associated with the strategy
		Modify	the corresponding action 1 of the strategy, support modifying cos, dscp, vlan and other actions
		Modify Value	Strategy action one corresponding value
		Speed Limit	Action 2 corresponding to the policy, speed limit
		CIR	speed limit waterline in kbps
		CBS	burst capability, unit Kbyte
		Delete	Delete policy
	Application	Name	Port
		Entry Policy	Select the created policy
		Application	The policy is applied to the port to take effect

4.2.3 QoS Configuration Example

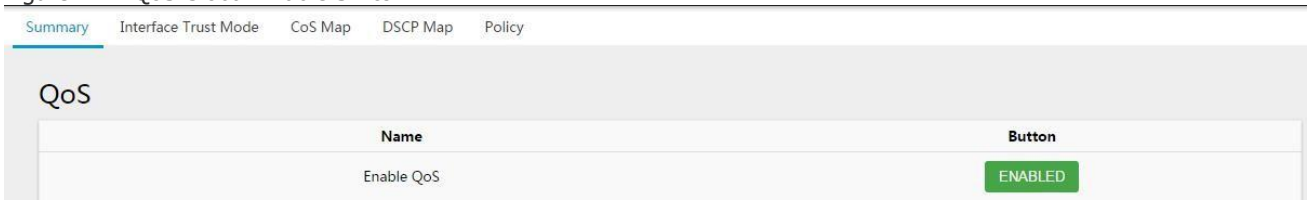
Configuration example 1:

Case requirements: limit the ingress rate of the flow whose source IP is 192.168.64.1 on port eth0/1, and limit the rate to 1024kbps.

Step 1: Enable QOS function globally

Select [Security]→QoS in the menu to enter the QoS configuration interface. As shown in Figure 4-11, click the [Overview] tab and click the [Disabled] button to enable the global QoS switch.

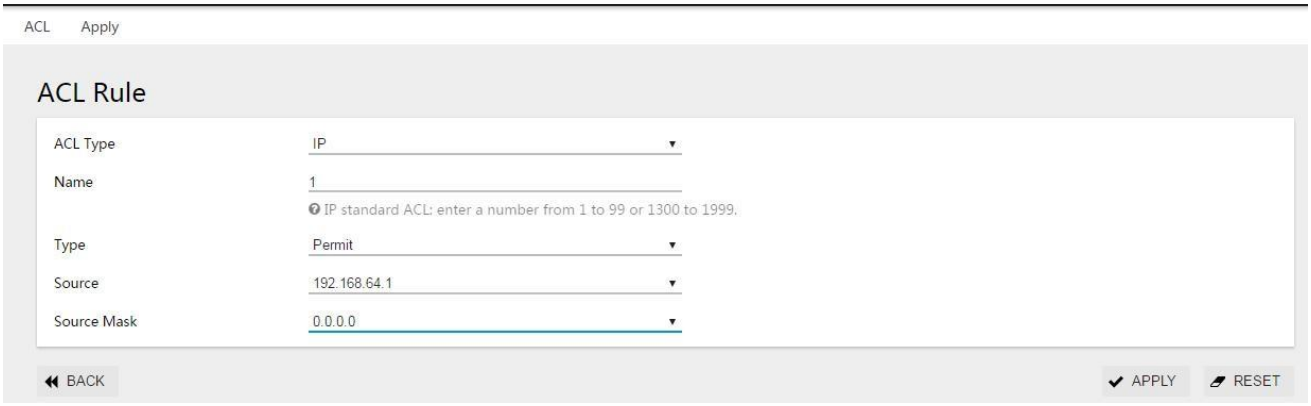
Figure 4-11 QoS Global Enable Switch



Step 2: Create standard ACL 1, matching source IP: 192.168.64.1, mask 255.255.255.255

Click [Security]→ACL in the menu to enter the ACL configuration interface. Click the [Add] button, as shown in Figure 4-12, the name is "1", the type is "permit", the matching IP is "192.168.64.1", the mask is "255.255.255.255", and the inverse is "0.0.0.0".

Figure 4-12 Create an ACL Rule



Step 3: Create classification c1, match ACL 1

Click [Security]→QoS in the menu to enter the QoS configuration interface. As shown in Figure 4-13, click the [Policy] tab to enter the QoS policy configuration interface.

Figure 4-13 QoS Policy Configuration Interface

Click "add" button to configure QoS policy according to figure 4-14.

Figure 4-14 QoS Policy Configuration Interface

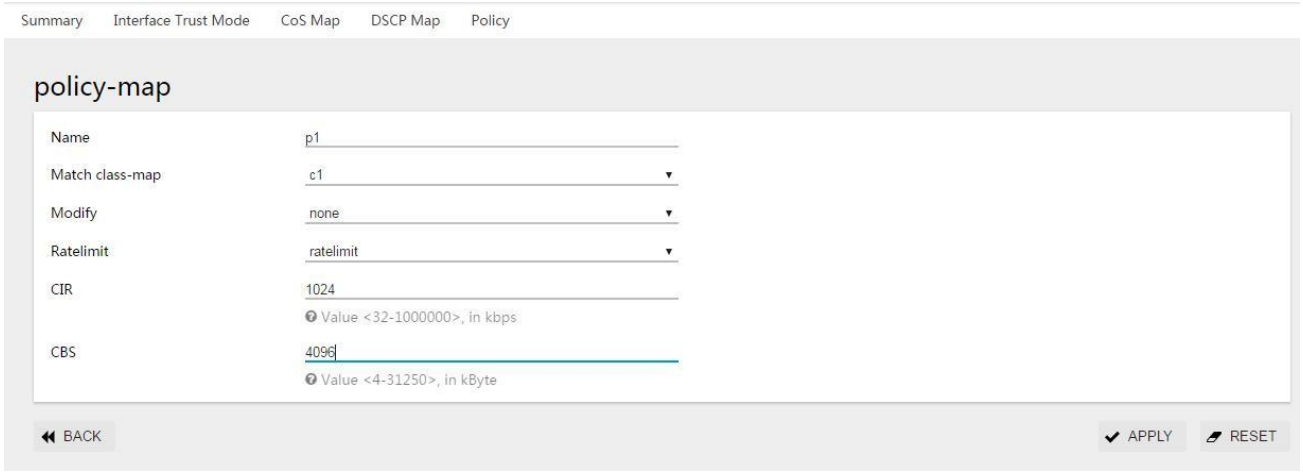
Click [Apply] to complete the configuration and return to the interface as shown in Figure 4-15.

You can see the successfully created rules.

Figure 4-15 QoS Policy Configuration Interface

Step 4: Create policy p1, associate category c1, and set the action 2 speed limit to 1024kbps
Under the current QoS policy interface, select the policy-map option, and click the [Add] button to enter the policy-map configuration interface. The specific configuration method is shown in Figure 4-16.

Figure 4-16 Policy-map Configuration Interface



Click [Apply] to complete the configuration and return to the interface as shown in Figure 4-17. You can see the successfully created strategy.

Figure 4-17 Policy-map Display Interface

Step 5: Policy p1 is applied on port eth0/1
Under the current QoS policy interface, select the application option, select the ingress policy of port eth0/1 as p1, and click the [Apply] button of the port, as shown in Figure 4-18.

Figure 4-18 QoS Policy Application Configuration Interface

Step 6: Click the [Save] button in the menu to save the configuration.
Configuration example 2:
Case requirements: In the case of network congestion, ensure normal forwarding of ingress packets on port eth0/2, and eth0/2 is the access port
Step 1: Enable QOS function globally
Select [Security] QoS in the menu to enter the QoS configuration interface. As shown in Figure 4-19, click the [Overview] tab and click the [Disabled] button to enable the QoS global switch.

Figure 4-19 QoS Global Enable Switch

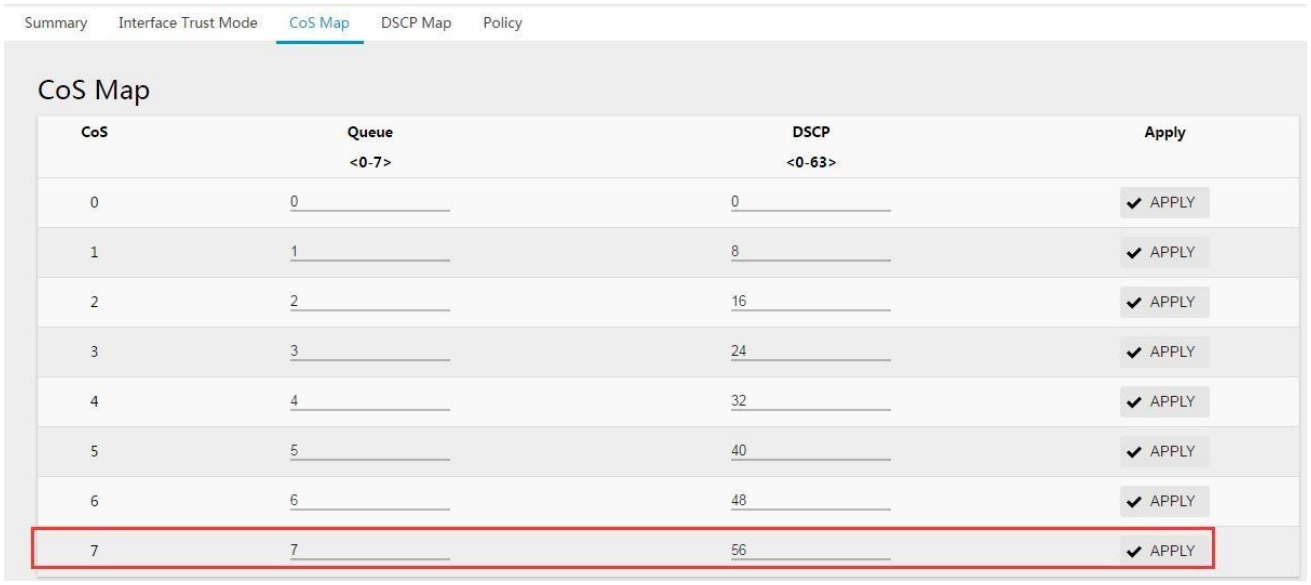
Step 2: Configure the default cos of the port of eth0/2 to 7, the port trusts cos, and the default cos of other ports is 0, which is not trusted by default.

In the current QoS configuration interface, click the [Port Trust] tab to enter the port trust configuration interface, as shown in Figure 4-20. The default CoS of port eth0/2 is "7", the trust is "cos", and other ports keep the default configuration.

Figure 4-20 Port Trust Configuration Interface

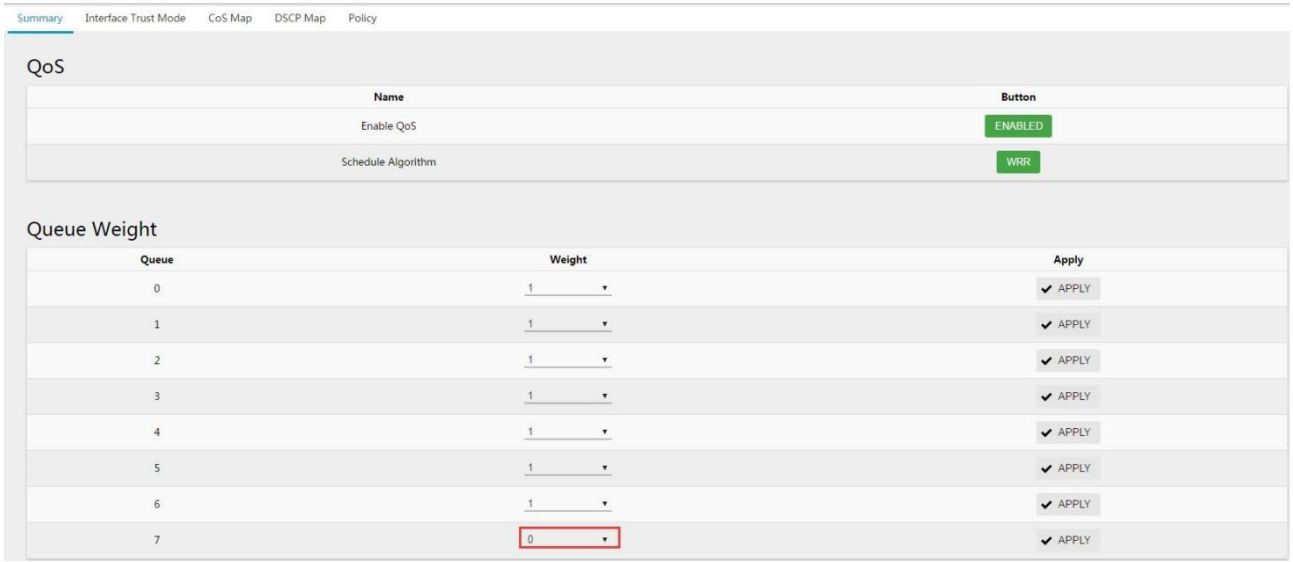
Step 3: Configure the queue mapping relationship, cos 7 mapping queue is 7
In the current QoS configuration interface, click the [CoS mapping] tab to enter the CoS mapping configuration interface, as shown in Figure 4-21, the mapping queue of cos 7 is selected as "7" and click the [Apply] button.

Figure 4-21 CoS Mapping Configuration Interface



Step 4: Configure the scheduling mode as wrr and configure the weight of queue 7 as 0
In the current QoS configuration interface, click the [Overview] tab, as shown in Figure 4-22. Under the QoS options, select the scheduling algorithm as "wrr" and the weight of queue 7 as "0".

Figure 4-22 QoS Overview Interface



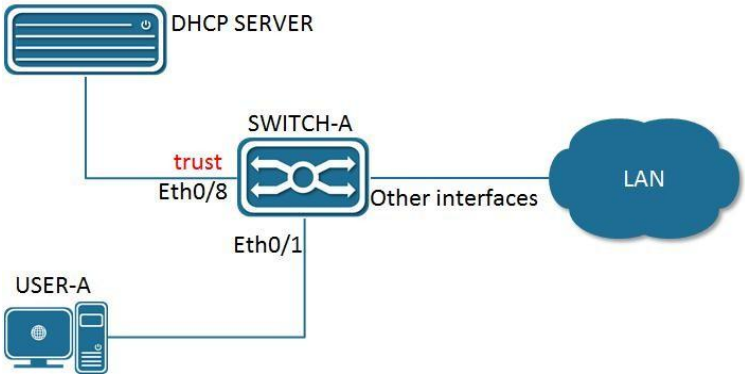
Step 5: Click the [Save] button in the menu to save the configuration.

4.3 DHCP Snooping

4.3.1 Overview

DHCP (Dynamic Host Configuration Protocol) is a local area network network protocol, which is widely used to dynamically allocate reusable network resources. It is a means for users or internal network administrators to centrally manage all computers. DHCP Snooping is a DHCP security technology. It can isolate illegal DHCP servers by detecting and managing DHCP exchange messages. DHCP Snooping divides ports into two types, TRUST port and UNTRUST port. The device only forwards the DHCP Offer messages received by the TRUST port, and discards all DHCP Offer messages from the UNTRUST port, thus realizing the shielding of illegal DHCP servers.

Figure 4-23 DHCP Application Topology



4.3.2 DHCP Snooping Configuration

Table 4-11 DHCP Snooping Global Enable Switches

Configuration Items	Instructions
Disable/enable	Global enable or disable DHCP Snooping
Disabled/enabled	Enable or disable DHCP Snooping for a specific port

Configuration steps:

(1) Select [Security] in the navigation to jump to the DHCP Snooping interface.

(2) Click the [Enable/Disable] button to turn on the DHCP Snooping function.

Figure 4-24 DHCP Snooping Global Enable Switches

(3) Select the corresponding port that needs to open this function, select enable, and click the [Apply] button to complete the configuration.

Figure 4-25 DHCP Snooping Trust Port Configuration

(4) Click the [Save] button in the menu to save the configuration.

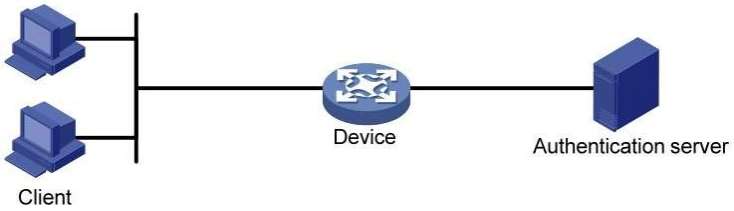
4.4 802.1 X authentication

4.4.1 Overview

Initially, the IEEE 802 LAN/WAN committee proposed the 802.1X protocol to solve the problem of wireless LAN network security. Later, the 802.1X protocol was widely used in Ethernet as a common access control mechanism of the local area network, mainly to solve the problems of authentication and security in the Ethernet.
The 802.1X protocol is a port-based network access control protocol, which authenticates the accessed user equipment on the port of the LAN access device so that the user equipment can control access to network resources.

4.4.1.1 802.1X architecture

The 802.1X system includes three entities: client (Client), device (Device) and authentication server (Authentication server), as shown in Figure 4-26.
Figure 4-26 802.1x Architecture



- The client is a user terminal device that requests to access the LAN, and it is authenticated by the device in the LAN. Client software that supports 802.1X authentication must be installed on the client.
- The device side is a network device that controls client access in the local area network. It is located between the client and the authentication server. It provides a port (physical port or logical port) for the client to access the local area network, and communicates with the server through interaction with the server. The connected client is authenticated.
- The authentication server is used to authenticate, authorize, and account for clients, usually a RADIUS (Remote Authentication Dial-In User Service) server. The authentication server verifies the legitimacy of the client according to the client authentication information sent by the device, and notifies the device of the verification result, and the device decides whether to allow the client to access. In some small-scale network environments, the role of the authentication server can also be replaced by the device side, that is, the device side performs local authentication, authorization, and accounting on the client.

4.4.1.2 802.1x control of ports

1. Controlled/uncontrolled ports

The port that the device provides for the client to access the LAN is divided into two logical ports: a controlled port and an uncontrolled port. Any frame arriving at this port is visible on both the controlled port and the uncontrolled port.

