Product Model	Classified
GPEM-R Series Industrial SW	Public
Product version	Total 129 pages
V1.6	

GPEM-R Industrial SW

Web Configuration Manual

Prepared by Mr.Zhu Date 2024-10-13

Reviewed by Pinka Liu Date 2024-10-15

Reviewed by ________ Date ________

Granted by ________ Date ________

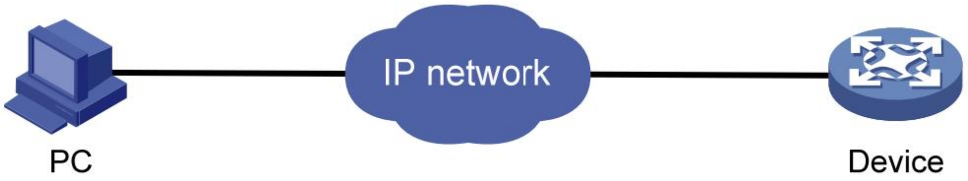
CONTENT

1 Web Overview

1.1 Brief

The device provides the Web-based network management function to facilitate the operations and maintenance on devices. Through this function, the administrator can visually manage and maintain network devices through the Web-based configuration interfaces. Figure 1-1 shows a Web-based network management operating environment:

Figure 1-1 Web-based network management operating environment



1.2 Log in to the Web Interface

The device is provided with the default Web login information. The user can use the following default information to log in to the Web interface:

- **Username**: admin
- **Password**: admin
- **IP address of the device:** 172.16.10.10

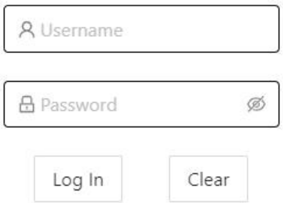
To log in to the device through the Web interface:

1. Connect the Ethernet interface of the device to the PC using a crossover Ethernet cable.
2. Configure an IP address for the PC and ensure that the PC and device can communicate with each other properly.
3. Modify the IP address of the PC to one that within the network segment 172.16.10.0/24 (except for 172.16.10.166), for example, 172.16.10.2.
4. Open the browser, and input the login information.
5. On the PC, open the browser, type the IP address http://172.16.10.166 in the address bar, press **Enter** and users can enter the login page of the Web interface, as shown in Figure 1-2. Input the username **admin** and password **admin**, and click Login.

NOTE:

- For better display results, please use Edge, Chrome or Firefox browser for that other browsers may have compatible issues.

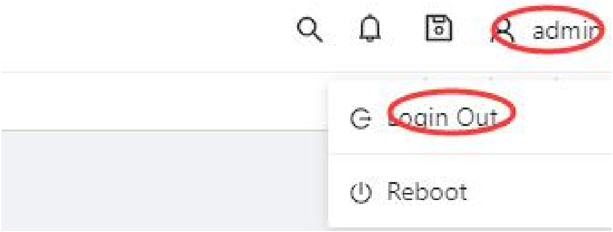
Figure 1-2 Login page of the Web interface



1.3 Log out of the Web Interface

Click **Logout** button in Auxiliary area to quit Web-based network management, as shown in Figure 1-3. The system does not save the current configuration before the user log out of the Web interface. Therefore, we recommend that the user save the current configuration before logout.

Figure 1-3 logging out of Web interface



NOTE:

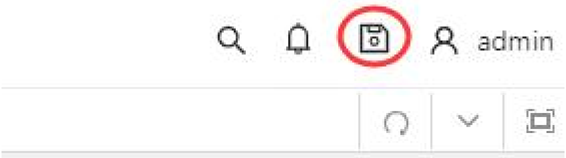
- You cannot log out by directly closing the browser.

1.4 Save Configuration

The save configuration module provides the function to save the current configuration to the configuration file for the next startup.

Click the **Save** button in Auxiliary area to save the current configuration to the configuration file, as shown in Figure 1-4.

Figure 1-4 Save configuration



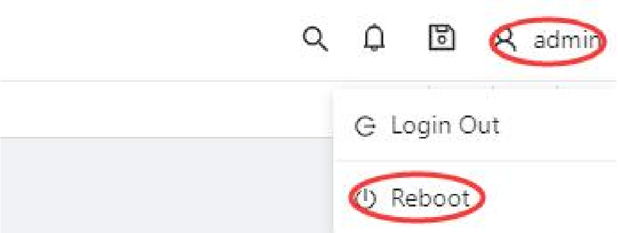
1.5 Reboot

NOTE:

- Before rebooting the device, save the configuration; otherwise, all unsaved configurations are lost after device reboot. After the device reboots, you must re-log in to the Web interface.

Click **Reboot** button ⏻ in Auxiliary area to reboot the device, as shown in Figure 1-5.