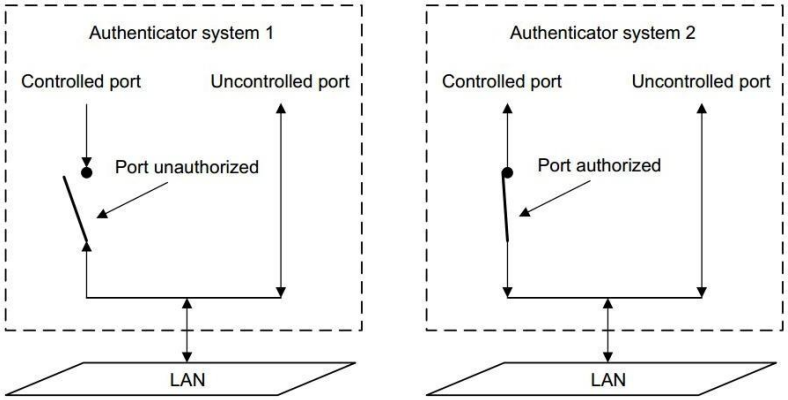
- Uncontrolled ports are always in a two-way connection state and are mainly used to transmit EAPOL (Extensible Authentication Protocol over LAN) protocol frames to ensure that the client can always send or receive authentication messages.
- The controlled port is in a two-way connection state in the authorized state, and is used to transmit business packets; in the unauthorized state, it is prohibited to receive any packets from the client.

2. Authorized/unauthorized status

The device uses the authentication server to authenticate the clients that need to access the LAN, and controls the authorization status of the controlled ports according to the authentication results (Accept or Reject).

Figure 4-27 shows the influence of different authorization states on the controlled port on the packets passing through the port. The figure compares the port status of two 802.1X authentication systems. The controlled port of system 1 is in an unauthorized state, and packets are not allowed to pass; the controlled port of system 2 is in an authorized state, and packets are allowed to pass.

Figure 4-27 Impact of Authorization Status on Controlled Ports



3. Controlled Direction

In an unauthorized state, the controlled port can be set to one-way controlled and two-way controlled.

- When in a two-way controlled state, frame sending and receiving are prohibited;
- When in a one-way controlled state, it is forbidden to receive frames from the client, but is allowed to send frames to the client.

instructions

The controlled port on our equipment can only be in a one-way controlled state.

4.4.1.3 802.1x Authentication Trigger Mode

The 802.1X authentication process can be initiated by the client or the device.

1. Client Active Trigger Mode

- Multicast trigger: The client actively sends an EAPOL-Start message to the device to trigger authentication. The destination address of the message is the multicast MAC address 01-80-C2-00-00-03.
- Broadcast trigger: The client actively sends an EAPOL-Start message to the device to trigger authentication. The destination address of the message is the broadcast MAC address. This method can solve the problem that the authentication device cannot receive the client authentication request because some devices in the network do not support the above-mentioned multicast message.

2. Device-side Active Trigger Mode

The device-side active trigger mode is used to support clients that cannot actively send EAPOL-Start messages, such as the 802.1X client that comes with Windows XP. There are two ways for devices to actively trigger authentication:

- Multicast trigger: The device actively multicasts Identity type EAP-Request frames to the client every N seconds (the default is 30 seconds) to trigger authentication.
- Unicast trigger: When the device receives a packet with an unknown source MAC address, it actively unicasts an Identity type EAP-Request frame to the MAC address to trigger authentication. If the device does not receive a response from the client within the set time period, it will resend the message.

4.4.1.4 802.1x Certification Process

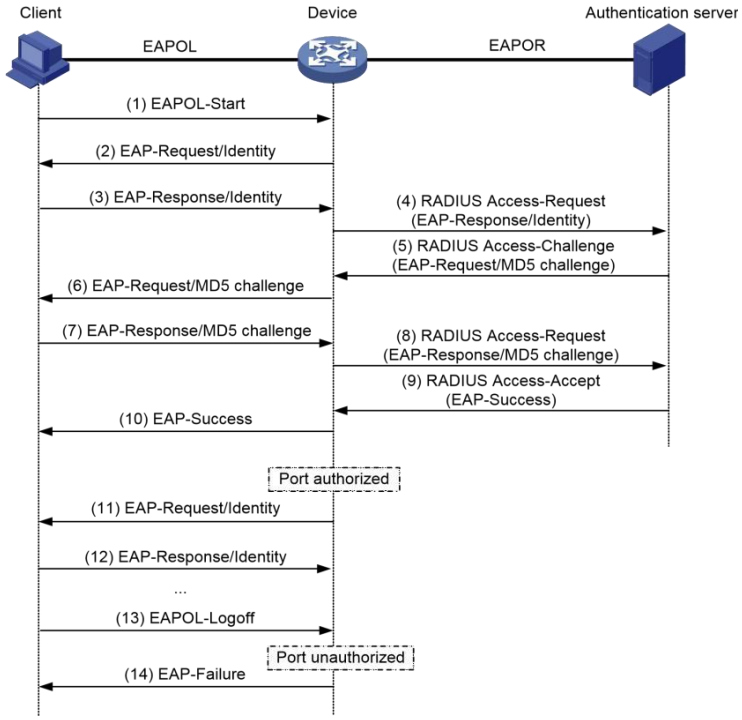
802.1X system supports the use of EAP relay mode and EAP termination mode to interact with the remote RADIUS server.

EAP relay

This method is stipulated by the IEEE 802.1X standard. EAP 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 RADIUS server is required to support EAP attributes: EAP-Message and Message-Authenticator are used to encapsulate EAP messages and protect RADIUS messages carrying EAP-Message, respectively.

The following takes the MD5-Challenge authentication method as an example to introduce the basic business process. The authentication process is shown in Figure 4-28.

Figure 4-28 EAP Relay Business Process for IEEE 802.1X Certification System



(2) When the user needs to access the external network, open the 802.1X client program, enter the user name and password that have been applied for and registered, and initiate a connection request. At this point, the client program will send an authentication request frame (EAPOL-Start) to the device to start an authentication process.

(3) After receiving the authentication request frame, the device will send an Identity type request frame (EAP-Request/Identity) to request the user's client program to send the entered user name.

(4) The client program responds to the request sent by the device and sends the user name information to the device via an Identity type response frame (EAP-Response/Identity).

(5) The device encapsulates the EAP message in the response frame sent by the client in a RADIUS message (RADIUS Access-Request) and sends it to the authentication server for processing.

(6) After receiving the user name information forwarded by the device, the RADIUS server compares the information with the user name list in the database, finds the password information corresponding to the user name, and encrypts the password with a randomly generated MD5 Challenge , And this MD5

The Challenge is sent to the device through RADIUS Access-Challenge packets.

(7) The device forwards the MD5 Challenge sent by the RADIUS server to the client.

(8) After the client receives the MD5 Challenge from the device, it uses the Challenge to encrypt the password, generates an EAP-Response/MD5 Challenge message, and sends it to the device.

(9) The device encapsulates this EAP-Response/MD5 Challenge packet in a RADIUS packet (RADIUS Access-Request) and sends it to the RADIUS authentication server.

(10) The RADIUS server compares the received encrypted password information with the local encrypted password information. If they are the same, the user is considered to be a legitimate user and sends an authentication pass message (RADIUS Access- Accept).

(11) After receiving the authentication pass message, the device sends an authentication success frame (EAP-Success) to the client, and changes the port to an authorized state to allow the user to access the network through the port.

(12) During the user's online period, the device side will monitor the user's online status by periodically sending handshake messages to the client.

(13) After receiving the handshake message, the client sends a response message to the device, indicating that the user is still online. By default, if the two handshake request messages sent by the device are not answered by the client, 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.

(14) The client can send an EAPOL-Logoff frame to the device to actively request to go offline.

(15) The device changes the port status from authorized status to unauthorized status, and sends an EAP-Failure message to the client.

instructions

In the EAP relay mode, you need to ensure that the same EAP authentication method is selected on the client and the RADIUS server. On the device, you only need to configure the authentication method for 802.1X users to EAP.

4.4.1.5 802.1x Access Control Mode

The device not only supports the port-based access authentication method specified by the protocol (Port Based), but also expands and optimizes it to support the MAC-based access control method (MAC Based).

- When the port-based access control method is adopted, as long as the first user under the port is successfully authenticated, other access users can use network resources without authentication, but when the first user goes offline, other users can also use network resources. Will be denied access to the network.
- When the MAC-based access control method is adopted, all access users under this port need to be individually authenticated. When a user goes offline, only that user cannot use the network.

4.4.2 Configure 802.1 X

Read 802.1X Overview

Select "Security> 802.1X" in the menu to enter the page shown in Figure 4-30. The 802.1X configuration can be displayed in the "Overview", and the description of each parameter is shown in Table 4-12.

Figure 4-30 802.1X Overview Interface

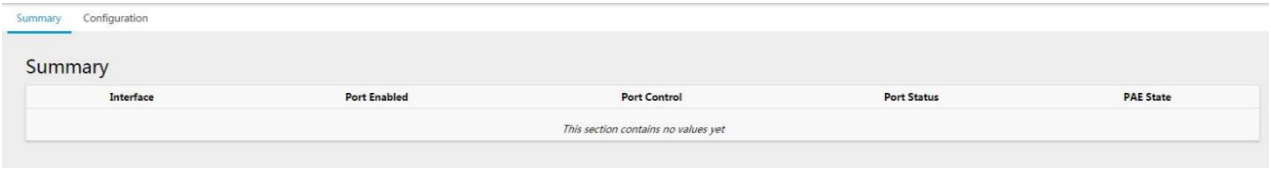


Table 4-12 802.1x Overview Parameters

Configuration Items	Instructions
Interface	Physical port
Port Enable	Whether the 802.1x function is enable on the port
Port Controlled	Port controlled mode
Port Status	Port controlled status
PAE Status	Port Access Entity

Configure 802.1X

Select "Security> 802.1X> Configuration" in the menu to enter the page shown in Figure 4-31. On this page, you can perform the global configuration of 802.1X and the configuration based on each port. The configuration parameter description is shown in Table 4-13.

Figure 4-31 802.1X Configuration Interface

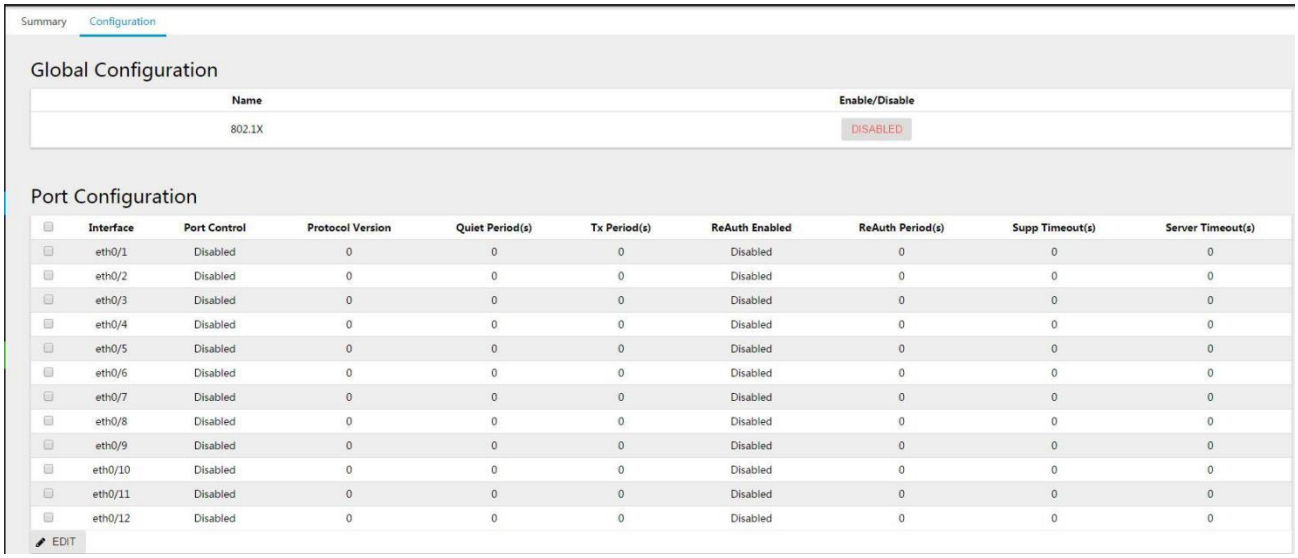


Table 4-13 802.1X Configuration Parameters

Configuration Items		Instructions
Global Configuration	802.1 X	Function switch
Port Configuration	Interface	Physical port
	Port Controlled	Port controlled mode
	Protocol version	802.1X
	Silent time	Set the value of the silent timer. After the 802.1X user authentication fails, the device needs to be silent for a period of time (by setting the "quiet duration") before re-initiating authentication. During the silent period, the device does not perform 802.1X authentication related processing.
	Transmission cycle	Message retransmission cycle
	Enable re-authentication	Whether to enable automatic re-authentication
	Recertification Cycle	Set the value of the periodic re-authentication timer When the periodic re-authentication function is enabled on the port, the device will start the periodic re-authentication timer after the user is successfully authenticated, which is used to periodically initiate re-authentication of online users, so as to regularly update the server's authorization information for users
	Client Timeout	Set the client timeout timer value After the device sends an EAP-Request/MD5 Challenge request message to the client, the device starts this timer. If the device does not receive a response from the client within the time set by the timer, the device will resend it The message
	Server Timeout	Set the server timeout timer value After the device sends a RADIUS Access-Request request message to the authentication server, the device starts the server timeout timer. If the device does not receive a response from the authentication server within the time set by the timer, the device will resend it Authentication request message

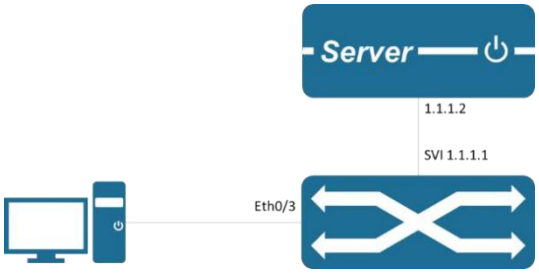
4.4.2.1 802.1X Configuration Example

1) Scene Requirement

- Required to authenticate access users on port Eth0/3 to control their access to the Internet.
- RADIUS server group IP address 1.1.1.2.
- Set the shared key for the message exchange between the system and the RADIUS server as name.

2) Network Diagram

Figure 4-32 802.1X Authentication Typical Network Diagram



3) Typical Configuration Example

Step 1: Configure server side

Server side:

Configure NAS authentication device 1.1.1.1 and communication key name.

In this example, freeradius is used as the server, and the main configuration is as follows:

```
# vim /etc/freeRADIUS/3.0/clients.conf
add

The client 1.1.1.1 {
        Ipaddr =
        1.1.1.1 Secret
        = name
}
```

Add user account test password test.

```
# cat /etc/freeRADIUS/3.0/mods-config/files/authorize | grep "password"
Testing Cleartext - Password: = "password"
Need to support the corresponding authentication method, such as EAP-MSCHAPv2
```

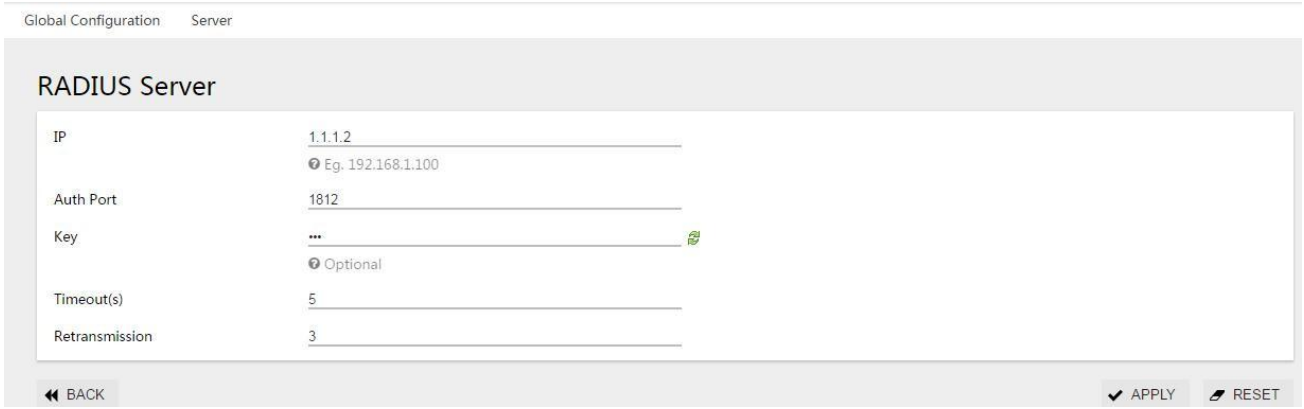
Step 2: Configure RADIUS server.

Select "Security> RADIUS> Server" in the menu to enter the page shown in Figure 4-33

Figure 4-33 RADIUS Server Display Interface

Click the [Add] button to enter the interface shown in Figure 4-34, configure the RADIUS server IP as 1.1.1.2, the default authentication port is 1812, enter the password, the timeout time is the default 5S, the number of retransmissions is 3, click the [Apply] button to complete the configuration.

Figure 4-34 RADIUS Server Configuration Interface



After the configuration is completed, it will automatically return to the following interface, as shown in Figure 4-35, and you can see the successfully created RADIUS server.

Figure 4-35 the RADIUS Server Display Interface

Step 3: Turn on 802.1x authentication global enablement.

Select "Security> 802.1X> Configuration" in the menu to enter the page shown in Figure 4-36, and click the [Enable/Disable] button to enable 802.1X authentication.

Figure 4-36 802.1x Global Configuration Interface

Step 4: Configure switch port 3 and enable 802.1X authentication globally.

Select "Security> 802.1X> Configuration" in the menu to enter the 802.1X configuration page, under port configuration, check the port eth0/3 that needs to be configured, and click the [Edit] button to enter the following configuration interface.

Figure 4-37 802.1X Port Configuration Interface

Click the [Apply] button to complete the configuration and automatically return to the following interface, as shown in Figure 4-38, you can see the successfully created port.

Figure 4-38 802.1X Port Configuration Display Interface

Port Configuration

Interface	Port Control	Protocol Version	Quiet Period(s)	Tx Period(s)	ReAuth Enabled	ReAuth Period(s)	Supp Timeout(s)	Server Timeout(s)
eth0/1	Disabled	0	0	0	Disabled	0	0	0
eth0/2	Disabled	0	0	0	Disabled	0	0	0
eth0/3	Auto	2	60	30	Disabled	3600	30	30

Step 5: Configure the authentication client

Open the 802.1X authentication client and log in with the account test.

Need to support the corresponding authentication method, such as EAP-MSCHAPv2 method.

4.5 MAC Authentication

4.5.1 Overview

4.5.1.1 Introduction to MAC Address Authentication

MAC address authentication is an authentication method that controls users' network access rights based on ports and MAC addresses. It does not require users to install any client software. After the device detects the user's MAC address for the first time on the port where MAC address authentication is enabled, it starts the authentication operation for the user. During the authentication process, the user does not need to manually enter the user name or password. If the user is successfully authenticated, it is allowed to access network resources through the port, otherwise the user's MAC address will be added as a silent MAC. During the silent time (which can be configured by the silent timer), when a user message from this MAC address arrives, the device directly discards it to prevent repeated authentication of illegal MAC in a short time.

note

If the configured static MAC is the same as the silent MAC, the MAC silent function will be invalid after the MAC address authentication fails.