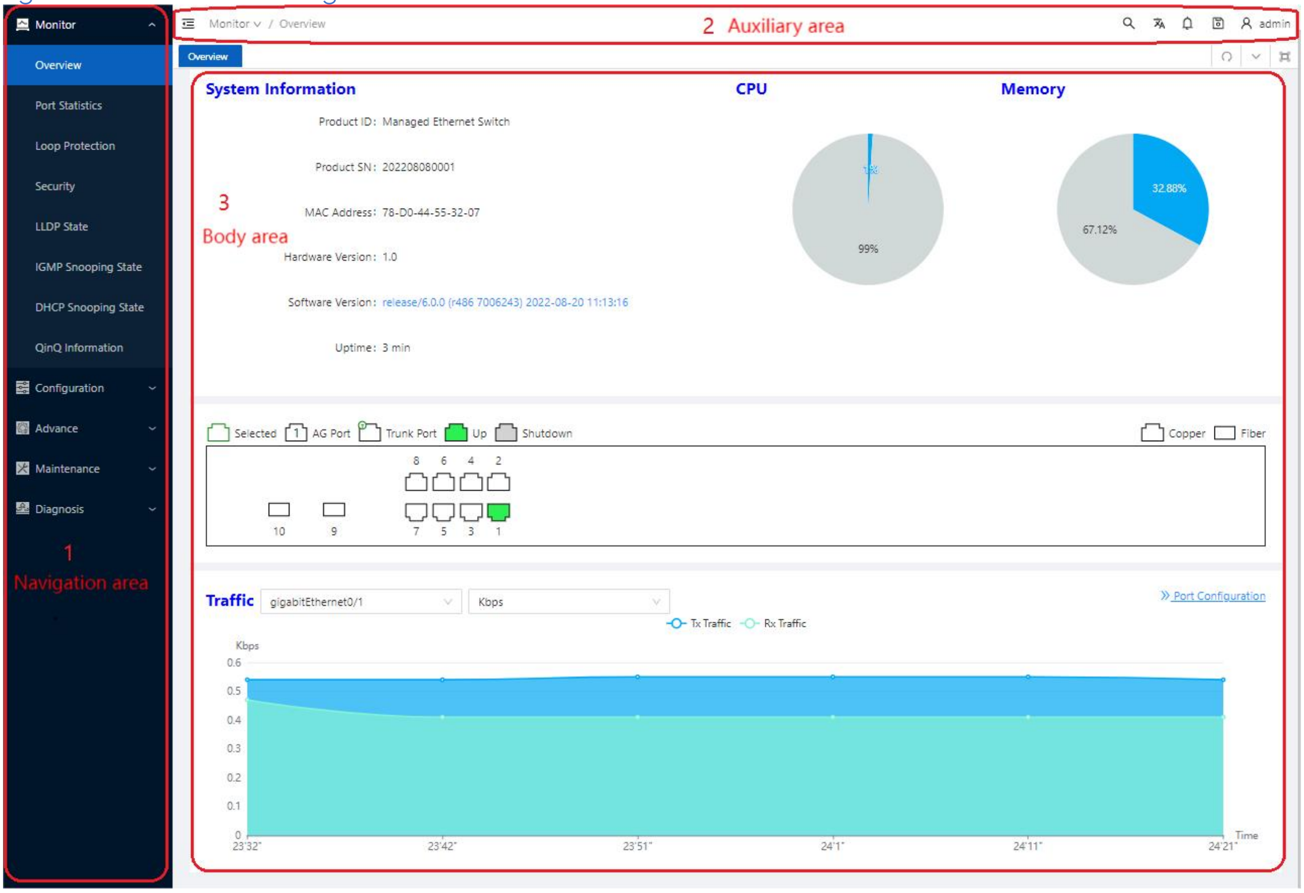
Figure 1-5 Reboot configuration



1.6 Introduction to the Web Interface

The Web interface is composed of three parts: navigation area, auxiliary area, and body area, as shown in Figure 1-6.

Figure 1-6 Web-based configuration interface



Product ID: Managed Ethernet Switch

Product SN: 202208080001

MAC Address: 78-D0-44-55-32-07

Hardware Version: 1.0

Software Version: release/6.0.0 (r486 7006243) 2022-08-20 11:13:16

Uptime: 3 min

（1）Navigation area	（2）Auxiliary area	（3）Body area

- Navigation area: Organize the Web-based NM function menus in the form of a navigation area where the user can select function menus as needed. The result is displayed in the body area. The Web network management functions not supported by the device are not displayed in the navigation area.
- Auxiliary area： The area where the user can search, alarm message prompt, save, exit, restart device, etc.
- Body area: The area where you can configure and display a function.

1.7 Introduction to the Web-based Functions

Table 1-1 describes the Web-based network management functions in detail.

Table 1-1 Description of Web-based functions

Menu/ tab			Function Description
Monitor	Overview		Display the device's MAC address, serial number, software and hardware version, CPU usage, operating status such as uptime, and the link status and flow of the port
	Port Statistics		Display the count of ports
	Loop Protection		Display the loop protection status of the device
	Security		Display the security class relating status of the device
	Serial Server State		Display the working status of the serial port server of the device
	LLDP State		Display the LLDP working status of the device
	IGMP Snooping State		Display the device’s IGMP Snooping status
	DHCP Snooping State		Display the DHCP snooping status of the device
	QinQ Information		Display the device’s QinQ status
	LoopDetect State		Display the port’s loop status
	ARP/Neighbor Information		Display the port’s ARP/neighbor information
Configuration	VLAN		Create, modify, delete VLANs, and configure port attributes and VLAN attribution
	Port	Port Configuration	Set ports’ relating properties
		Port Extension	Set ports’ rate limit, storm suppression and isolation
		Port Mirroring	Add/remove mirroring of ports

		Port Aggregation	Add/delete aggregation of ports
		Port Violation	Set the port’s violation rule
	Spanning Tree		Set STP, RSTP, MSTP
	ERPS		Set ERPS single ring, tangent ring, intersecting ring
	PoE		Set PoE power, non-standard mode. Enable/disable PoE port power supply
	Security	Port Security	Configure and delete the port’s security function
		IP Source Guard	Configure and delete the IP Source Guard function
		Dot1x	Configure 802.1X Authentication
		MAC Auth	Configure MAC Authentication Profiles
		RADIUS	Configure the RADIUS server
	Control	Serial Server	Configure serial server
		IO Control	Configure DI, DO
	LoopDetect		Configure the port’s loop detection function
Advance	Layer 2	LLDP Configuration	Configure and delete the LLDP function of the device
		IGMP Snooping Configuration	Display/Configure IGMP Snooping
		MAC Configuration	Configure the MAC address management mode of the device
		DHCP Snooping Configuration	Configure DHCP Snooping on the Device
		QinQ Configuration	Configure the QinQ function of the device
	Layer 3	ARP/Neighbor Configuration	Configure the ARP/Neighbor function
		Static Route	Configure the static route
	Security	ACL Configuration	Configure the ACL function of the device

		QoS Configuration	Configure the QoS function of the device
		DoS Configuration	Configure the DoS function of the device
Maintenance	System Configuration		Set the electronic label of the device, enable/disable Telnet, SSH, HTTP, HTTPS functions, Set management IP
	File Management		Firmware upgrade management, configuration management, certificate management, page package management
	User Management		Create/delete users, set user passwords
	Time Management		Display/set system current date and time
	SNMP		Create, modify, delete SNMP configuration
	Syslog Server		Create a new, edit, and delete the Syslog server
Diagnosis	Network Utility		Execute ping/trace route operation and display the execution result
	Transceiver Information		View optical module information, such as manufacturer information, serial number, optical power, etc.
	One-click Collection		Generate a diagnostic information file and open the file for viewing or saving to the local host
	Dying Gasp		Enable/disable the power failure alarm function of dying gasp
	Cable Detect		Check the electrical port ‘s cable status

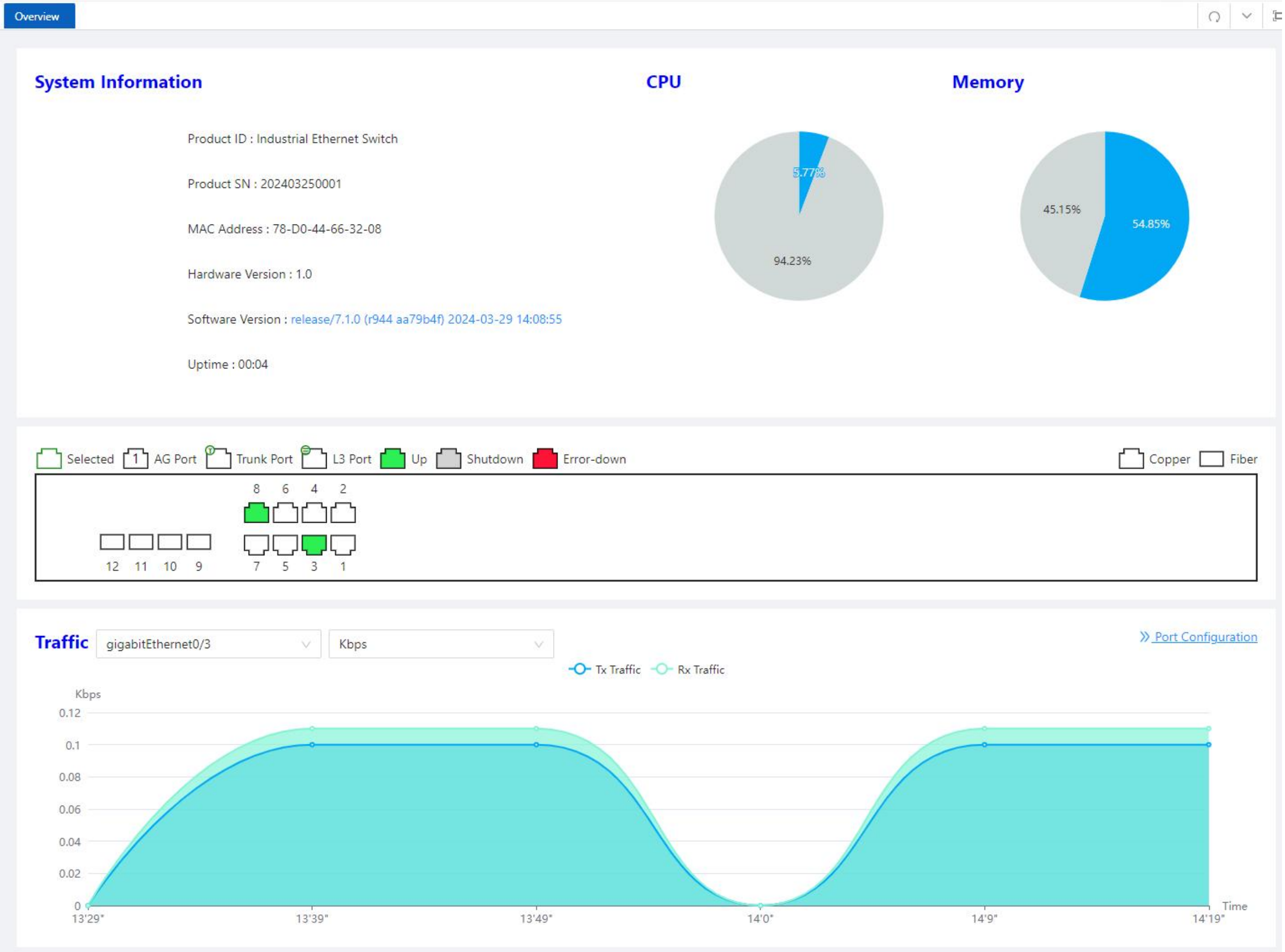
2 Monitor

2.1 Overview

Select **Monitor** > **Overview** from the navigation tree to enter the Overview page. As shown in Figure 2-1, The Overview page is divided into 3 sections, namely System Information, Panel Port, and Traffic.

1. In the **System Information** section, the user can check the product ID, serial number, MAC address, hardware and software version of the device, and the specific parameters are described as shown in Table 2-1.

Figure 2-1 Overview page



Product ID : Industrial Ethernet Switch

Product SN : 202403250001

MAC Address : 78-D0-44-66-32-08

Hardware Version : 1.0

Software Version : release/7.1.0 (r944 aa79b4f) 2024-03-29 14:08:55

Uptime : 00:04

Traffic: gigabitEthernet0/3, Kbps

Table2-1 Basic information configuration items

Item	Description
Host Name	Display the device name. Allows user to change it.
MAC Address	Display the device’s MAC address.
Hardware Version	Display the device’s hardware version.
Software Version	Display the device’s software version.

Release Date	Display the device software's release date.
Product SN	Display the device's serial number.
CPU Used	Display the device's cpu status.
Memory Avail	Display the device's memory status.
System Uptime	Display the time from last system start.

2. In the **Panel Port** section, the user can see the panel diagram of the device and the working conditions of the panel ports.

3. In the **Traffic** part, the user can observe the traffic situation of the port.

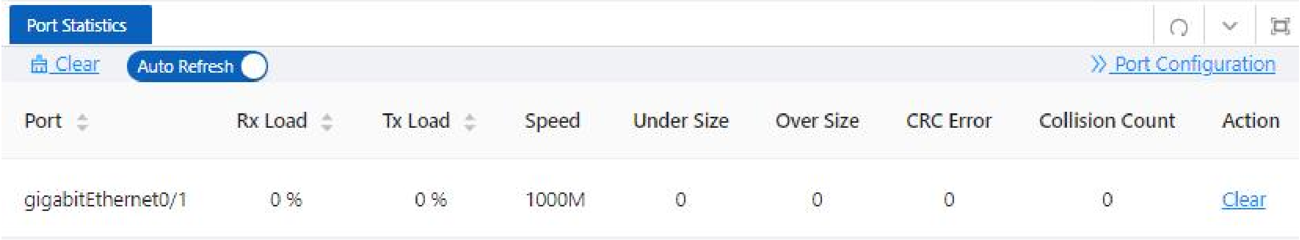
2.2 Port Statistics

The port statistics module displays statistics about the packets received and sent through ports.

Displaying Port Statistics

Select **Monitor** > **Port Statistics** in the navigation area to enter the page shown in Figure 2-2. The page displays the port's Rx Load, Tx Load, Speed, Under size, Over size, CRC Error and Collision Count. Table 2-2 describes the items of port statistics.

Figure 2-2 The port statistics page



Port	Rx Load	Tx Load	Speed	Under Size	Over Size	CRC Error	Collision Count	Action
gigabitEthernet0/1	0 %	0 %	1000M	0	0	0	0	Clear

Table 2-2 The parameters of port statistics

Item	Description
Port	The name of the logical interface.
Rx Load	The port receives the load rate
Tx Load	The port sends the load rate
Speed	The port operating rate
Under Size	The number of packets received by the port is less than 64 bytes
Over Size	The number of packets received by the port is greater than the maximum MTU configuration
CRC Error	The number of packets received of CRC checking error
Collision Count	The number of conflicting packets received by the port
Clear	Click to clear the statistics.

2.3 Loop Protection

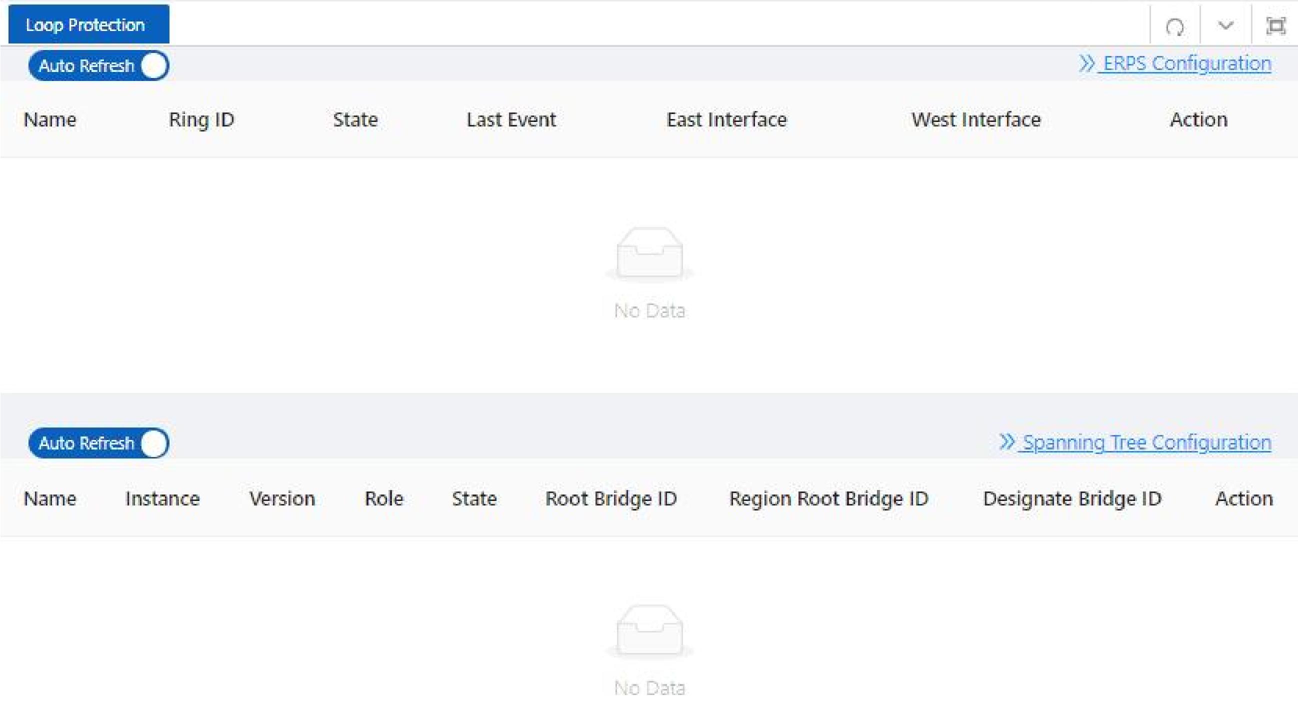
The Loop Protection page is used to display the working status of device loop-related protocols, such as ERPS and Spanning Tree Protocols.