Currently the device supports MAC address authentication:

Perform remote authentication through a RADIUS (Remote Authentication Dial-In User Service) server.

Currently, MAC address authentication supports two types of username formats:

MAC address user name: use the user's MAC address as the user name and password for authentication.

MAC Address Authentication by RADIUS Server Authentication

When the RADIUS server authentication method is selected for MAC address authentication, the device acts as a RADIUS client and cooperates with the RADIUS server to complete the MAC address authentication operation:

When using a MAC address user name, the device sends the detected user MAC address as the user name and password to the RADIUS server.

When a fixed user name is used, the device uses the user name and password configured locally as the user name and password of the user to be authenticated and sends it to the RADIUS server.

After the RADIUS server authenticates the user, the authenticated user can access the network.

MAC Address Authentication Timer

The MAC address authentication process is controlled by the following timers:

Authentication timeout timer: used to set the connection timeout time between the device and the RADIUS server. During the user authentication process, if the device has not received a response from the RADIUS server when the authentication timeout timer expires, the device will prohibit the user from accessing the network on the corresponding port.

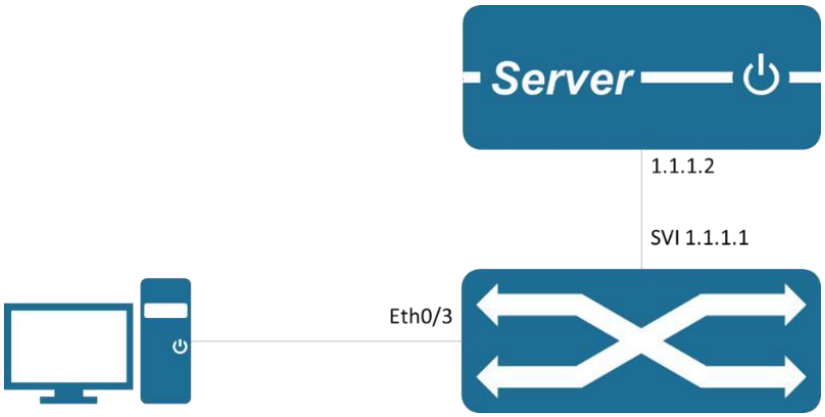
4.5.2 Configure MAC Authentication

Read MAC Certification Overview

Select "Security> MAC Authentication" in the menu to enter the page shown. The MAC authentication configuration can be displayed in the "Overview", and the description of each parameter is shown in the table.

Figure 4-39 MAC Certification Overview Interface

Figure 4-41 Typical MAC Authentication Networking Diagram



1) Typical Configuration Examples

Step 1: Configure the Server

Server side:

Configure NAS authentication device 1.1.1.1 and communication key name.

Add the client MAC address to the user database as the user account and password.

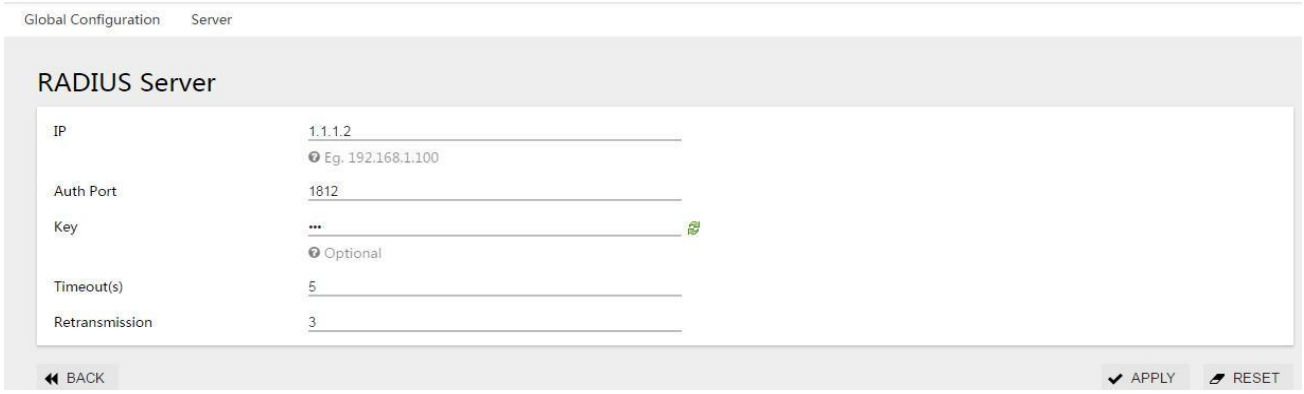
Step 2: Configure the RADIUS Server

Select 'Security > RADIUS > Server' in the menu and go to the page shown in figure 4-42

Figure 4-42 RADIUS Server Display Interface

Click 'ADD' button to enter the interface shown in figure 4-43. Configure RADIUS server IP as 1.1.1.2, default authentication port is 1812, enter password. Timeout is 5 seconds by default, re-transmission is 3 times, and click the 'APPLY' button to complete the configuration.

Figure 4-43 RADIUS Server Configuration Interface



When the configuration is complete, it is automatically returns to the following interface, as shown in Figure 4-35, where you can see that the RADIUS server is created successfully.

Figure 4-44 RADIUS Server Display Interface

Step 3: MAC Authentication Global Configuration

Select 'Security> MAC Authentication > Configuration' in the menu, enter the page shown in figure 4-45, click 'enable/disable' button to start MAC authentication.

Figure 4-45 MAC Authentication Global Configuration Interface

Step 4: Configure Switch Port 3 to Enable MAC Authentication Global Configuration

Select 'Security> MAC Authentication > Configuration' in the menu and enter the MAC Port Configuration page. Tick the port eth0/3 to configure, and click 'edit' button to enter the following configuration interface.

Figure 4-46 MAC Authentication Port Configuration Interface

Click the 'APPLY' button to complete the configuration and automatically return to the following interface, as shown in figure 4-47, you can see the port successfully created.

Port Configuration

Interface	Port Control	MAC Address Aging
eth0/1	-	Disabled
eth0/2	-	Disabled
eth0/3	Enable	Enabled

Figure 4-47 MAC Authentication Port Configuration

Step 5: Configure the Authentication Client Side

Open the 802.1x authentication client and log in with any account.

4.6 The RADIUS

4.6.1 Overview

RADIUS (Remote Authentication dial-in User Service) is a common protocol for implementing AAA (Authentication, Authorization and Accounting).

4.6.1.1 RADIUS Profile

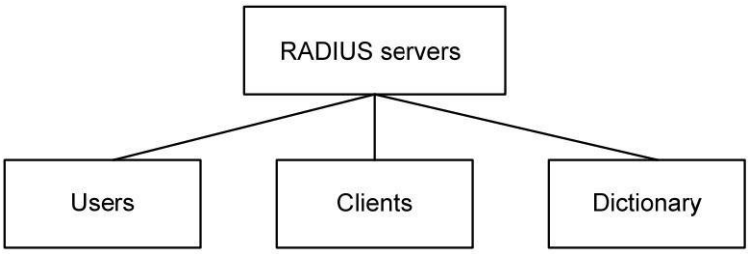
RADIUS is a distributed, client-server structured information interaction protocol that protects networks from unauthorized access and is often used in various network environments that require high security and allow remote users to access.This protocol defines the RADIUS message format and its message transmission mechanism, and stipulates that UDP is used as the transport layer protocol to encapsulate RADIUS message (UDP ports 1812 and 1813 are used as authentication and billing ports respectively). At the beginning, RADIUS was just a AAA protocol for dial-up users. Later, with the diversified development of user access methods, RADIUS also ADAPTS to a variety of user access methods, such as Ethernet access and ADSL access.It provides access services through authentication authorization and collects and records users' use of network resources through billing.

4.6.1.2 Client/Server Mode

- Client: the RADIUS client is typically located on a NAS device and can span the entire network, transmitting user information to a designated RADIUS server and then processing the information returned from the server (such as accepting/rejecting user access) accordingly.
- Server: the RADIUS server typically runs on a central computer or workstation, maintains relevant user authentication and network service access information, is responsible for receiving and authenticating user connection requests, and then returns all required information to the client (such as accepting/rejecting authentication requests).

The RADIUS server typically maintains three databases, as shown in figure 4-48.

Figure 4-48 the composition of the RADIUS server creates a successful MAC authentication port



- Users: used to store user information (such as user name, password, and configuration information such as the protocol used, IP address, etc.).
- 'Clients' : is used to store information about RADIUS Clients (such as Shared keys of access devices, IP addresses, etc.).
- 'Dictionary' : information used to store properties and the meaning of property values within the RADIUS protocol.

4.6.1.3 Security and Authentication Mechanism

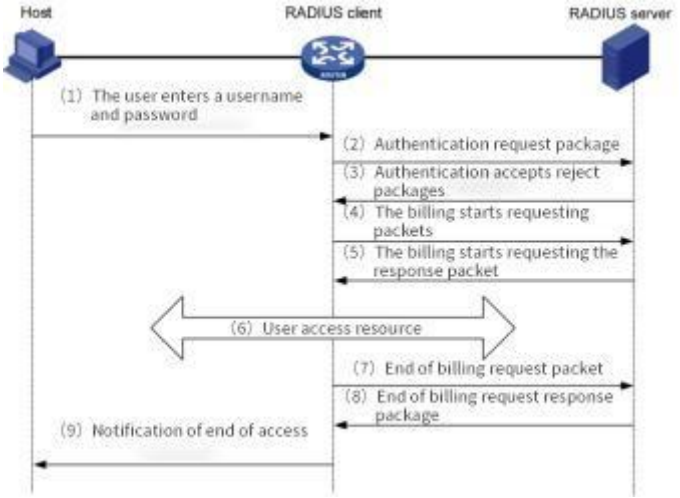
The interaction of authentication messages between RADIUS client and RADIUS server is accomplished through the participation of Shared key, and the Shared key cannot be transmitted through the network,

which enhances the security of information interaction.In addition, passwords are encrypted during transmission to prevent them from being stolen when they are transmitted over insecure networks.
The RADIUS server supports several methods for authenticating users, such as PAP, CHAP authentication based on PPP.In addition, RADIUS server can also act as a proxy to communicate with other RADIUS authentication servers as RADIUS client and be responsible for forwarding RADIUS authentication and billing messages.

4.6.1.4 Basic Message Interaction Flow of RADIUS

The interaction flow between the user, RADIUS client, and RADIUS server is shown in figure 4-49.

Figure 4-49 basic message interaction flow of RADIUS



The flow of message interaction is as follows:

(1) The user initiates a connection request to send the username and password to the RADIUS client.

(2) According to the acquired user name and password, RADIUS client sends access-request to RADIUS server, where the password is encrypted by MD5 algorithm with the participation of Shared key.
(3) The RADIUS server authenticates the user name and password.If the authentication is successful, the RADIUS server sends an access-accept to the RADIUS client;If authentication fails, access-reject is returned.Because the RADIUS protocol merges the authentication and authorization processes, the authentication acceptance package also contains the user's authorization information.
(4) RADIUS clients access/deny users based on the authentication results received.If a user is allowed access, the RADIUS client sends a billing start Request package to the RADIUS server.
(5) The RADIUS server returns the billing to begin the account-response and start the billing.

(6) Users start accessing network resources;

(7) The user requests to disconnect, and the RADIUS client sends the Accounting stop Request package to the RADIUS server.
(8) The RADIUS server returns the account-response package and stops the billing. User ends access to network resources.

instructions

Our equipment does not support RADIUS billing function

4.6.2 Configure RADIUS

RADIUS global configuration

Select Security > RADIUS in the menu and go to the page shown in figure 4-50.The global configuration parameters are described in table 4-16.

Figure 4-50 the RADIUS global configuration interface

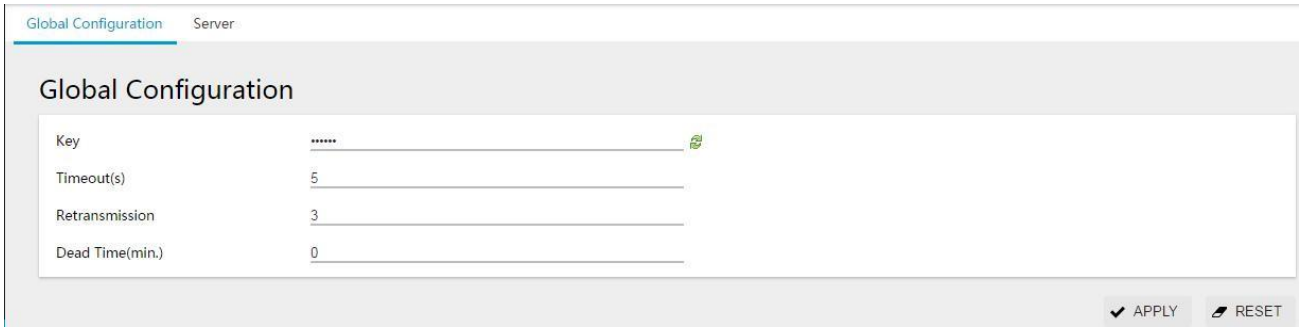


Table 4-16 MAC overview parameters

Configuration items	instructions
Password	Global default password configuration; Configurable, not readable; Optional configuration
Timeout	Global server timeout; Optional configuration
The retransmission	Global server retransmission times; Optional configuration
The time of death	Duration of server death; Optional configuration; The default is 0, which means the server is resurrected immediately after death

The RADIUS server

Select 'Security > RADIUS > server' in the menu and go to the page shown in figure 4-51.The parameters of the server are described in table 4-17.

Figure 4-51 RADIUS server configuration interface

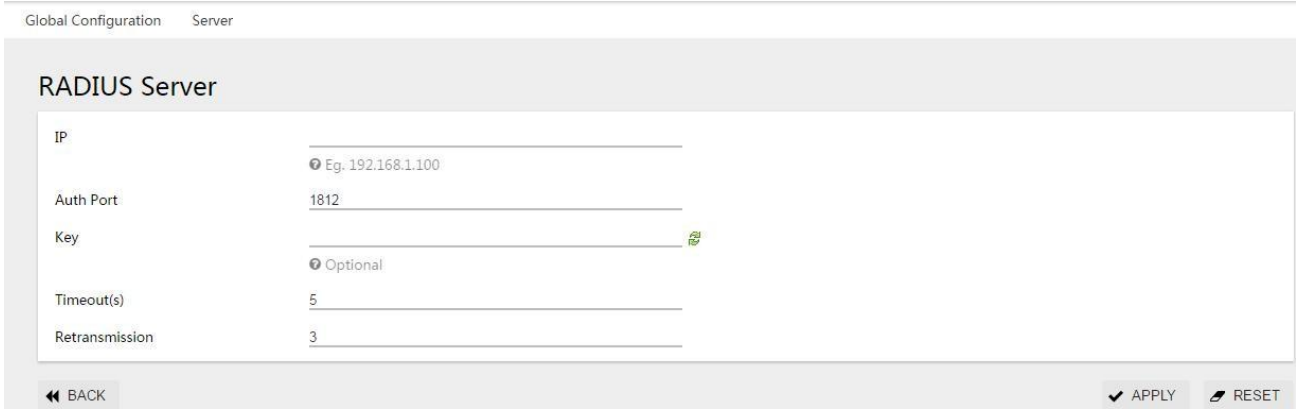


Table 4-17 RADIUS server parameter description

Configuration items	instructions
IP	Server IP address
Certification of port	Server authentication port number;The default is 1812
Password	Server key; Global configuration is used when there is no configuration
Timeout	Server timeout; The default 5 s
The retransmission	Server retransmission times, default 3 times

4.6.3 RADIUS Configuration Example

The RADIUS configuration steps are shown in the 802.1x or MAC authentication configuration steps.

4.7 Port Security

4.7.1 overview

The Port Security function limits the number of valid MAC addresses on a Port to prevent unauthorized users from accessing the Port. Packets with invalid MAC addresses are directly discarded.
Valid MAC addresses can be generated statically or dynamically.Static legal MACs are generated through user command line configuration;Dynamic legal MAC is dynamically generated by MAC address learning function.
When the number of secure MAC addresses on a port reaches the maximum value, the new MAC access port is regarded as an invalid MAC address and a violation event is generated. You can configure restrict or shutdown the port when the violation event occurs.
Restrict: Restrict the illegal MAC address data and generate an alarm log message.Invalid MAC addresses will be barred from accessing the port during the MAC address aging time.Run shutdown and no shutdown to restore the port.
Shutdown: forces the port down and configures the port recovery time. When the time is up, the port automatically recovers.You can also run the shutdown, no shutdown command to restore the port.
If you want to switch dynamic security users to static security users, you can enable the sticky function on the port.If the sticky function is enabled on a port, the dynamic user learned on the port will exist as a static user. If the configuration is saved, the dynamic user will still exist after the device is restarted.

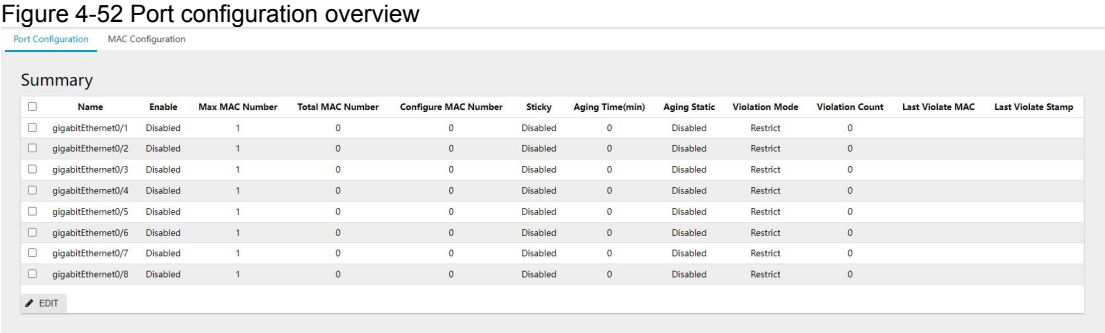
note

- Port security can be configured only for L2 ports, such as common physical ports and aggregation ports.
- Port security can be configured only in Access mode.
- Port security is not supported on aggregate port member ports.
- SPAN destination ports do not support port security.
- Port security is not supported on ports with static MAC addresses.