1. Select **Monitor** > **Loop Protection** in the navigation area to enter the Loop Protection Status page, as shown in Figure 2-3.

2. The user can see the working status of the ERPS and Spanning Tree Protocol that have been enabled, and the specific parameters can be described in the relevant sections of the protocol.

3. Click the **ERPS Configuration** and **Spanning Tree Configuration** buttons to directly switch to the relevant configuration page.

Figure 2-3 Loop protection status



Name	Ring ID	State	Last Event	East Interface	West Interface	Action

No Data

Name	Instance	Version	Role	State	Root Bridge ID	Region Root Bridge ID	Designate Bridge ID	Action

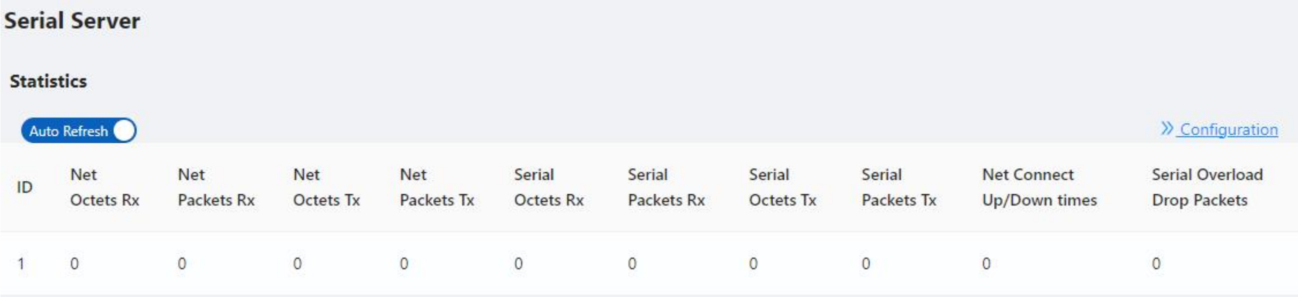
No Data

2.4 Serial Server State

The Serial Server State page is used to display the working status of Serial Server.

1. Select **Monitor** > **Serial Server State** in the navigation area to enter the Serial Server State page, as shown in Figure 2-4.

Figure 2-4 Serial server status


Serial Server

Statistics

ID	Net Octets Rx	Net Packets Rx	Net Octets Tx	Net Packets Tx	Serial Octets Rx	Serial Packets Rx	Serial Octets Tx	Serial Packets Tx	Net Connect Up/Down times	Serial Overload Drop Packets
1	0	0	0	0	0	0	0	0	0	0

2. In this page, you can see the working status of the serial server. Table 2-3 describes the items of port statistics.

Table 2-3 Items of serial server

Item	Description
ID	Serial port ID number of the serial port server
Net Octets Rx	The number of bytes received by the network
Net Packets Rx	The number of packets received by the network
Net Octets Tx	The number of bytes sent by the network
Net Packets Tx	The number of packets sent by the network
Serial Octets Rx	The number of bytes received by the serial port
Serial Packets Rx	The number of packets received by the serial port
Serial Octets Tx	The number of bytes sent by the serial port
Serial Packets Tx	The number of packets sent by the serial port
Net Connect Up/Down times	Number of network connections
Serial Overload Drop Packets	Number of packets discarded by serial port overflow

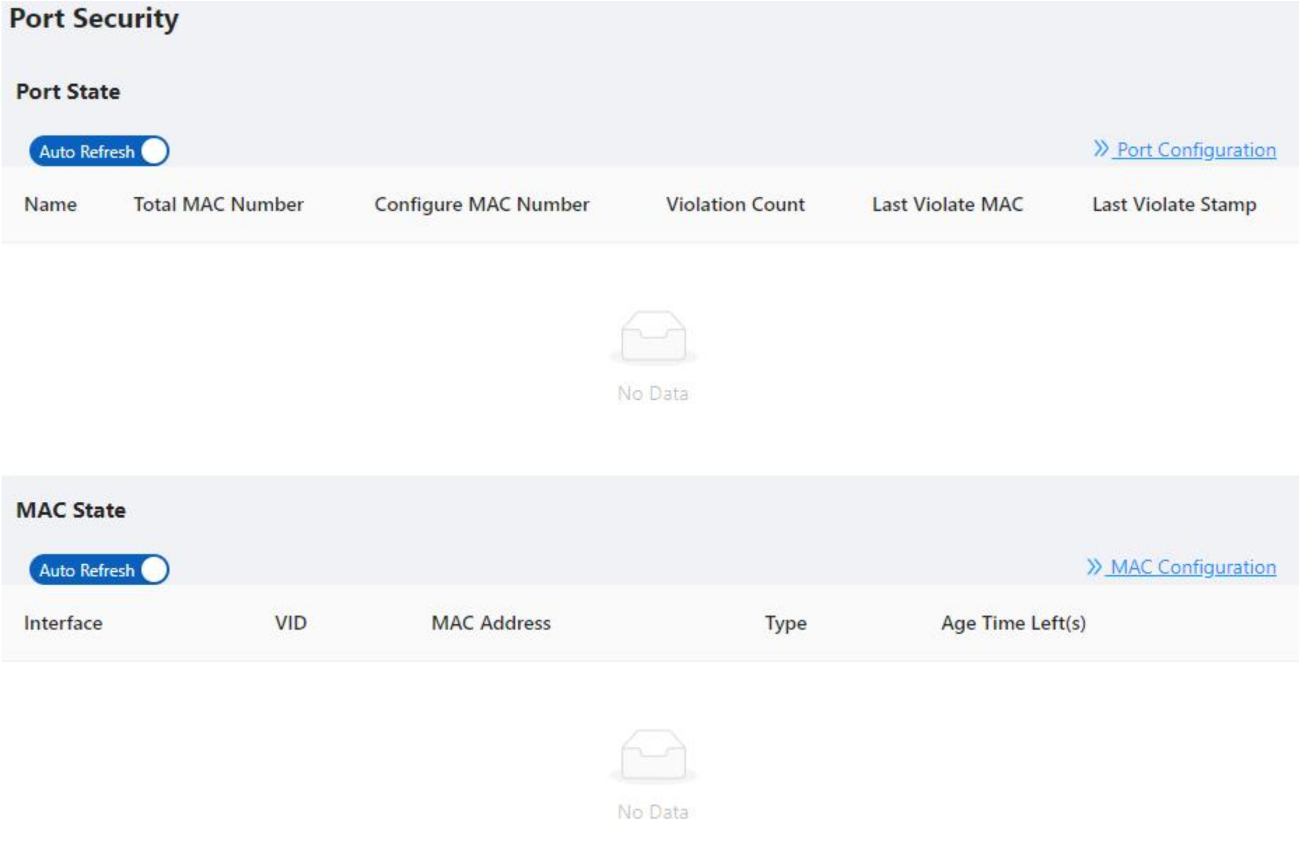
3. Click the **Configuration** button to directly switch to the relevant configuration interface.