4.7.2 Configuring Port Security

Port configuration

On the navigation bar, choose Security > Port Security. Figure 4-52 shows the port configuration information.
Figure 4-52 Port configuration overview



Select the port you want to configure and click the "Edit" button to enter the port configuration page, as shown in Figure 4-53.Table 4-19 shows the port configuration parameters.
Figure 4-53 Port configuration page

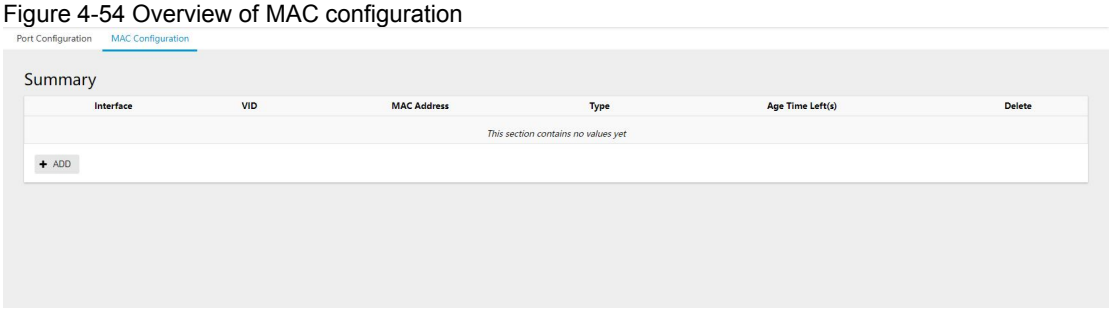
Table 4-19 Port configuration parameters

Configuration items		instructions
Port configuration	Start the	Enable/disable port security on the interface
	The largest number of MAC	This parameter specifies the maximum number of secure MAC addresses for a port. The default maximum number of secure MAC addresses is 1 1-1024 > <
	Sticky	Turn on/off the Sticky function
	Aging time	Set the security address aging time, in minutes.The default aging time is 0, indicating that the aging function is disabled Aging time range <0-1440> The default aging function only works for dynamic and sticky secure addresses
	Aging Static Addresses	Configure to enable static secure address aging
	Violation mode	Set the port security violation handling mode to Restrict by default Restrict: prohibit illegal user data and log the message Shutdown: Shutdown the port and restore the port after the errdisable recovery time The shutdown/no shutdown command is used to restore the port

MAC configuration

Choose Security > Port Security > MAC Configuration from the navigation tree. The MAC Configuration page is displayed, as shown in Figure 4-54.

Figure 4-54 Overview of MAC configuration



Click the [Add] button button to enter the MAC configuration page, as shown in Figure 4-55.

Figure 4-55 MAC configuration screen

Table 4-20 describes the MAC configuration parameters.

Table 4-20 MAC configuration parameters

Configuration items		instructions
Port configuration	interface	Select the interface you want to configure
	The MAC address	Configure a static secure address in the format of XXXX.xxxx.xxxx The secure address cannot be a broadcast or multicast address
	type	Set the MAC address to dynamic or static
	Remaining Aging Time	The remaining aging time of the current MAC address, in seconds
	delete	Delete the current MAC address, only for static addresses and dynamic addresses with sticky enabled

4.7.3 Configuration Examples

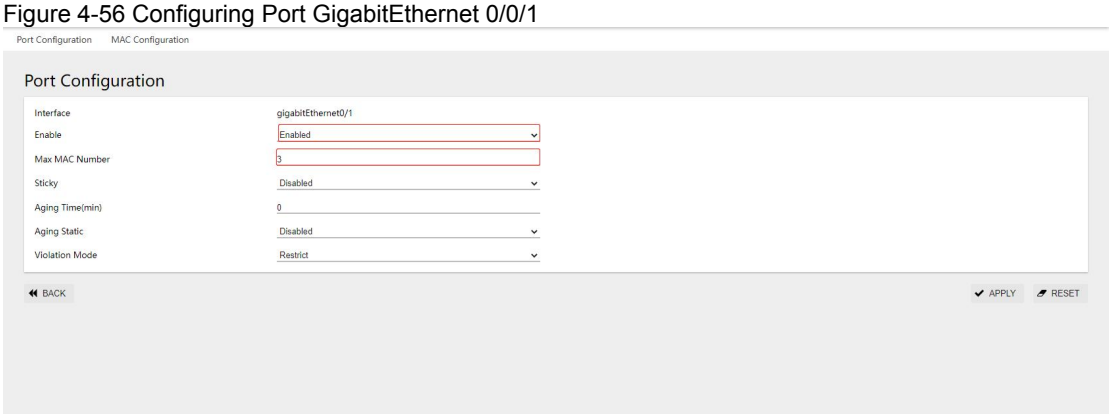
1) demand

- Limit the number of valid users on GigabitEthernet 0/0/1 to three, and set the MAC addresses to 0001.0001.0001, 0001.0001.0002, and 0001.0001.0003 Unauthorized users cannot access the device.

2) Typical Configuration examples

Step 1: On the navigation bar, choose Security > Port Security. The port configuration page is displayed. Select GigabitEthernet 0/0/1 and click Edit.

Figure 4-56 Configuring Port GigabitEthernet 0/0/1

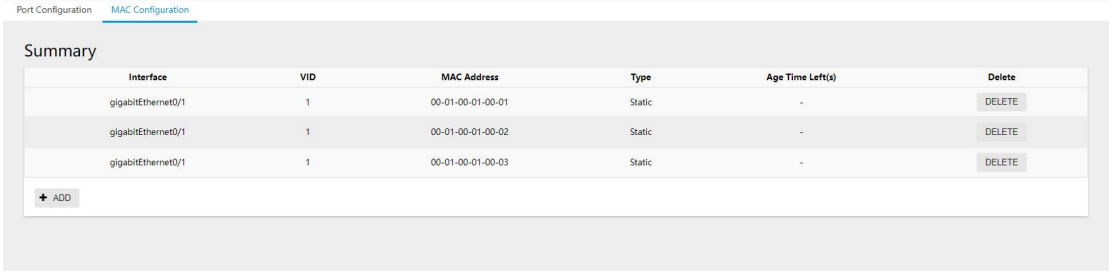


Step 2: On the current page, click the "MAC Configuration" TAB to enter the MAC configuration screen. Click the "Add" button to configure the interface as shown in Figure 4-57.

Figure 4-57 MAC Configuration screen

In the MAC address bar, enter three static MAC addresses in sequence. Figure 4-58 shows the interface after the configuration is complete.

Figure 4-58 MAC address successfully configured



4.8 IP Source Guard&ARP Check

4.8.1 overview

IP Source Guard:

Ip Source Guard allows Ip packets that match the Ip +MAC binding to pass through the port. Packets that do not match the Ip Source Guard binding are discarded to prevent Ip /MAC spoofing attacks.
Ip Source Guard binding entries are obtained from two sources: static configuration and dynamic acquisition in the Ip DHCP snooping environment.
Static user configuration: applies to host users whose IP addresses are statically configured in the LAN.
Ip DHCP snooping Dynamic obtain: applies to host users who obtain Ip addresses dynamically through DHCP on the LAN.
IP/MAC spoofing attacks: Illegitimate MAC users send IP packets with valid source IP addresses to legitimize their access identities.

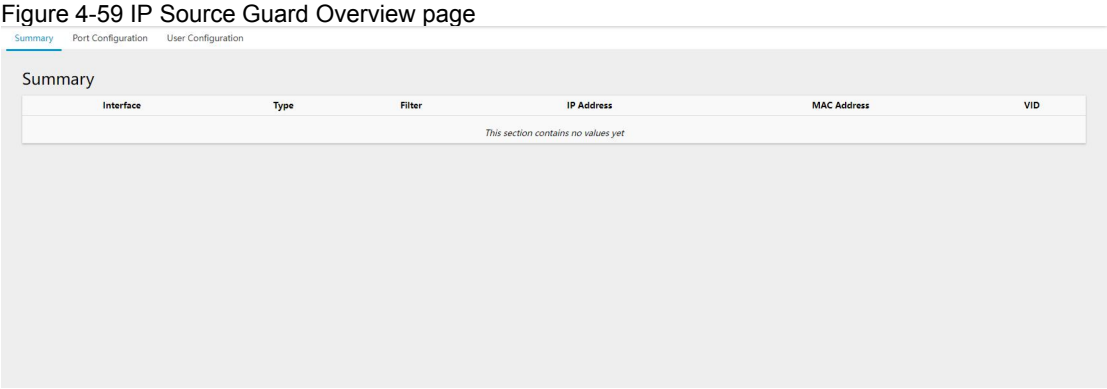
ARP Check:

The arp-check (Arp packet check) function filters all Arp packets on a port and discards all invalid Arp packets, effectively preventing Arp spoofing on the network and improving network stability.
On devices that support the arp-check function, the ARp-check function generates Arp filtering information based on the valid user information (IP+MAC) generated by security application modules such as IP Source Guard to filter out invalid Arp packets on the network.

4.8.2 Configuring IP Source Guard

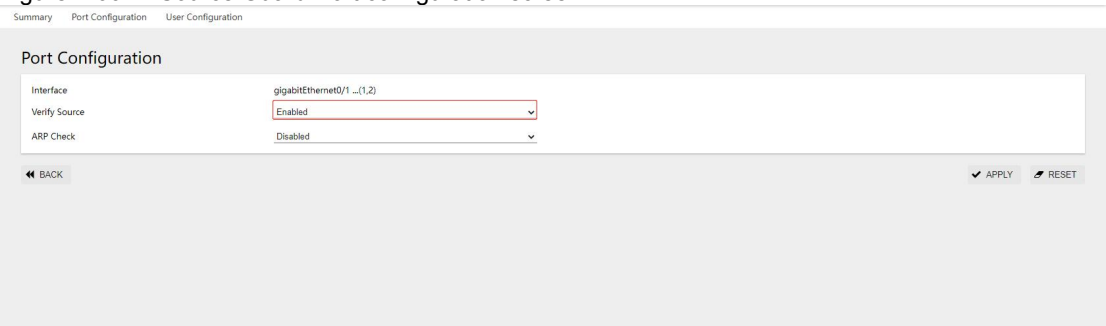
Step 1: In the navigation bar, tap Security IP Source Guard to go to the Overview page, as shown in Figure 4-59.→

Figure 4-59 IP Source Guard Overview page



Step 2: On the current page, click the Port Configuration TAB in the upper left corner to go to the IP Source Guard&ARP-Check port configuration screen.Select the check box in front of the port you want to configure, click the "Edit" button, Verify Source select "Enabled", as shown in Figure 4-60, and click the "Apply" button to complete the configuration.

Figure 4-60 IP Source Guard Port configuration screen

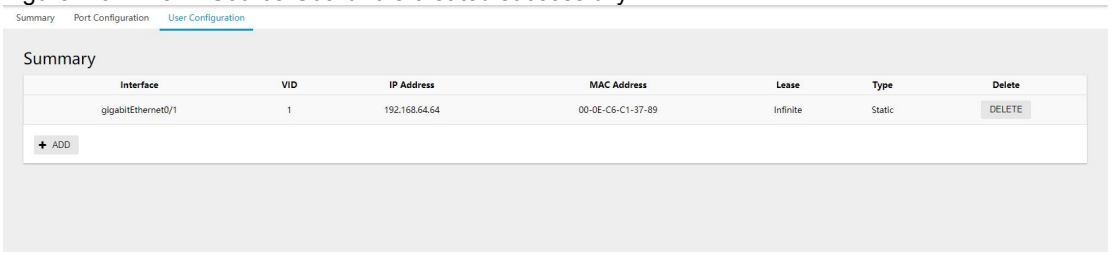


Step 3: On the current page, click the "User Configuration" TAB in the upper left corner to enter the IP Source Guard&ARP-Check user configuration screen.Click the "Add" button, select the interface and VID to be configured, and enter the MAC address and IP address, as shown in Figure 4-61.

Figure 4-61 IP Source Guard user configuration page

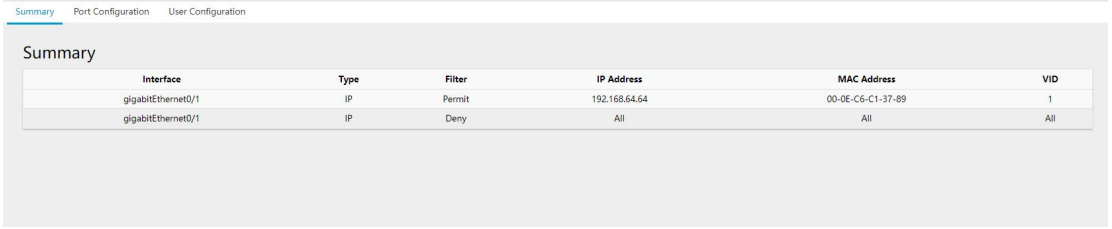
Click the "Apply" button to complete the configuration. The created IP Source Guard rule is displayed on the user configuration screen, as shown in Figure 4-62.

Figure 4-62 The IP Source Guard rule created successfully



Click the Overview TAB, and you can view the IP Source Guard overview. In this case, port gigabitethernet0/1 allows only the device whose IP address is 192.168.64.64 and MAC address is 00-0E-C6-C1-37-89 to access.

Figure 4-63 IP Source Guard profile created successfully

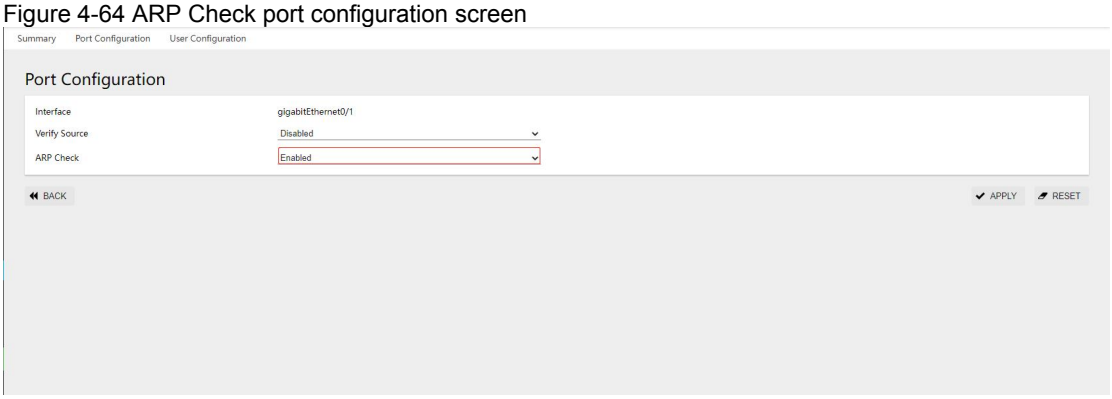


4.8.3 Configuring ARP Check

Step 1: In the navigation bar, tap Security IP Source Guard to go to the Overview page, as shown in Figure 4-58.→

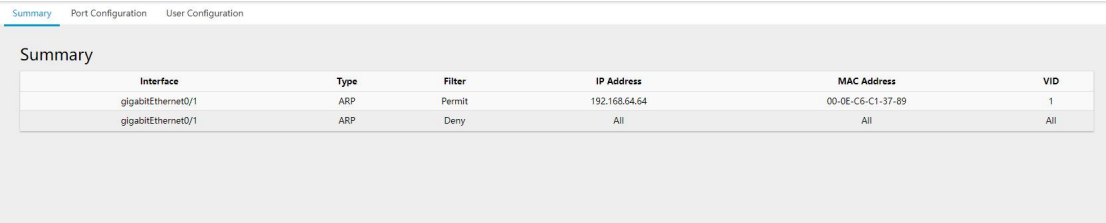
Step 2: On the current page, click the "Port Configuration" TAB in the upper left corner to enter the IP Source Guard&ARP-Check port configuration screen.Select the Check box in front of the port to be configured, click the "Edit" button, and select "Enabled" for ARP Check, as shown in Figure 4-64. Click the "Apply" button to complete the configuration.

Figure 4-64 ARP Check port configuration screen



Step 3: On the current page, click the "User Configuration" TAB in the upper left corner to enter the IP Source Guard&ARP-Check user configuration interface.Click the "Add" button, select the interface and VID to be configured, and enter the MAC address and IP address, as shown in Figure 4-60.Click "Apply" to complete the configuration. The newly created ARP Check rule is displayed on the User configuration page, as shown in Figure 4-65.

Figure 4-65 Overview of the newly created ARP Check rule



5 System

5.1 Manage IP Addresses

- After changing the IP address, you need to manually point the page to the new address and re-access the switch.

note

- The configuration of VLAN (VID) management is complicated, and improper operation will cause failure to log on the device. If you need to change the VID, please refer to the specific operation method

  Manage VLAN configuration instances.

As shown in figure 5-1, select 'manage IP address' from the menu of 'system' to enter the IP address management interface.

Figure 5-1 IP address management interface

Table 5-1 parameter description

Configuration items	Instructions
VID	Manage the VLAN configuration, specifying which VLAN to use as the administrative VLAN that must already exist.
IPV4 type	None: addresses are not managed using IPV4 Static: specifies the IPv4 address manually, which requires the IPv4 address and mask length to be set DHCP: means to get the IPv4 address through DHCP allocation
IPV4 address	Set IPV4 to manage IP addresses. IPV4 addresses are available when 'static' is selected
IPV4 mask	Set the subnet mask to 255.255.255.0 by default. The IPv4 address is available When 'static' is selected
IPV4 gateway	Specify the IP address of the gateway. The IPv4 address is available when 'static' is selected
IPV6 type	None: addresses are not managed using IPV6 Static: means to specify IPv6 address manually, which is required to be set when selecting this option DHCP: means to get IPv6 address through DHCP assignment

IPV6 address	Set IPV6 administrative IP address. IPV6 address can be obtained by selecting 'static'
IPV6 prefix length	Set the IPV6 prefix length. IPV6 address is available when 'static' is selected
IPV6 gateway	Set up IPV6 gateway. IPV6 address is available when 'static' is selected

Configuration example 1

Case requirements: management VLAN 1, management IP 192.168.64.200, subnet mask 255.255.255.0, gateway address 192.168.64.1.
Configuration steps:

Step 1: click [system] -> in the menu to enter the IP address managementinterface.

Step 2:enterthechangesasshowninfigure5-2andclicktheapplybuttontomaketheconfiguration effective.

Figure 5-2 IP address management interface

Step 3: modify the login IP of the browser to be 192.168.64.200. The PC needs to be equipped with the same network segment and log in again.
After re-logging in, the system will prompt whether to save the current IP address, and users can choose 'save' or 'ignore' according to their needs.

Step 4: click the 'save' button on the menu to save the configuration.

Configuration example 2

Case requirements: the device manages VLAN 1 by default, and the management IP address is 192.168.1.168. The management VLAN needs to be modified to VLAN 100, and the management IP needs to be modified to 192.168.1.100.

note

- Ensure that the VLAN of the PC and switch is accessible before modifying the management VLAN, otherwise the switch may not be accessible.