2.5 Security

The Security page is used to display the working status of device security-related protocols, with three parts: Port Security, IP Source Guard, and MAC Auth.

1. Select **Monitor** > **Security** in the navigation area to enter the Security Display page, as shown in Figure 2-5, Figure 2-6, and Figure 2-7.

Figure 2-5 Port security state



Port Security

Port State

Name	Total MAC Number	Configure MAC Number	Violation Count	Last Violate MAC	Last Violate Stamp

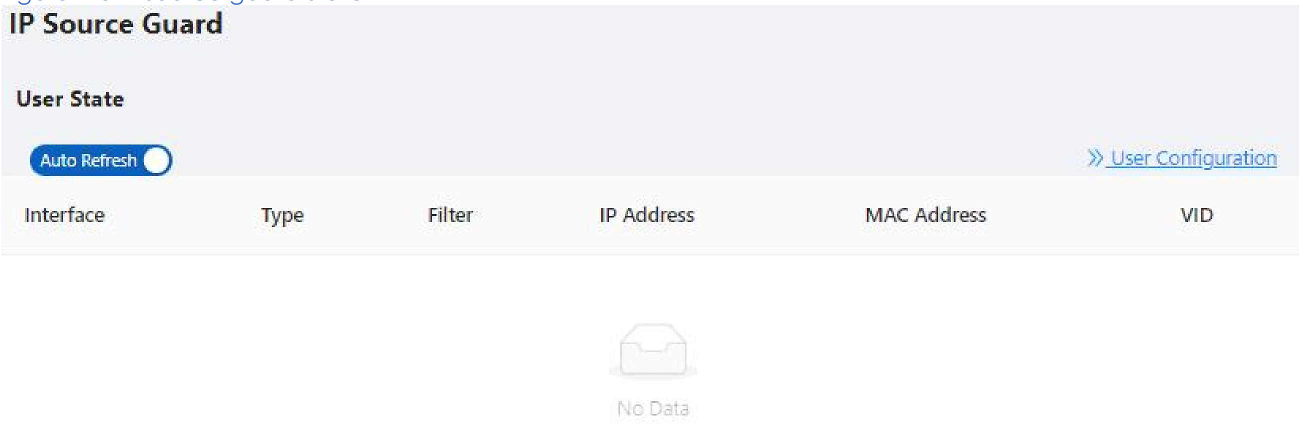
No Data

MAC State

Interface	VID	MAC Address	Type	Age Time Left(s)

No Data

Figure 2-6 IP source guard state



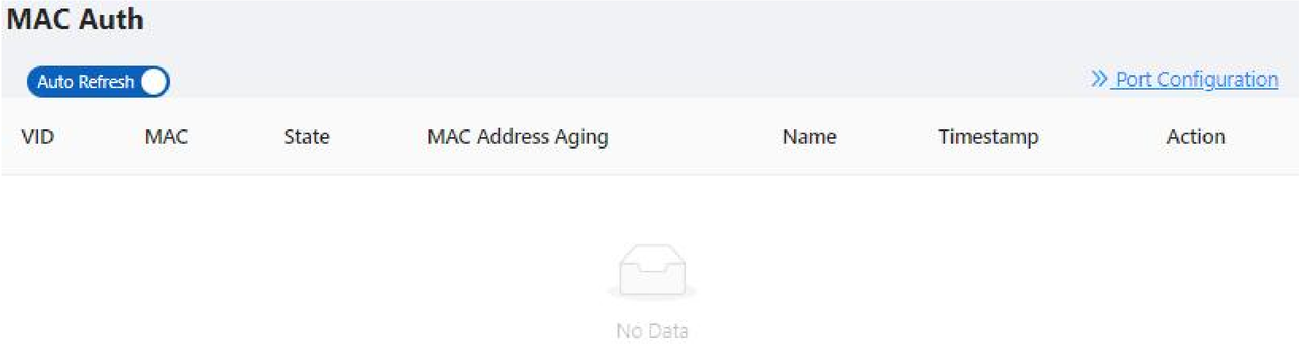
IP Source Guard

User State

Interface	Type	Filter	IP Address	MAC Address	VID

No Data

Figure 2-7 MAC auth state



MAC Auth

VID	MAC	State	MAC Address Aging	Name	Timestamp	Action

No Data

2. In this page, you can see the working status of the ERPS, Spanning tree, IP Source Guard, and MAC Auth, and the specific parameters can be described in the relevant sections of the protocol.

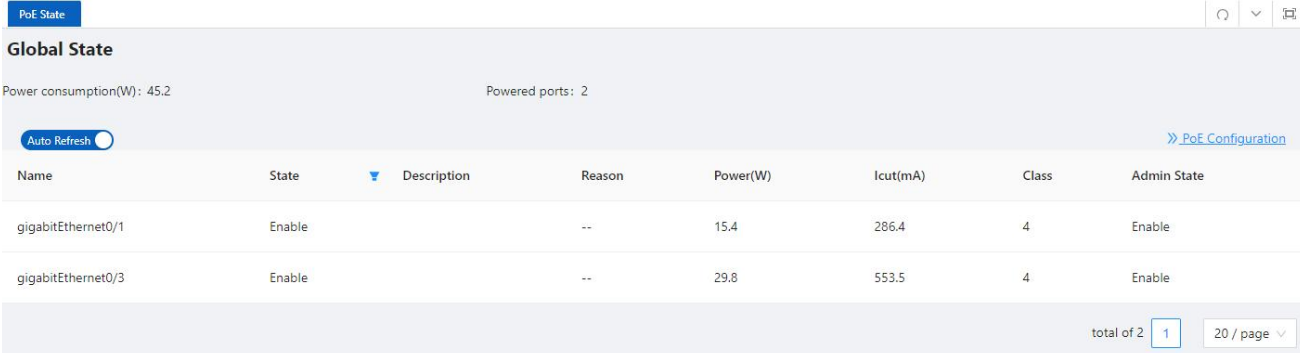
3. Click the corresponding **Configuration** button to directly switch to the relevant configuration interface.

2.6 PoE State

The PoE State page is used to display the current PoE working status of the device.

1. Select **Monitor** > **PoE State** in the navigation bar to enter the PoE Status page, as shown in Figure 2-8.

Figure 2-8 PoE state



Global State

Power consumption(W)：45.2

Powered ports：2

Name	State	Description	Reason	Power(W)	Icut(mA)	Class	Admin State
gigabitEthernet0/1	Enable		--	15.4	286.4	4	Enable
gigabitEthernet0/3	Enable		--	29.8	553.5	4	Enable

2. On the current page, the user can see the total power supply of the device, the number of power supply ports, and the power supply status of each port. Specific parameter descriptions are shown in Table 2-4.

Table 2-4 Items of PoE state

Item	Description	
Global state	Power Consumption (W)	Current PoE external power supply of the device
	Powered ports	The current total number of powered up ports
Port	Name	Indication panel port number
	State	PoE current power supply status, disable: power supply off state enable: power supply on state
	Description	PoE port description
	Reason	The reason why the port cannot supply power, Short: load short Management: insufficient power
	Power(W)	The power consumed by the current port
	Icut(mA)	The working current of the current port

	Class	Class level of the PD device connected to this port
	Admin State	Display whether the PoE function of this port is enabled or disabled

3. Click the **PoE Configuration** button to directly switch to the PoE Configuration interface.

2.7 LLDP State

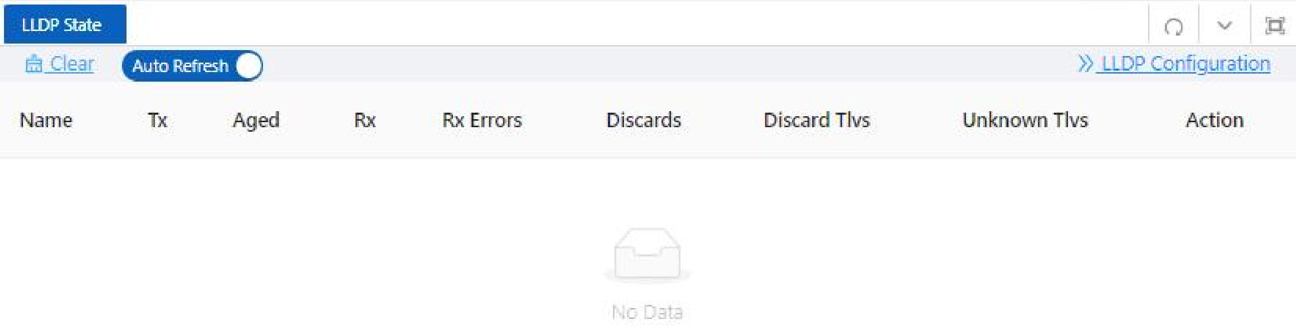
The LLDP Status page is used to display the device LLDP working status.

1. Select **Monitor** > **LLDP State** in the navigation area to enter the LLDP Status page, as shown in Figure 2-9.

2. The user can see the working status of the LLDP protocol that has been enabled in the page, and the specific parameters are described in the relevant sections of the protocol.

3. Click the **LLDP Configuration** button to directly switch to the LLDP Configuration interface.

Figure 2-9 LLDP state



Name	Tx	Aged	Rx	Rx Errors	Discards	Discard Tlvs	Unknown Tlvs	Action

No Data

2.8 IGMP Snooping State

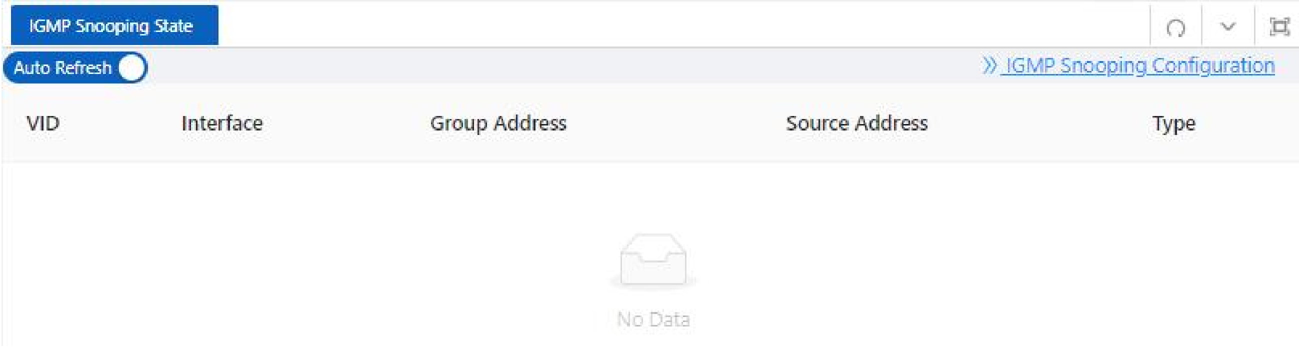
The IGMP Snooping State page is used to display the working status of the device IGMP Snooping protocol.

1. Select **Monitor** > **IGMP Snooping State** in the navigation area to enter the IGMP Snooping Status page, as shown in Figure 2-10.

2. The user can see the working status of the IGMP Snooping protocol that has been enabled in the page, and the specific parameters can be described in the relevant sections of the protocol.

3. Click the **IGMP Snooping Configuration** button to directly switch to the IGMP Snooping Configuration interface.

Figure 2-10 IGMP snooping state



VID	Interface	Group Address	Source Address	Type

2.9 DHCP Snooping State

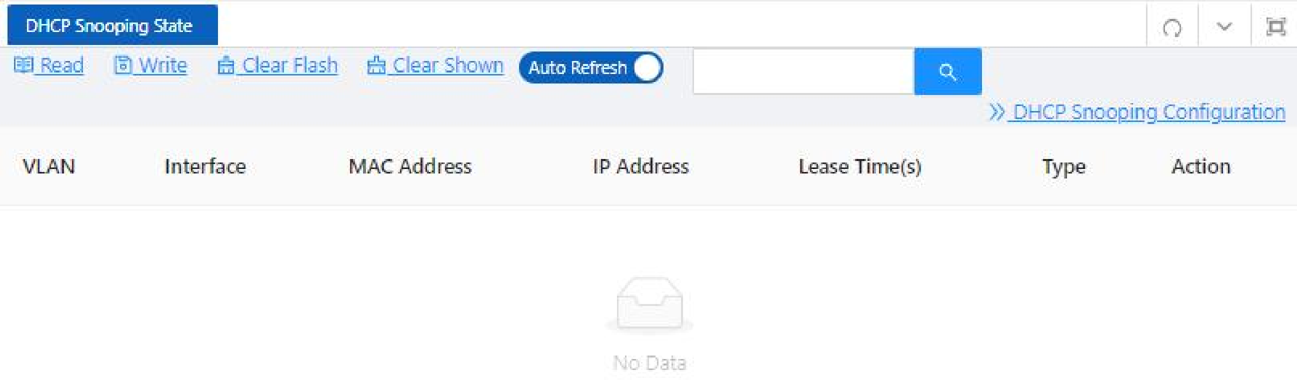
The DHCP Snooping State page is used to display the working status of the DHCP Snooping protocol of the device.

1. Select **Monitor** > **DHCP Snooping State** in the navigation area to enter the DHCP Snooping State page, as shown in Figure 2-11.