Scenario 1: PC is connected directly to the switch. The PC is connected to the switch eth0/1, which is configured by default as an access port and Native VLAN 1.

Step 1: create VLAN 100;

Click menu [switch] -> [VLAN], enter the VLAN interface, and click [add] button, as shown in the figure.VLAN ID is '100', tagged member port is empty, click apply to return to VLAN main interface.

Figure 5-3 VLAN creation interface

Return confirmation that the administrative VLAN configuration was successful

Figure 5-4 VLAN display interface

Step 2: configure an idle port as access port and Native VLAN as new administration VLAN100. For example, use the eth0/2 port, select eth0/2, and click the edit button to enter the following configuration screen.Change the mode of eth0/2 to access and PVID to 100, and click the 'apply' button to complete the configuration.

Figure 5-5 interface configuration interface

Go back and check the modified configuration to make sure port eth0/2 is configured correctly

Figure 5-6 interface display interface

Step 3: modify the administration VLAN to 100 and configure the new IP address.

Click [system] -> [management IP address] in the menu to enter the management VLAN configuration interface

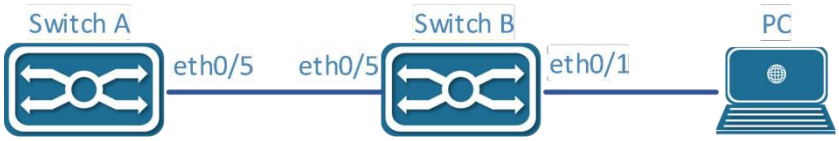
Modify the management VLAN to the expected configuration of 100, and modify the management IP to the expected configuration of 192.168.1.100, and click [apply] to modify.

Figure 5-7 IP address management interface

Step 4: switch the PC from eth0/1 to eth0/2 to connect to the switch and log in to theswitch WEB interface using the new IP 192.168.1.100.

Step 5 :(optional) if you want to access the switch from other devices, you need to add anew management VLAN 100 to the trunk of other devices.
Scenario 2: as shown in figure 5-8, Switch A is the Switch to which the configuration is expected to be modified, and the PC is connected to SW1 through the Switch B Switch.

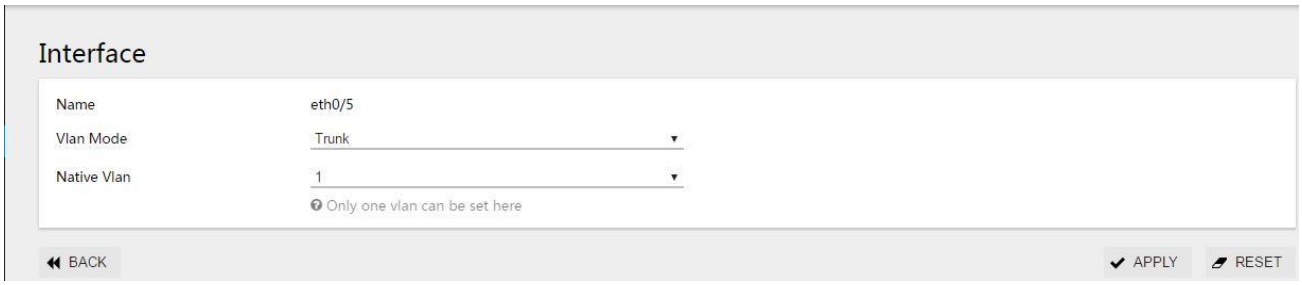
Figure 5-8 scenario 2 topology diagram



Step 1: configure the Switch A and Switch B interconnect eth0/5 as their trunk.

Click the menu [switch] -> [VLAN], enter the interface interface, select port eth0/5, click the button [edit], as shown in the figure, select Trunk for VLAN mode, Native VLAN default is 1, click [apply] to complete the configuration.

Figure 5-9 interface configuration interface



Step 2: Switch A and Switch B to create A VLAN 100, tagged member port select eth0/5.

Click the menu [switch] -> [VLAN] to enter the VLAN interface, click the button [add], VLAN ID is '100', Tagged member port select eth0/5, and click [apply] to return to the VLAN main interface.

Figure 5-10 VLAN configuration interface

Return confirmation that the administrative VLAN configuration was successful

Figure 5-11 VLAN display interface

Step 3: modify Switch A management VLAN to 100 and configure the new IP address.

Click the menu [system] -> [IP address management] to enter the IP address management interface.Modify the management VLAN to the expected configuration of 100, and modify the management IP to the expected configuration of 192.168.1.100, and click [apply] to modify.

Figure 5-12 IP address management interface

Step 4: change the eth0/1 of Switch B directly connected to PC to access mode,NativeVLAN100, to ensure that Switch A device can be accessed from PC after PC's management message and Switch A's management VLAN100 are accessible.

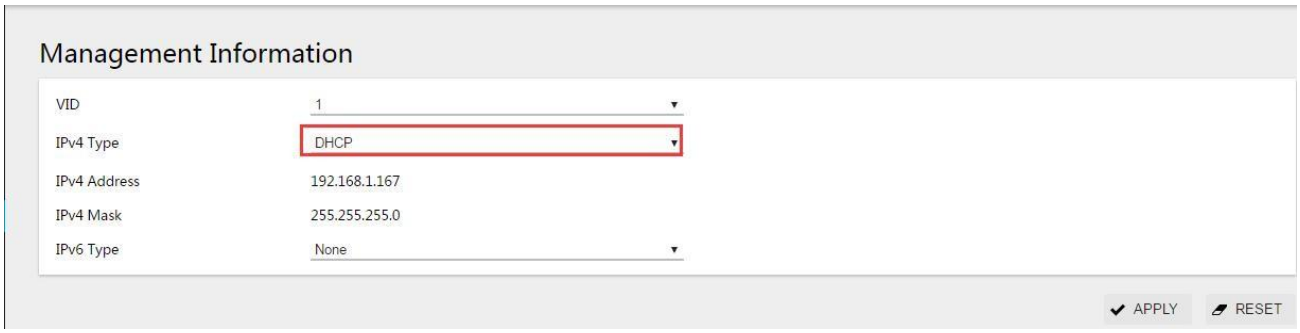
Configuration example 3

Case requirements: VLAN management is 1, and IP management is DHCP allocation.

Step 1: click [system] -> in the menu to enter the IP address managementinterface.

Step 2: select DHCP according to the IPV4 type shown in figure 5-2, and click the 'apply' button to make the configuration effective.

After the configuration takes effect, the IP address of the device can be seen on the DHCP server side, or the device



can be logged in by serial port, and the IP address of the device can be viewed by entering 'show management summary' command.

```
SWITCH#show management summary
 Management interface with Ipv4:
      Type:         Dhcp
      Vlan:         1
      Ip address:   192.168.1.6/24
      Gateway:      192.168.1.1
SWITCH#
```

Step 3: log in the device with the new IP address and re-enter the IP management interfaceto see the IP address of the device.

Step 4: click the 'save' button on the menu to save the configuration.

5.2 User Management

note

- In order to improve the security of the device, please change the password as soon as possible, and be sure to save the changed password. If you forget the password, you will be unable to log in the device.

Click the menu [system] -> [user management] to enter the user management interface, as shown in FIG. 5-13.

Figure 5-13 user management interface

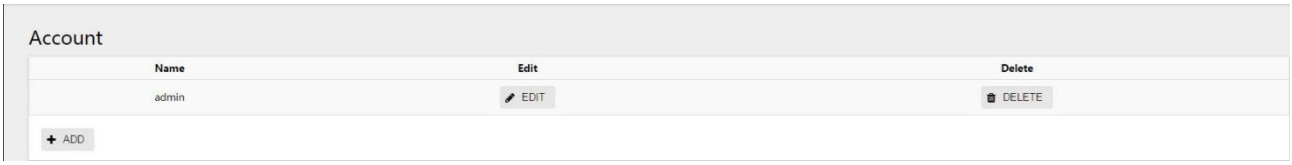


Table 5-3 user management parameters

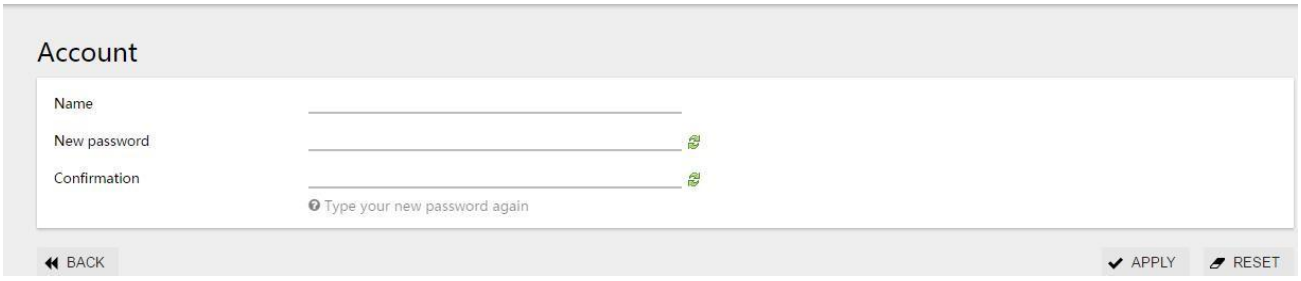
Configuration items	Instructions
The name	User name
The editor	I'm gonna go edit user
Delete	Click delete the user
Add	Add a new user

Steps to add an account:

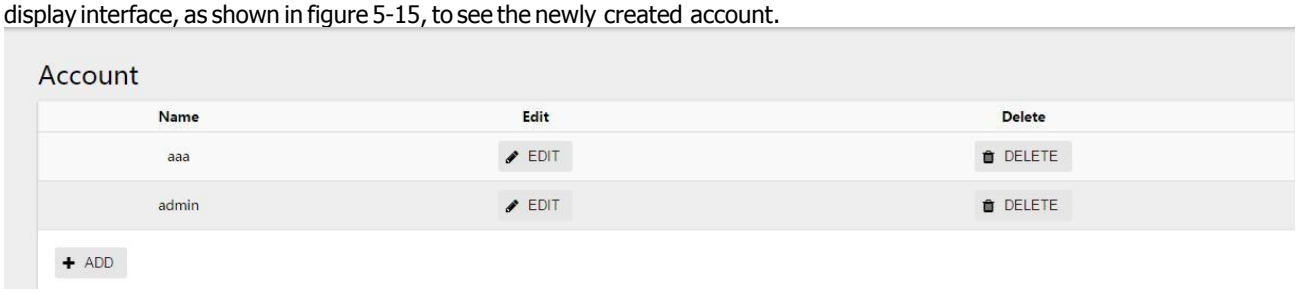
Step 1: click 'system' -> 'user management' in the menu to enter the user management interface.

Step 2: click the 'add' button to enter the add account interface, as shown in figure 5-14. After logging into the device for the first time, please modify the password as soon as possible and enter the new password twice according to the prompts, as shown in figure 5-13.Passwords are composed of Numbers and letters that are 0-32 bytes long and case-sensitive.

Figure 5-14 add account interface



Step 3: click the 'apply' button to complete the configuration, and the interface will automatically return to the account display interface, as shown in figure 5-15, to see the newly created account.



Step 4: click the 'save' button on the menu to save the configuration.

5.3 Services

5.3.1 Overview

The service management module provides management functions of Telnet and SSH services, enabling users to enable the service only when they need to use the corresponding service, or close the service.This can improve the performance of the system and the safety of equipment, to achieve the safety management of equipment.
1. The Telnet service

Telnet protocol belongs to the application layer protocol in TCP/IP protocol family, which is used to provide remote login and virtual terminal functions in the network. 2. SSH services
SSH is short for Secure Shell. When the user logs into the device remotely through a network environment that cannot guarantee security, SSH can use encryption and powerful authentication functions to provide security to protect the device from attacks such as IP address fraud and plaintext password interception.
5.3.2 Configuration Service Management
As shown in figure 5-14, select 'service' from the drop-down menu of 'system' to enter the configuration interface. Click on the enable/disable button to switch Telnet/SSH service state to enable or disable Telnet/SSH service.

Figure 5-14 service configuration interface

5.4 The SNMP

5.4.1 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 managed devices.SNMP has the following characteristics:

- Support intelligent management of network equipment. Using the network management platform based on SNMP, network administrators can query the running status and parameters of network equipment, set parameter values, find faults, complete fault diagnosis, carry out capacity planning and generate reports.
- Support for managing devices with different physical characteristics.SNMP only provides a basic set of functions, making management tasks relatively independent from the physical characteristics and networking technologies of managed devices, so as to realize the management of devices from different manufacturers.

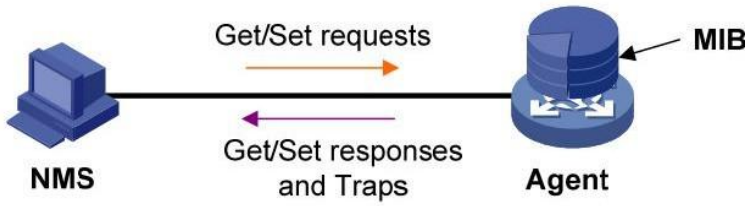
5.4.1.1 Working Mechanism of SNMP

SNMP network contains NMS and Agent.

- NMS (Network Management System) is the manager of SNMP Network, which can provide a very friendly human-computer interaction interface and facilitate Network administrators to complete most of the Network Management work.
- Agent is the manager of SNMP network, responsible for receiving and processing the request message from NMS.In some emergencies, such as the change of interface state, Agent will actively send warning information to NMS.

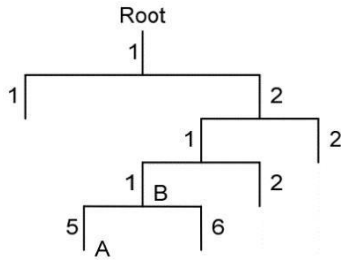
When NMS manages devices, it usually pays close attention to some parameters, such as interface status, CPU utilization, etc. The set of these parameters is called MIB (Management Information Base).These parameters are called nodes in the MIB.The MIB defines hierarchical relationships between nodes and a set of properties of an object, such as its name, access rights, and data types. Each Agent has its own MIB. Managed devices have their own MIB files, which can be generated by compiling these MIB files on the NMS.NMS carries out read/write operations on MIB nodes according to access rights, so as to realize Agent management.The relationship between NMS, Agent and MIB is shown in figure 5-15.

Figure 5-15 relationship between NMS, Agent and MIB



The MIB is organized in a tree structure and consists of several nodes, each of which represents the managed Object. The managed Object can be uniquely identified by a string of Numbers representing the path starting from the root, which is called OID (Object Identifier).
As shown in figure 5-16, 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 5-16 MIB tree structure



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

- GET operation: the NMS USES this operation to query the value of one or more nodes in the Agent MIB.
- SET operation: this operation is used by the NMS to SET the value of one or more nodes in the Agent MIB.
- Trap operation: this operation is used by the Agent to send Trap information to the NMS.
  Agent does not require NMS to send response message.
  Nor does the NMS respond to Trap information. SNMPv1, SNMPv2c, and SNMPv3 support Trap operations.

5.4.1.2 Protocol version of SNMP

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

- SNMPv1 adopts Community Name authentication mechanism. Group names are similar to passwords and are used to limit NMS and
  Communication between agents. If the group name set by NMS is different from that set by the managed device, the SNMP connection between NMS and Agent cannot be established, so that the NMS cannot access the Agent, and the warning information sent by the Agent will also be NMS discarded.
- SNMPv2c also adopts the group name authentication mechanism.SNMPv2c extends the functions of SNMPv1 by providing more operation types;Support for more data types; Provides richer error code, allowing for more detailed error differentiation.
- SNMPv3 adopts USM (user-based Security Model) authentication mechanism. Network administrators can set authentication and encryption functions. Authentication is used to verify the legitimacy of message sender and avoid access by illegal users. Encryption is to encrypt the transmission message between NMS and Agent to avoid eavesdropping. Authentication and encryption functions can provide higher security for communication between NMS and Agent.

instructions

The prerequisite for the successful connection between NMS and Agent is that the SNMP version used by NMS and Agent must be the same.

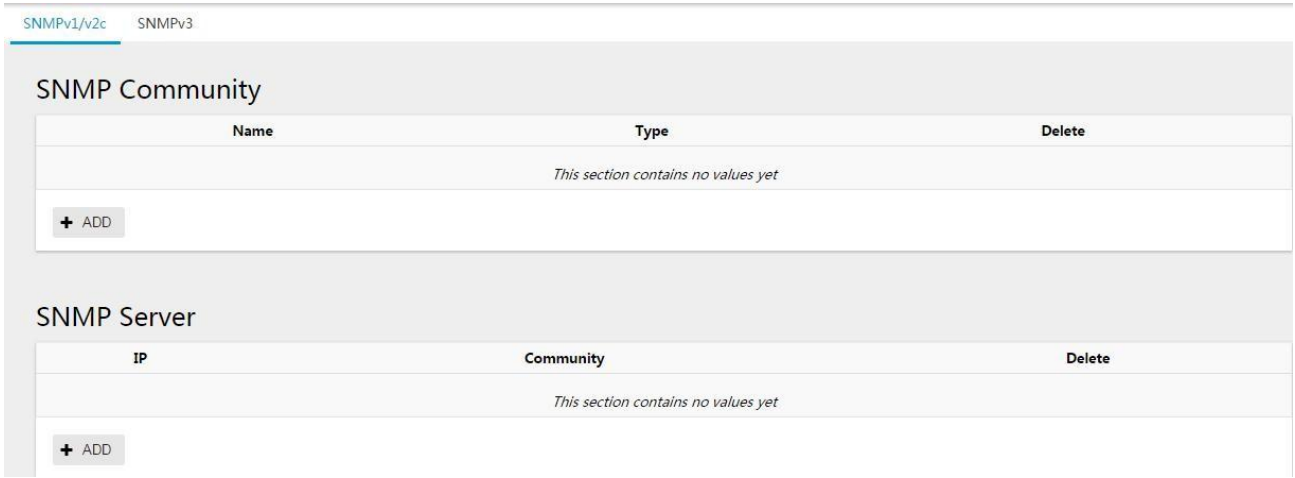
5.4.2 Configure SNMP

Since the configuration of SNMPv3 version is quite different from that of SNMPv1 version and SNMPv2c version, there are two types below
Introduction.