2. The user can see the working status of DHCP Snooping Protocol that has been enabled in the page, and the specific parameters can be described in the relevant sections of the protocol.

3. Click the **DHCP Snooping Configuration** button to directly switch to the DHCP Snooping Configuration interface.

Figure 2-11 DHCP snooping state



VLAN	Interface	MAC Address	IP Address	Lease Time(s)	Type	Action

2.10 QinQ Information

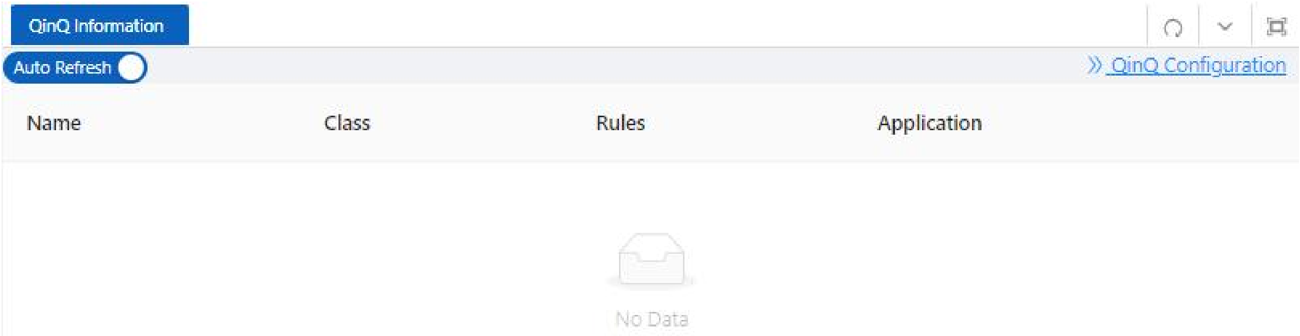
The QinQ Information page is used to display the working status of the device QinQ information.

1. Select **Monitor** > **QinQ Information** in the navigation area to enter the QinQ Status page, as shown in Figure 2-12.

2. The user can see the working status of QinQ that has been turned on in the page, and the specific parameters can be described in the relevant sections of the protocol.

3. Click the **QinQ Configuration** button to quickly switch to the QinQ Configuration interface.

Figure 2-12 QinQ information



QinQ Information

Auto Refresh

» QinQ Configuration

Name	Class	Rules	Application

No Data

2.11 LoopDetect State

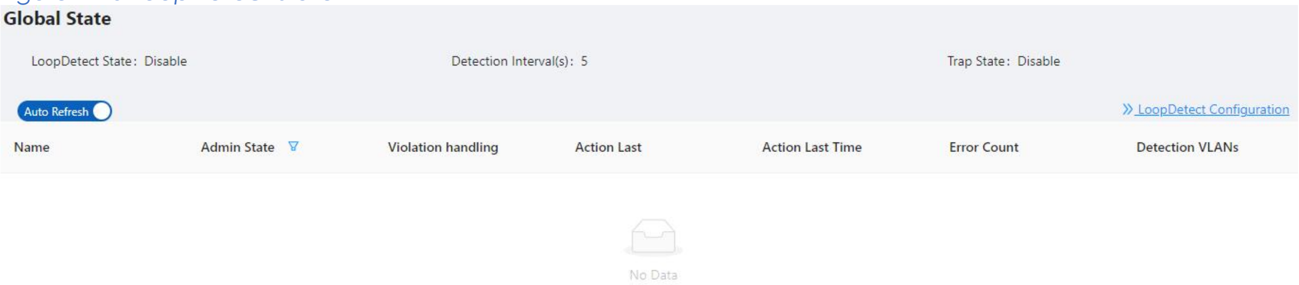
The LoopDetect State page is used to display the working status of the loop.

1. Select **Monitor** > **LoopDetect State** in the navigation area to enter the LoopDetect Status page, as shown in Figure 2-13.

2. The user can see the working status of loop detection that has been turned on in the page, and the specific parameters can be described in the relevant sections of the protocol.

3. Click the **LoopDetect Configuration** button to quickly switch to the Loopdetect Configuration interface.

Figure 2-13 LoopDetect state



Global State

LoopDetect State: Disable

Detection Interval(s): 5

Trap State: Disable

Auto Refresh

» LoopDetect Configuration

Name	Admin State	Violation handling	Action Last	Action Last Time	Error Count	Detection VLANs

No Data

2.12 ARP/Neighbor Information

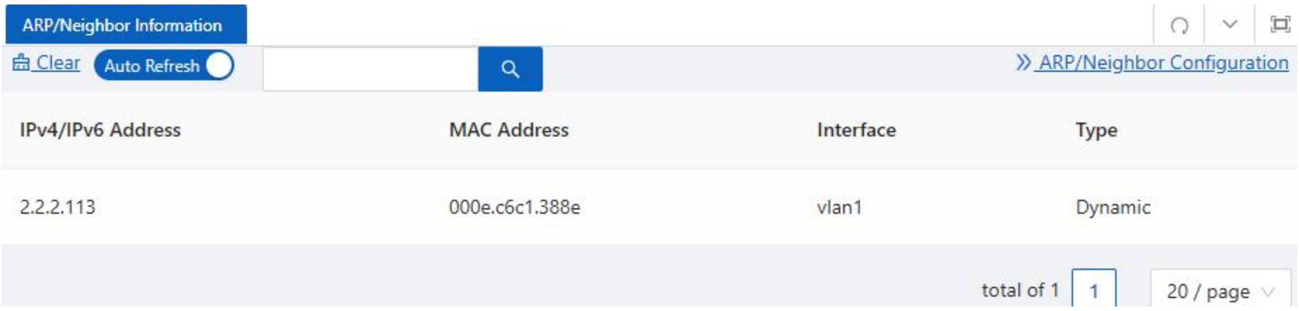
The ARP/Neighbor Information page is used to display the working status of the device ARP/Neighbor information.

1. Select **Monitor** > **ARP/Neighbor Information** in the navigation area to enter the ARP/Neighbor status page, as shown in Figure 2-14.

2. You can see the working status of ARP/Neighbor that has been turned on in the page, and the specific parameters can be described in the relevant sections of the protocol.

3. Click the **ARP/Neighbor Configuration** button to quickly switch to the ARP/Neighbor Configuration page.

Figure 2-14 ARP/Neighbor information



IPv4/IPv6 Address	MAC Address	Interface	Type
2.2.2.113	000e.c6c1.388e	vlan1	Dynamic

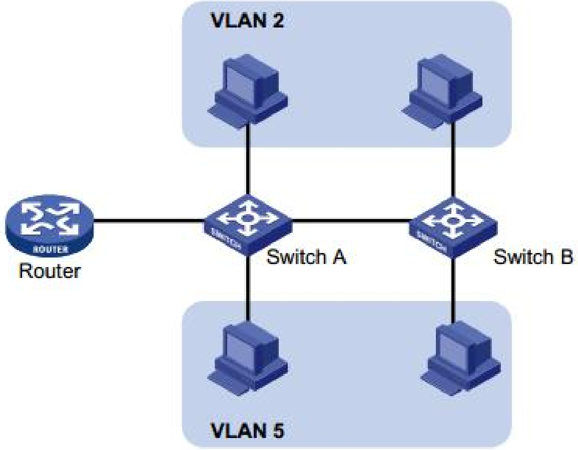
3 Configuration

3.1 VLAN

3.1.1 Introduction

Ethernet is a network technology based on the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) mechanism. As the medium is shared, collisions and excessive broadcasts are common on an Ethernet. To address the issue, virtual LAN (VLAN) was introduced. The idea is to break a LAN down into separate VLANs, that is, Layer 2 broadcast domains whereby frames are switched between ports assigned to the same VLAN. VLANs are isolated from each other at Layer 2. A VLAN is a bridging domain, and ll broadcast traffic is contained within it, as shown in Figure 3-1.