5.4.2.1 SNMPv1 / v2c 5.4.2.1 configuration

SNMP group word is the authentication field agreed between the device and SNMP server, which needs to ensure that the server configuration is consistent with the device side.SNMP group word has two types of permissions: read-only and read-write. Configure group word with read-only permissions.GET and SET operations can only be performed on the server that has read and write access to the group word.The device side can support configuring multiple sig words for use by different servers.
(1) select [system] [SNMP] in the menu, enter the SNMP configuration page, click the SNMPv1/v2c TAB, and the page will display all SNMP group word information and server information currently configured.

Figure 5-17 SNMP group word



(2) configure SNMP group word, click [+ add] button to enter the new page and add new SNMP group word, as shown in figure 5-18, and SNMP group word parameters 5-4 are described as shown in the table.

Figure 5-18 SNMP group word configuration

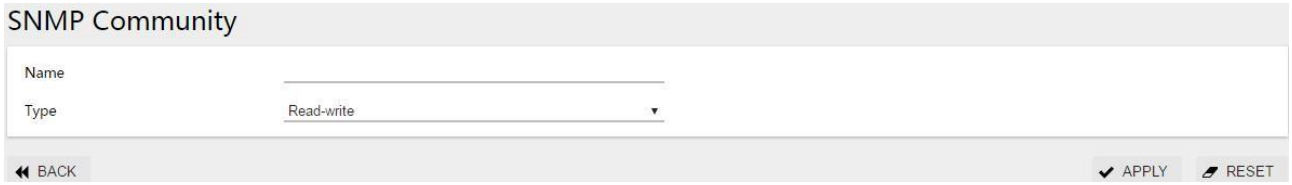


Table 5-4 SNMP group word parameter description

Configuration items	Instructions
The name	Group name
Type	Group name permission type; Where read-write is Read and write and read-only is Read only.

(3) configure SNMP server, click [+ add] button to add SNMP server, the page of adding server is shown in figure 5-19, and the parameter description of SNMP server is shown in table 5-5.

Figure 5-19 SNMP server configuration

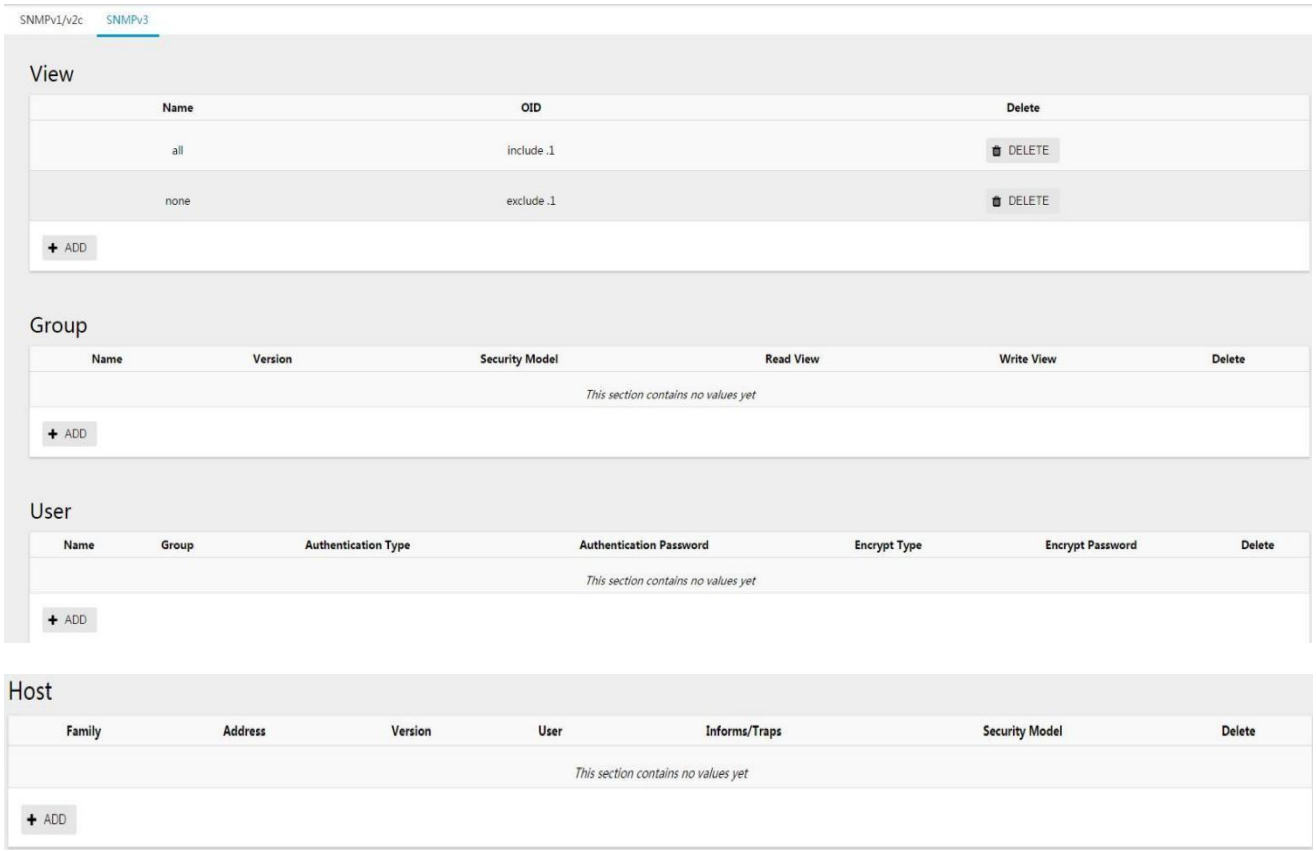
Table 5-5 SNMP server parameter description

Configuration items	instructions
IP	SNMP server IP address.
Groups of words	SNMP server authentication group word.

5.4.2.2 Configuration SNMPv3

(1) select [system] [SNMP] from the menu, enter the SNMP configuration page, click the SNMPv3 TAB, as shown in figure 5-20, and the page will display all SNMPv3 information currently configured.

Figure 5-20 SNMPv3 interface



(2) configure SNMPv3 view, click [+ add] button to enter the page of adding new view, as shown in figure 5-21, and view parameters are described in table 5-6.

Figure 5-21 add the SNMPv3 view interface

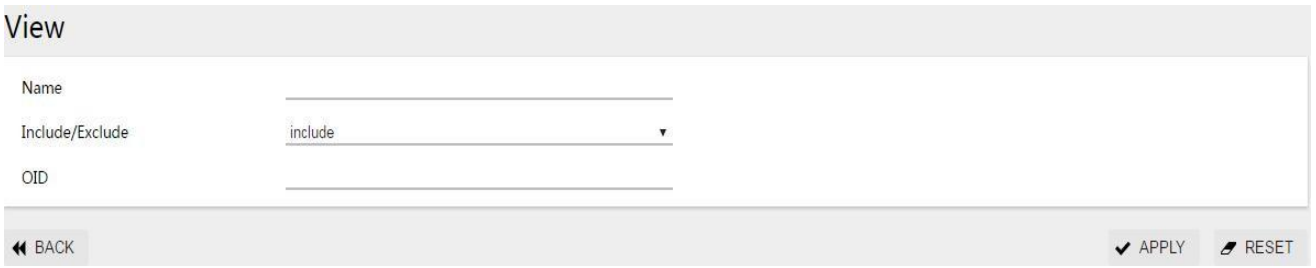


Table 5-6 detailed configuration of SNMP view rules

Configuration items	instructions
The name of the	Displays the name of the SNMP view All view and none view exist by default in the system. All view contains all oids; The none view does not contain any OID
Include/Exclude	Set objects that will be identified by the MIB subtree OID and subtree mask to be included or excluded from the view scope outside
The OID	OID (such as 1.4.5.3.1) or name (such as system) MIB subtree OID shall indicate the node in A position in the MIB tree that uniquely identifies an object in an MIB library

(3) configure SNMPv3 group, click [+ add] button to enter the page of new SNMP group, as shown in figure 5-22, and the parameters of SNMP group are shown in table 5-7.

Figure 5-22 new SNMP group interface

Table 5-7 detailed configuration of SNMP group

Configuration items	instructions
The name of the	Set the name of the SNMP group
version	
Security model	Set the security level of SNMP group AuthPriv: both authentication and encryption AuthNoPriv: authentication only, no encryption NoAuthNoPriv: no authentication, no encryption prompt Currently SNMPv3 users and groups support only authenticated and encrypted levels of security.
Read the view	Set up a read view of the SNMP group All: select the All view None: select the None view prompt You can select other views
Write a view	Set up the write view of the SNMP group All: select the All view None: select the None view prompt You can select other views

(4) configure SNMPv3 user, click [+ add] button to enter the new SNMP user interface, as shown in figure 5-23, and SNMP user parameters are shown in table 5-8.

Figure 5-23 new SNMP user

Configuration items	Instructions
The name	Set the name of SNMP user
Group	Sets the name of the group to which the user belongs • select the 'no authentication, no encryption' group when the user's security level is 'no authentication, no encryption' • when the user's security level is selected as 'authentication without encryption only', you can choose 'non-authentication without encryption' or 'authentication only' Unencrypted groups • select groups of all security levels when the user's security level is 'both authenticated and encrypted. prompt Currently SNMPv3 users and groups support only authenticated and encrypted levels of security.
The authentication type	When the security level selects 'authentication without encryption only' or 'both authentication and encryption', set the authentication mode, including: MD5,SHA
The authentication code	Set the authentication password when the security level selects authentication only and not encryption or both authentication and encryption
Encryption type	When the security level selects 'both authentication and encryption', set the encryption mode, including: DES, AES
Encrypted password	When the security level selects both authentication and encryption, set the encrypted password

Table 5-8 detailed configuration of SNMP users

(5) configure SNMPv3 host, click [+ add] button to enter new SNMP host, as shown in figure 5-24, and SNMP host parameter description is shown in table 5-9.

Figure 5-24 create a new SNMP host

Table 5-9 detailed configuration of SNMP hosts

Configuration items	instructions
family	IP address family, used to distinguish between IPv4 and IPv6 hosts
address	IP address values
version	The SNMP version number
The user	SNMPv3 version of the user name
Security model	User security model for SNMPv3
Informs/Traps	Type of notification message sent Informs: needs to wait for a response from the server to support retransmission Traps: do not support re-transmission, do not wait for response

5.5 Date/Time

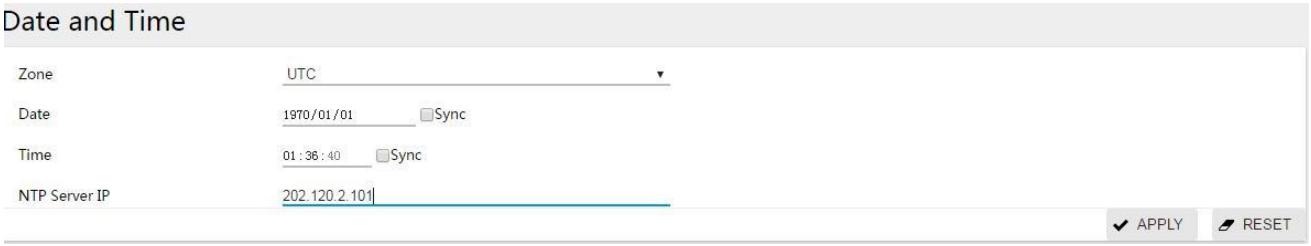
In order to ensure the coordination between the equipment and other equipment, users need to configure the system time accurately.The date and time Settings module is used to display and set the system time on the webmaster, and to set the system time zone.The device supports manual configuration of system Time and automatic synchronization of NTP Protocol (Network Time Protocol) server Time.

NTP (Network Time Protocol) is a Time synchronization Protocol defined by RFC 1305 for Time synchronization between distributed Time servers and clients.The purpose of using NTP is to synchronize the clocks of all devices with clocks in the network so that the clocks of all devices in the network are consistent, thus enabling the devices to provide multiple applications based on uniform time.For a local system running NTP, synchronization from other clock sources can be accepted and used as a clock source to synchronize other clocks and with other devices.

5.5.1 View the Current Date and Time of the System

(1) select [system] [date and time] in the menu to enter the date and time interface, as shown in FIG. 5-25.
(2) view the current date and time of the system displayed in real time on the page.

Figure 5-25 date and time configuration interface



instructions

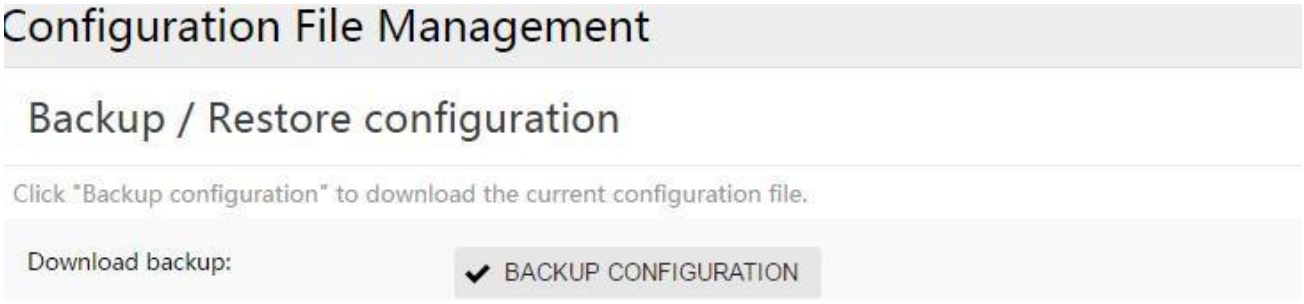
- The device must be able to access the NTP server.
- Aftertheconfigurationiscomplete,thedeviceautomaticallysynchronizesthetimeinformationfromtheserver. The first time synchronization takes about 4-8 minutes.
- For devices without built-in RTC, the time and date of device restart will be restored to factory Settings, and the equipment configured with NTP server will automatically be the same
  Step network time.

5.6 Profile Management

5.6.1 Configure Backup

Configuration backup function, you can download the configuration of the machine to the computer, used to restore the configuration or import to other devices.
Select 'configuration file management' from the drop-down menu of 'system' in the menu and enter the configuration file management interface, as shown in FIG. 5-28.

Figure 5-28 configure backup

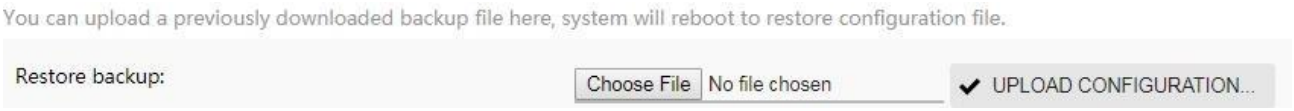


Click the 'backup configuration' button to pop up the 'file download' dialog box and save the configuration file locally.

5.6.2 Configuration Recovery

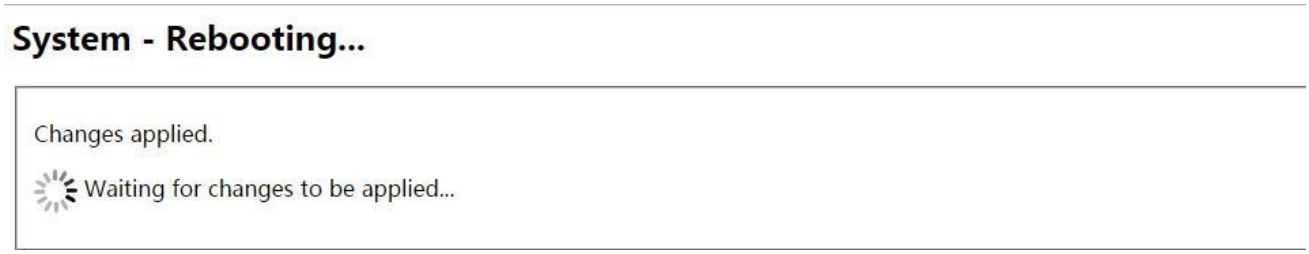
Configuration recovery allows you to quickly import configuration files into the machine.

Figure 5-29 configuration recovery



As shown in figure 5-29, click the 'select file' button, select the configuration file with the suffix '.conf 'to be imported, and click the' upload configuration 'button.The device will restart automatically during the import configuration process and wait for the interface shown in figure 5-30.

Figure 5-30 configuration recovery wait interface

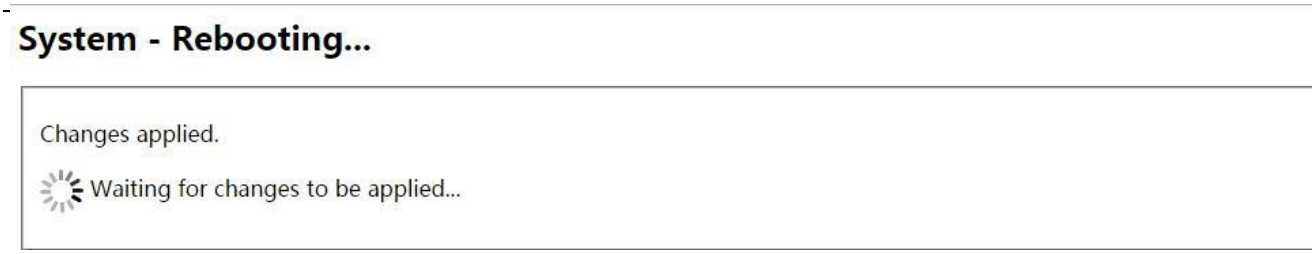


5.6.3 Restore Factory Settings

The restore factory configuration module provides the ability to restore all configurations in the device to the factory default configuration, delete the current configuration file, and restart the device.

Step 1: select system [profile management] in the menu. Step 2: click the 'restore Settings' button, as shown in figure 5-31.

Figure 5-31 restore factory Settings interface



Step 3: wait for the device restart to complete, as shown in figure 5-32. Log in withdefault IP, user name and password after the device restart.

Figure 5-32 configuration recovery wait interface

5.7 System Upgrade

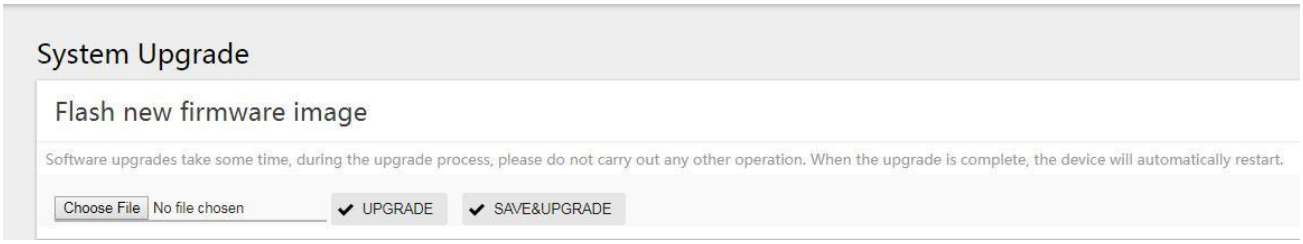
The software upgrade module provides the ability to get the target application file from localhost and set it to the same startup file that the device will use the next time it starts up.

note

- Softwareupgradestaketime.Pleasedonotdoanythingon theWebduringthesoftwareupgrade, as it may Cause software upgrade interruption.
- After the upgrade, the device will restart automatically.

Step1: select[system]-> in the menu and enter the page of 'update firmware', as shown in figure 5-33.

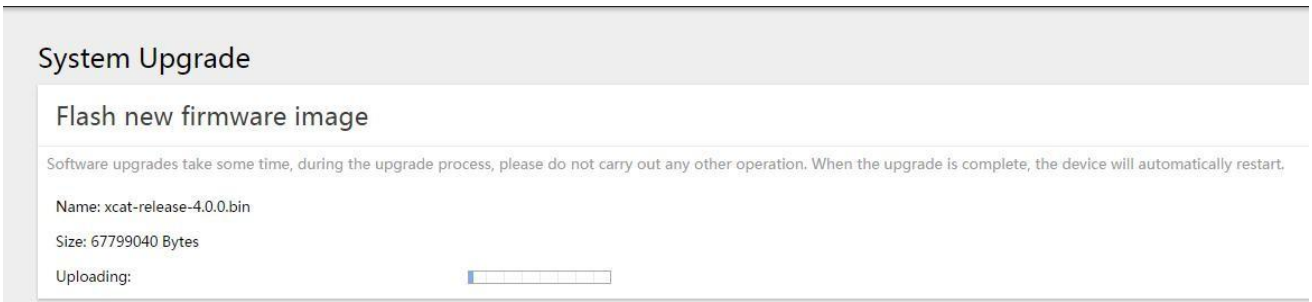
Figure 5-33 software upgrade



Step 2: click the 'Choose File' button and select the upgrade File corresponding to the device in the dialog box. The upgrade File is in the format of.bin.

Step3:clickthe'upgrade'or'saveconfiguration&upgrade'buttonstostartthesoftwareupgrade.

Figure 5-34 estimates the upgrade



5.8 Log/Diagnosis

Since each functional module has its corresponding running information, generally, users need to view the display information module by module. In order to collect more information at one time in case of routine maintenance or system failure, the device supports the diagnostic information module. When the user performs the operation of generating the diagnostic information file, the system will save the statistics information currently run by multiple functional modules in a file named 'backup-switch-year mon-day'-log 'file, which users can view to locate problems faster.

Step 1: select system [log/diagnostics] in the menu.

Step 2: click the 'backup log' button, pop up the 'file download' dialog box, and save the log file locally.

Figure 5-35 log/diagnostic interface

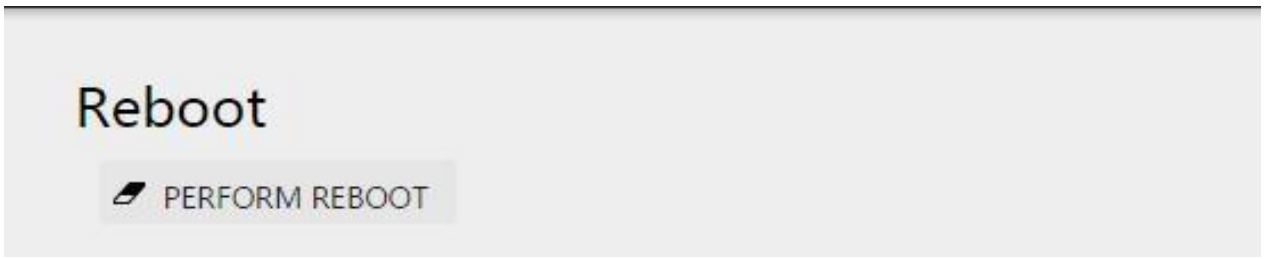
5.9 Restart

note

- Be sure to save the configuration before restarting the device, otherwise all unsaved configuration will be lost after restarting.
- After the device restarts, the user needs to log in again.

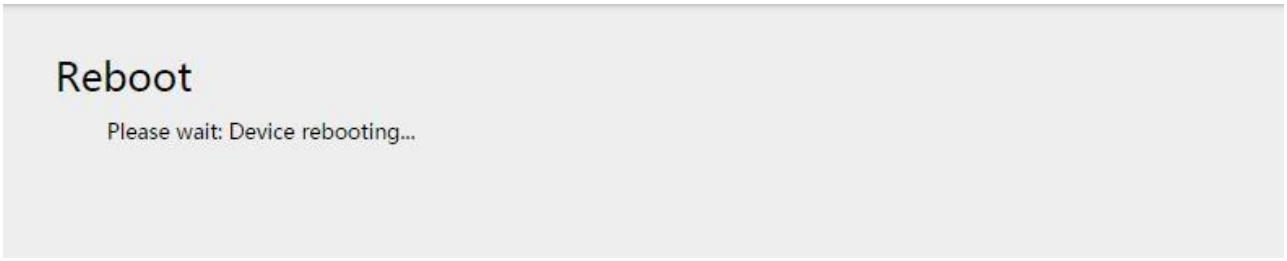
Step 1: select [system] [restart] in the menu and enter the restart interface, as shown in figure 5-36.

Figure 5-36 restart interface



Step 2: click the 'execute restart' button and wait for the device restart to complete.It will take some time for the device restart to complete. Please be patient and wait.

Figure 5-37 restart waiting interface



6 The Routing

6.1 The Routing

In the network, the router selects an appropriate path according to the destination address of the received message and forwards the message to the next router. The last router in the path forwards the message to the destination host.Routing is the path information in the forwarding process of message, which is used to guide message forwarding.

6.1.1 The Routing Table

The router selects the route through the routing table and sends the preferred route to the table of FIB (Forwarding Information Base), which instructs the Forwarding of message.Each router keeps at least one routing table and one FIB table.

The routing table contains the routes discovered by various routing protocols, which are usually divided into the following three categories according to the source:

- Direct connect routing: link-layer protocol discovery routing, also known as interface routing.
- Static routing: routing manually configured by the network administrator. Static routing configuration is convenient, low requirements for the system, suitable for simple topology and stable small network. The disadvantage is that whenever the network topology changes, it needs to be reconfigured manually and cannot be automatically adapted.
- Dynamic routing: routing discovered by dynamic routing protocols.

Each forwarding item in the FIB table indicates which physical interface of the router should be used to send a message to a subnet or host to reach the next router in that path, or to the destination host in the directly connected network without passing through another router.

6.1.2 Static Routing

A static route is a special route that is manually configured by an administrator.When networking is simple, you only need to configure static routing to make the network work properly.

Static routing cannot automatically adapt to changes in network topology. When the network fails or the topology changes, the configuration must be manually modified by the network administrator.

6.1.3 Configure Static Routing

View the static routing configuration

Select [route] [static route] in the menu and enter the static route display page, as shown in figure 6-1. The static routing configuration can be displayed in the 'overview', and the parameters are described in table 6-1.

Figure 6-1 static routing display interface

Table 6-1 description of static routing parameters

Configuration items	Instructions
The prefix IP	That is, routing prefix address, or routing network segment; For example, a common route is 0.0.0.0/0 192.168.1.1, the prefix IP is 0.0.0.0
The prefix length	Length of routing network segment; For example, in the example above, the length is 0
Next address	Routing next hop addresses; For example, the next jump in the above examples is 192.168.1.1
Describe	Routing description information, optional configuration

New static route

(1) select [switch] [VLAN] in the menu to create a VLAN.

(2) in the VLAN interface, add the VLAN created in step 1 to the specified port.

(3) select [route] [VLAN interface] in the menu, enter the page shown in figure 6-2, and complete the configuration of static routing VLAN interface.
(4) select [route] [static route] in the menu and enter the page shown in FIG. 6-1. Click 'add' button to enter the static route creation interface, as shown in FIG. 6-3.
(5) configure the information of static routing. Detailed configuration information is shown in table 6-1.
(6) click the 'ok' button to complete the operation.

Figure 6-2 static routing VLAN interface interface

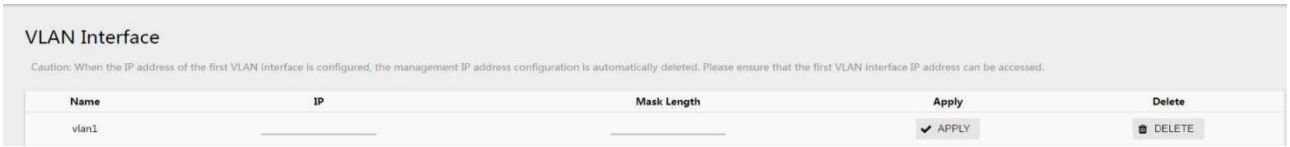


Figure 6-3 new static routing interface

note

When the first VLAN interface IP is configured, the administrative IP address is automatically removed.So in order to keep the IP address accessible,
Set the first VLAN interface to the device's administrative IP.
Take the defaultmanaged IP: 192.168.1.168, IP belongs to VLAN1 as an example, as shown in the figure below
First, migrate the device's management IP to the VLAN interface configuration.

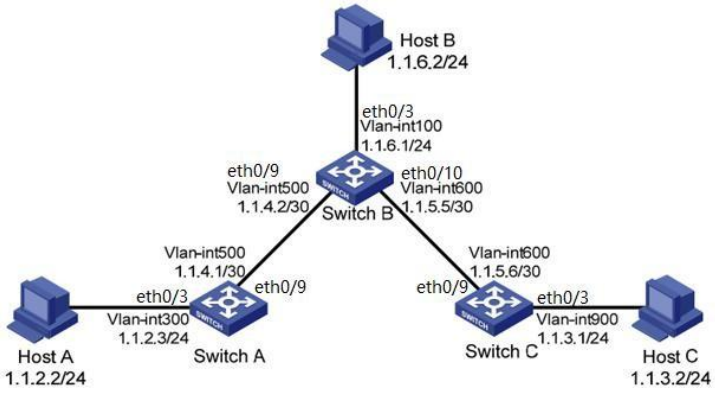
6.1.4 Configure Static Routing Examples

1. Networking requirements

IP addresses and masks of Switch A, Switch B and Switch C interfaces and hosts are shown in figure

6-4.When IPv4 static routing is required between Switch A, Switch B, and Switch C, any two hosts in the figure can communicate.

Figure 6-4 static routing configuration network diagram



2. Configure ideas

Configure IPv4 static routing using the following approach:

(1) VLAN creation and physical port VLAN partition.

(2) configure the SVI port IP address of the device.

(3) route planning: A and C are configured with default route to B, and B is configured with static route to A and C respectively according to network segment.

3. Configuration steps

Configure the Switch A

(1) Create VLAN 300 and 500

Select [VLAN] from the sub-item [switch] in the menu to enter the VLAN configuration interface. In the sub-page of VLAN, click the button [add], as shown in figure 6-5, to create VLAN300 and VLAN500.

Figure 6-5 creating a VLAN interface

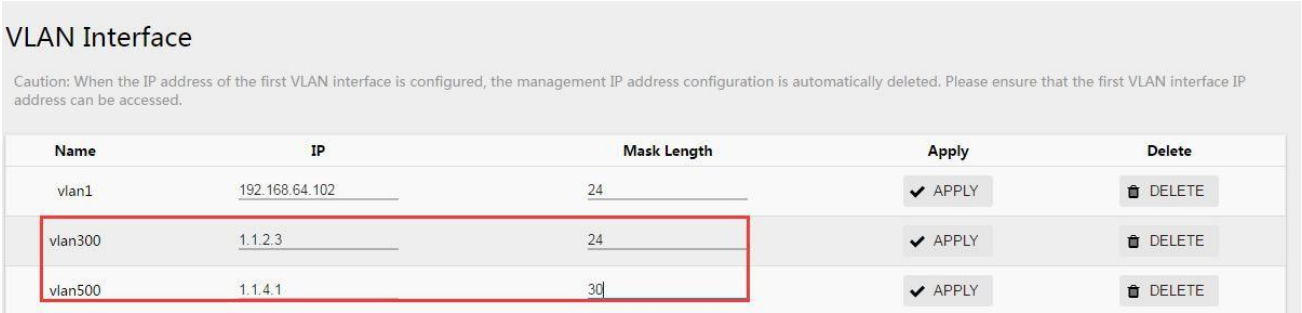
(2) VLAN mode configured for port 3 is access, VLAN 300, and VLAN mode configured for port 9 is access, VLAN500.
Select [VLAN] from the sub-item [switch] in the menu to enter the VLAN configuration interface. In the interface of port eth0/3, click the button [edit] to enter the configuration mode, as shown in FIG. 6-6.In VLAN mode, select Access and PVID 300.Do the same for port 9.

Figure 6-6 configure the interface VLAN pattern

(3) Configure SVI 300 and 500 IP addresses

Select [VLAN interface] from the sub-item [route] in the menu and enter the VLAN interface configuration interface, as shown in figure 6-7. Add SVI addresses of VLAN300 and VLAN500.

Figure 6-7 static routing VLAN interface configuration



(4) Configure the default route to Switch B

Select 'static route' from the sub-item of 'route' in the menu, enter the static route overview interface, and click 'add' button, as shown in figure 6-8, to complete the static route configuration.

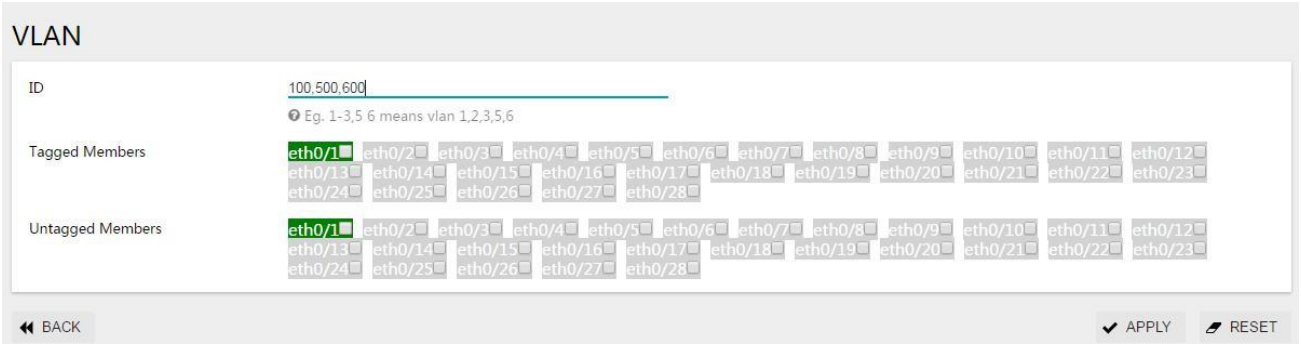
Figure 6-8 static routing configuration

Configure the Switch B

(1) Create VLAN 100,500 and 600.

Select [VLAN] from the sub-item [switch] in the menu to enter the VLAN configuration interface. In the sub-page of VLAN, click the button [add], as shown in figure 6-9, to create VLAN100, VLAN300 and VLAN500.

Figure 6-9 create a VLAN interface



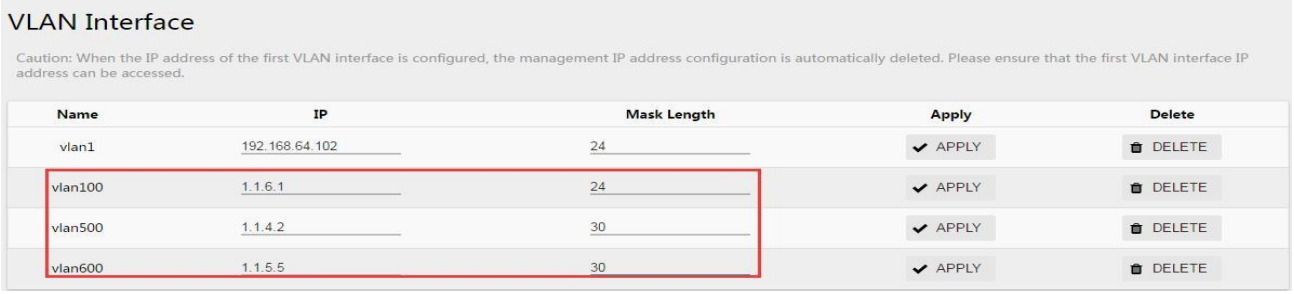
(2) VLAN mode configured for port 3 is access, VLAN 100, VLAN mode configured for port 9 is access, VLAN500, VLAN mode configured for port 10 is access, VLAN 600.
Select [VLAN] from the sub-item [switch] in the menu to enter the VLAN configuration interface. In the interface of port eth0/3, click the button [edit] to enter the configuration mode, as shown in figure 6-10.In VLAN mode, select Access and PVID 100.Do the same for ports 9 and 10.

Figure 6-10 configure the interface VLAN pattern

(3) Configure SVI 100, 300, and 500 IP addresses

Select [VLAN interface] from the sub-item [route] in the menu and enter the VLAN interface configuration interface, as shown in figure 6-11. Add SVI addresses of VLAN100, VLAN300 and VLAN500.

Figure 6-11 static routing VLAN interface



(4)Configure routing to Switch A and Switch C

Select 'static route' from the sub-item of 'route' in the menu, enter the static route overview interface, and click 'add' button, as shown in pictures 6-12 and 6-13, to complete the static route configuration.

Figure 6-12. Static routing configuration

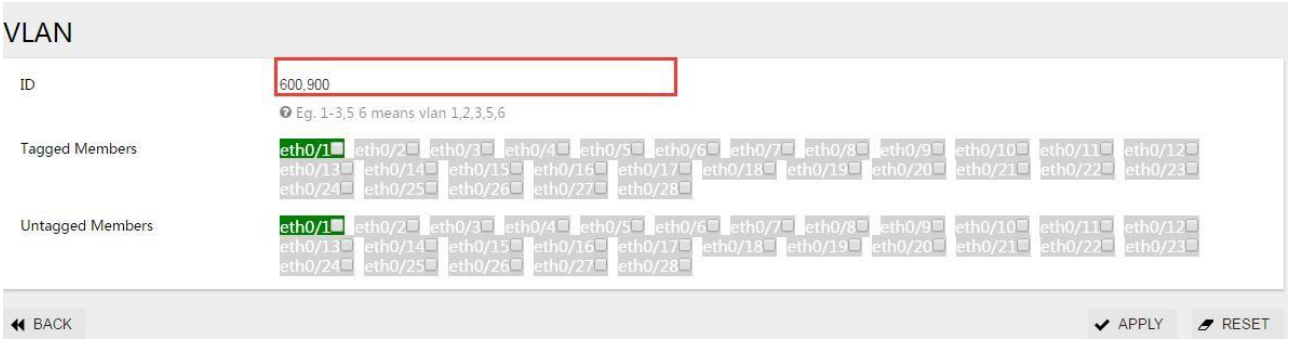
Figure 6-13. Static routing configuration

Configure the Switch C

(1) Create VLAN 100,500 and 600.

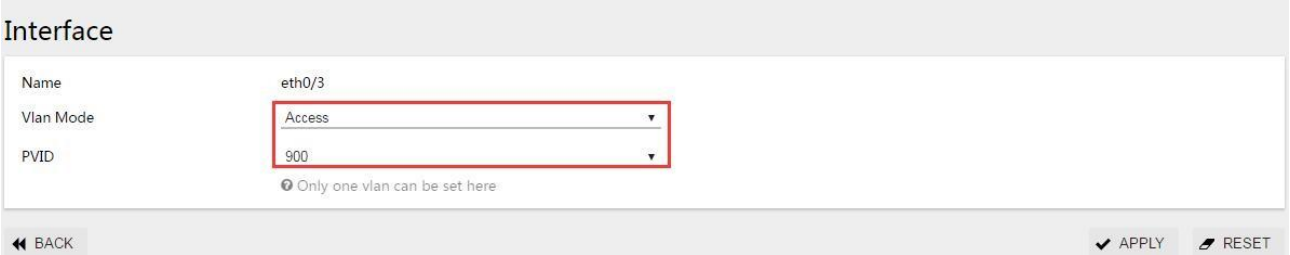
Select [VLAN] from the sub-item [switch] in the menu to enter the VLAN configuration interface. In the sub-page of VLAN, click the button [add], as shown in figure 6-14, to create VLAN600 and VLAN900.

Figure 6-14 create a VLAN interface



(2) VLAN mode configured for port 3 is access, VLAN 900, and VLAN mode configured for port 9 is access, VLAN600. Select [VLAN] from the sub-item [switch] in the menu to enter the VLAN configuration interface. In the interface of port eth0/3, click the button [edit] to enter the configuration mode, as shown in FIG. 6-15.In VLAN mode, select Access and PVID 900.Do the same for port 9.

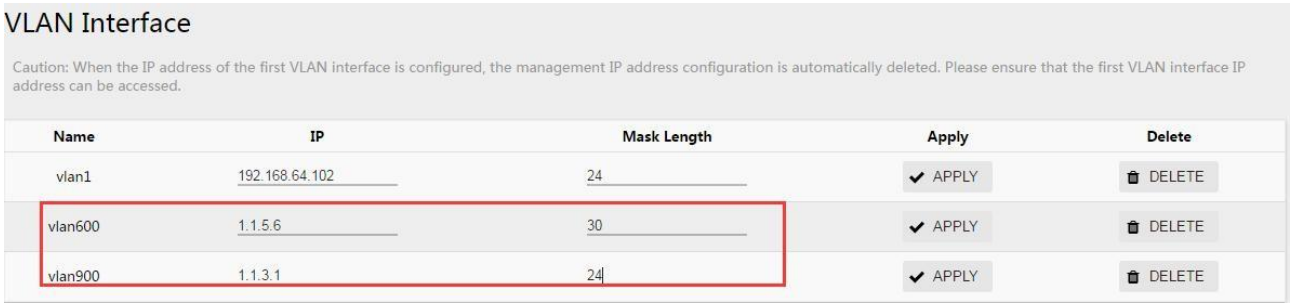
Figure 6-15 configure the interface VLAN pattern



(3) Configure SVI 100, 300, and 500 IP addresses

Select [VLAN interface] from the sub-item [route] in the menu and enter the VLAN interface configuration interface, as shown in figure 6-16. Add SVI addresses of VLAN600 and VLAN900.

Figure 6-16 static routing VLAN interface



(4) Configure the default route to Switch B

Select 'static route' from the sub-item of 'route' in the menu, enter the static route overview interface, and click 'add' button, as shown in figure 6-17, to complete the static route configuration. Figure 6-17. Static routing configuration

4. Configuration result verification

(1) view the active route list.

Enter the IPv4 routing display page of Switch A, Switch B and Switch C respectively.See the list of active routes on the page for newly configured static routes.

(2) use ping command on Host A to verify whether Host C is reachable.

C: \ Documents and Settings \ Administrator > ping 1.1.3.2

Pinging 1.1.3.2 with 32 bytes of data:

Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Ping statistics for 1.1.3.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms

6.2 Management of ARP

6.2.1 Overview

ARP (Address Resolution Protocol) is a Protocol that resolves IP addresses into Ethernet MAC addresses (or physical addresses).
In a LAN, when a host or other network device has data to send to another host or device, it must know the network layer address (IP address) of that host or device. However, IP address alone is not enough, because IP data packets must be encapsulated into frames before they can be sent through the physical network, so the sending station must also have the physical address of the receiving station, so a mapping from IP address to physical address is required. ARP is the protocol that implements this functionality.

ARP table

After the device parses the destination MAC address through ARP, it will add a mapping table item of IP address to MAC address in its own ARP table for subsequent forwarding of messages to the same destination.
ARP table items are divided into dynamic ARP table items and static ARP table items.

1. Dynamic ARP table entries

Dynamic ARP table entries are automatically generated and maintained by ARP protocol through ARP messages, which can be aged, updated by new ARP messages, and overwritten by staticARP table entries. The corresponding dynamic ARP table entry is deleted when the aging time and interface down are reached.

2. Static ARP table entries

StaticARPtableitemsaremanuallyconfiguredandmaintainedsotheyarenotagedandoverwritten by dynamic ARP table items.
Configuring static ARP table entries increases the security of communication. Static ARP table item can only use the designated MAC address when communicating with the designated IP address device. At this time, attack message cannot modify the mapping relationship between the IP address and MAC address of this table item, thus protecting the normal communication between the device and the designated device.

6.2.2 Configure ARP Management

View ARP table entries

Select [route] [ARP] in the menu and enter the ARP display page, as shown in figure 6-18. ARP table item information can be found in 'profile', and each parameter description is shown in table 6-2.

Figure 6-18 ARP table item information

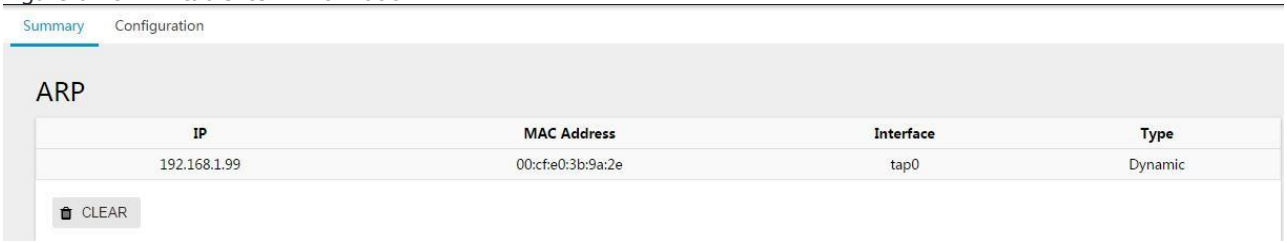


Table 6-2 ARP table item parameter description

Configuration items	Instructions	
IP	Terminal IP address	
The MAC address	Terminal MAC	Address
Interface	The name of the three-tier interface where the terminal resides	
type	ARP address type	

Configure ARP table entries

(1) select [route] [ARP] in the menu and enter the ARP profile interface. Click the'configuration' TAB to enter the ARP configuration interface, as shown in FIG. 6-19.

(2) click the 'add' button to enter the static routing creation interface, as shown in figure 6-20;

(3) configure the static routing information, as shown in table 6-2;

(4) click the 'ok' button to complete the operation.

Figure 6-19 new static routing interface

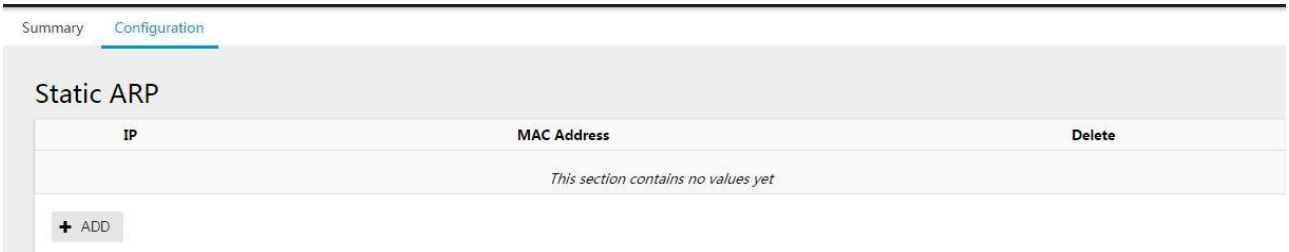


Figure 6-20 new static routing interface

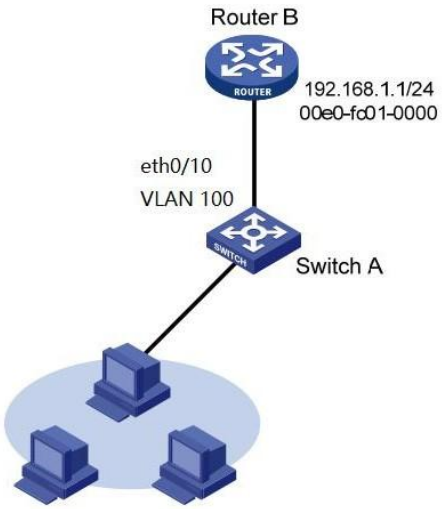
6.2.3 Examples of Configuring ARP

1. Networking Requirements

- Switch A connects to the host and Router B via the interface eth0/10.
- The interface eth0/10 belongs to VLAN 100.
- The IP address of Router B is 192.168.1.1/24, and the MAC address is 00e0-fc01-0000.

To increase the security of Switch A and Router B communication, static ARP table entriescan be configured on Switch A.

6-21 static ARP configuration networking diagram



2. Configuration Steps

(1) Create VLAN 100.

Select [VLAN] from the sub-item of [switch] in the menu to enter the VLAN configuration interface. In the sub-page of VLAN, click [add] button to create VLAN100, as shown in figure 6-22.

Figure 6-22 new VLAN interface

(2) VLAN mode of port 10 is access and VLAN 100.

Select [VLAN] from the sub-item of [switch] in the menu to enter the VLAN configuration interface. In the interface of interface, select port eth0/10 and click the button [edit] to enter the configuration mode, as shown in figure 6-23.In

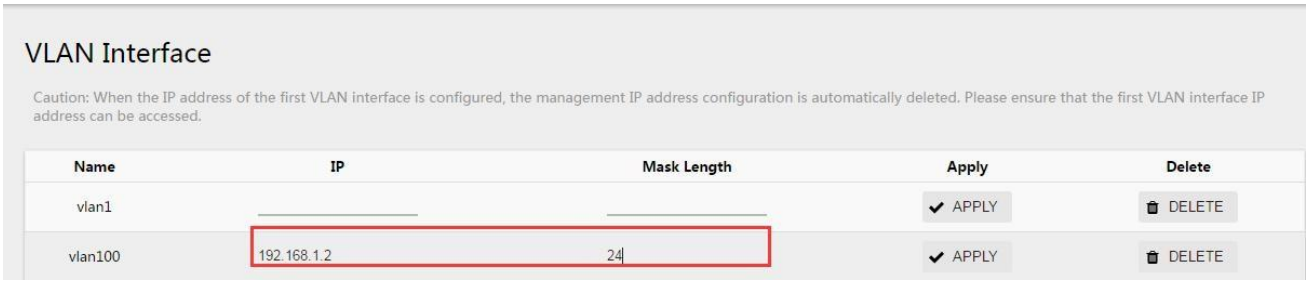
VLAN mode, select Access and PVID 100.

Figure 6-23 interface VLAN pattern

(3) Configure the interface IP address of VLAN 100

Select [VLAN interface] from the sub-item [route] in the menu to enter the VLAN interface configuration interface, as shown in figure 6-24, and add the SVI address of VLAN100.

Figure 6-24 static routing VLAN interface configuration



(4) configure Router B as static ARP

Select [route] [ARP] in the menu and enter the ARP profile interface. Click the 'configuration' TAB to enter the ARP configuration interface, as shown in figure 6-25, and add static ARP.

Figure 6-25 ARP configuration page

7 Diagnosis

7.1 Network Tools

7.1.1 Overview

ping

Using the ping tool, users can check the availability of devices with specified IP addresses and test for network connectivity failures. The successful execution of ping is:

(1) the source device sends ICMP ECHO-REQUEST message to the destination device.

(2) after receiving the request message, the destination device sends ICMP echo-reply messageto the source device.

(3) after receiving the reply message, the source device displays relevant statistical information. The output information of ping can be divided into the following situations:

- ping can be performed to the IP address or host name of the destination device, and if the host name of the destination device is not recognized, then a prompt message is printed on the sourcedevice.

• if the internal source device does not receive the ICMP echo reply message from the destination device within the timeout period, then the prompt message and statistical information of the ping process message will be output;If the internal source device receives the response message in the timeout, it will output the number of bytes, message sequence number, TTL (Time to Live), response Time and the statistics of the ping process message. The statistics of ping include the number of messages sent, the number of messages received, the percentage of messages not responded, the minimum value, average value and maximum value of response time.

Trace the route

Using the trace route tool, users can view the three-tier devices through which messages travel from source to destination.When the network fails, users can use this command to analyze the failed network nodes. The execution process of trace route is as follows:
(1) the source device sends a TTL message to the destination device.

(2) the first hop (that is, the first three-tier device that the message arrives at) responds to an ICMP TTL timeout message (which contains the IP address of the first hop), so that the source device gets the address of the first three-tier device.
(3) the source device resends a TTL message of 2 to the destination device.

(4) the second hop responds to a TTL timeout ICMP message, so the source device gets the address of the second three-tier device.
(5) the above process continues until the destination device is finally reached, and the source device gets the addresses of all three layers of devices passing from it to the destination device.
The trace route execution object can be the IP address or host name of the destination device, if the host name of the destination device is not recognized,

The prompt message is output on the source device.

7.1.2 Ping and Trace Route Operation

ping

(1) select [diagnosis] [network tools] in the menu and enter the ping/trace route page, as shown in fig.7-1. Enter the IP address in the ping operation IP address bar and click the ping button.

Figure 7-1 ping operation interface

(2) check the results of ping operation in the information box below, as shown in figure 7-2.

Figure 7-2 the ping operation returns results

```
PING 192.168.1.99 (192.168.1.99) 56(84) bytes of data.
64 bytes from 192.168.1.99: icmp_req=1 ttl=128 time=0.714 ms
64 bytes from 192.168.1.99: icmp_req=2 ttl=128 time=0.544 ms
64 bytes from 192.168.1.99: icmp_req=3 ttl=128 time=0.483 ms
64 bytes from 192.168.1.99: icmp_req=4 ttl=128 time=0.558 ms
64 bytes from 192.168.1.99: icmp_req=5 ttl=128 time=0.466 ms

--- 192.168.1.99 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.466/0.553/0.714/0.087 ms
```

Trace the route operation

(1) select [diagnosis] [network tools] in the menu and enter the ping/trace route page, as shown in fig.7-1. Enter the IP address in the ping operation IP address bar and click the ping button.

Figure 7-3 trace route operation interface

Figure 7-4 trace route operation returns the result

(2) check the results of ping operation in the information box below, as shown in figure 7-2.

```
traceroute to 14.215.177.39 (14.215.177.39), 30 hops max, 60 byte packets
 1  192.168.10.1  0.819 ms
 2  113.90.244.1  3.770 ms
 3  202.105.152.81  17.808 ms
 4  *
 5  113.96.0.18  11.972 ms
 6  219.135.96.94  14.489 ms
 7  14.29.121.182  9.820 ms
```

7.2 Dying Gasp

7.2.1 Overview

The Dying- pant function provides power supply for the moment when the equipment is cut off, and relies on 10-20ms of power supply time for energy storage devices such as capacitors inside the equipment to support the equipment to send out power warning messages.
According to the definition in 802.3ah, when the power failure event occurs, the device will send the OAM event message to the connected device. Since OAM is a point-to-point protocol, the power failure event message will not continue to be forwarded after it reaches the next oam-supporting device.The device receiving the power failure event will output the power failure LOG message.
In addition to the OAM warning message, the power failure device also sends a trap message to the SMMP server.

Node information	Data
The Mib files	DOT3 OAM - MIB. MIB
The oid	One, three, six, one, two, one, 158, one, six, one, four
The value	DyingGaspEvent (257)

7.2.2 Configure Gasp

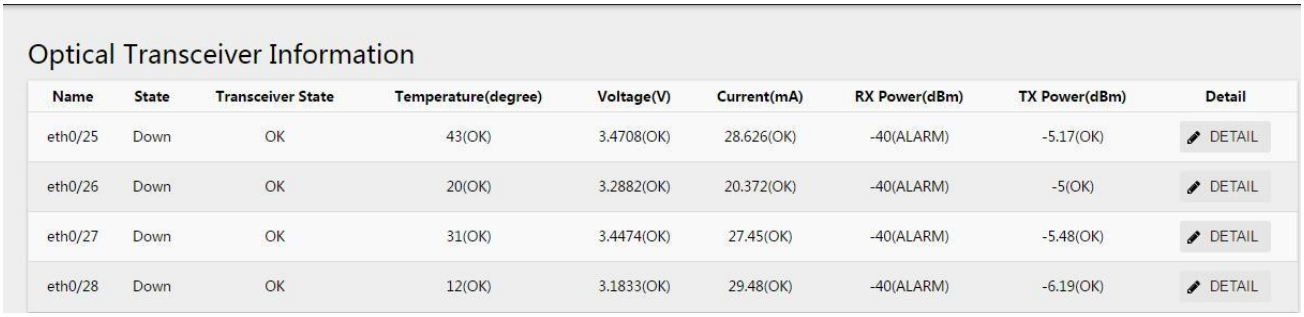
Choose 'Diagnosis' from the menu and go to the Dying pant power alarm page, as shown in figure 7-5, and click on the enable/disable button to enable or turn off the Dying pant feature, which is off by default.

Figure 7-5 trace route operation returns the result

7.3 Optical Transceiver Information

Select 'Diagnosis' and 'Optical Transceiver information' in the menu to enter the Optical Transceiver information monitoring page. As shown in figure 7-6, the digital diagnostic information of the optical module can be inquired.

Figure 7-6 digital diagnostic information of optical module



Click the detail button to query the supplier, serial number, production date and other basic information of the optical module, as shown in figure 7-7.

Figure 7-7 basic information of light module