Figure 3-1 A VLAN diagram



A VLAN is logically divided on an organizational basis rather than on a physical basis. For example, all workstations and servers used by a particular work group can be connected to the same LAN, regardless of their physical locations. VLAN technology delivers the following benefits:

- Confining broadcast traffic within individual VLANs. This reduces bandwidth waste and improves network performance.
- Improving LAN security. By assigning user groups to different VLANs, you can isolate them at Layer 2. For hosts in different VLANs to communicate, routers or Layer 3 switches are required.
- Flexible virtual work group creation. As users from the same work group can be assigned to the same VLAN regardless of their physical locations, network construction and maintenance is much easier and more flexible.

The user can create VLANs based on:

- Port
- MAC address
- Protocol

- IP subnet
- Policy
- Other criteria

Because the Web interface is available only for port-based VLANs, this chapter introduces only port-based VLANs.

3.1.1.1 VLAN Mode

Depending on the tag handling mode, the VLAN Mode of a port can be one of the following three:

- Access ：

An access port belongs to only one VLAN and usually connects to a user device.

- Trunk ：

A trunk port can join multiple VLANs to receive and send traffic for them. It usually connects to a network device.

- Hybrid ：

A hybrid port can join multiple VLANs to receive and send traffic for them. It can connect either a user device or a network device.

A hybrid port is different from a trunk port in that:

- A hybrid port allows traffic of multiple VLANs to pass through untagged.
- A trunk port allows only traffic of the default VLAN to pass through untagged.

3.1.1.2 Port Link Type

By default, VLAN 1 is the default VLAN for all ports. However, you can change the default VLAN for a port as required. When doing that, follow these guidelines:

- Because an access port can join only one VLAN, its default VLAN is the VLAN to which it belongs and cannot be configured.
- Because a trunk or hybrid port can join multiple VLANs, you can configure a default VLAN for the port.

3.1.1.3 Frame Handling Methods

Table 3-1 A port configured with a default VLAN handles a frame as follows:

Port type	Actions (in the inbound direction)		Actions (in the outbound direction)
	Untagged frame	Tagged frame	
Access	Tag the frame with the default VLAN tag.	• Receive the frame if its VLAN ID is the same as the default VLAN ID • Drop the frame if its VLAN ID is different from the default VLAN ID.	Remove the default VLAN tag and send the frame.

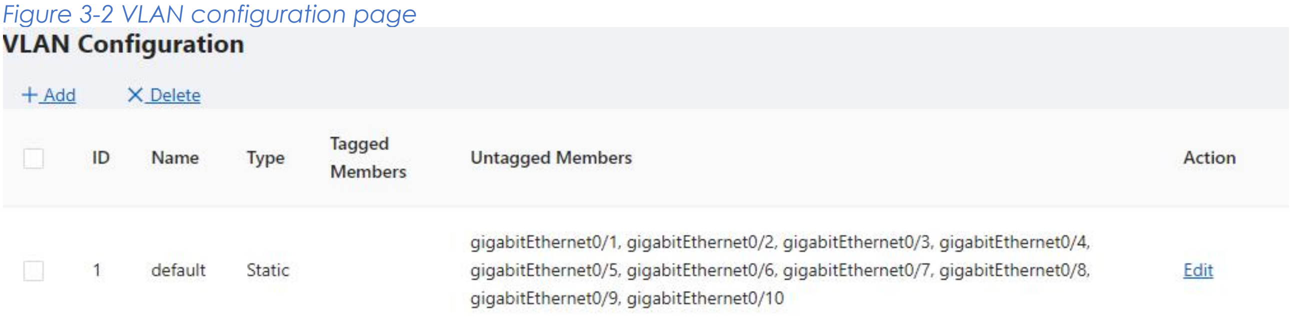
Trunk	Check whether the default VLAN is carried on the port: • If yes, tag the frame with the default VLAN tag. • If not, drop the frame.	• Receive the frame if its VLAN is carried on the port. • Drop the frame if its VLAN is not carried on the port.	• Remove the tag and send the frame if the frame Carries the default VLAN tag. • Send the frame without removing the tag if its VLAN is carried on the port but is different from the default one.
Hybrid			Send the frame if its VLAN is carried on the port. The frame is sent with the VLAN tag removed or intact depending on your configuration.

3.1.2 Configure VLAN

3.1.2.1 Creating VLAN

1. Select **Configuration** > **VLAN** in the navigation area. The system automatically enters the VLAN page as shown in Figure 3-2. Table 3-2 describes the configuration items of creating a VLAN.

Figure 3-2 VLAN configuration page



VLAN Configuration

+ Add   ✕ Delete

□	ID	Name	Type	Tagged Members	Untagged Members	Action
□	1	default	Static		gigabitEthernet0/1, gigabitEthernet0/2, gigabitEthernet0/3, gigabitEthernet0/4, gigabitEthernet0/5, gigabitEthernet0/6, gigabitEthernet0/7, gigabitEthernet0/8, gigabitEthernet0/9, gigabitEthernet0/10	Edit

Table 3-2 VLAN configuration items

Item	Description
ID	This field displays the ID of the VLAN
Name	By default, the description string of a VLAN is its VLAN ID, such as VLAN 0002.
Type	Display the type of VLAN
Tagged Members	Indicate that the port sends the traffic of the VLAN without removing the VLAN tag.
Untagged Members	Indicate that the port sends the traffic of the VLAN with removing the VLAN tag.
Edit	Click to enter the VLAN editing page
Add	Click to enter the VLAN adding page
Delete	Select the VLAN ID, click to delete

2. Click **+Add** button to enter the page for creating a VLAN, as shown in Figure 3-3.

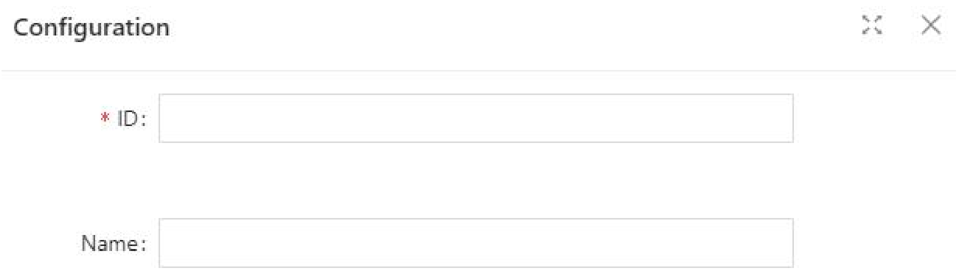
3. Type VLAN number into the **ID** box.

4. Enter a VLAN name.

5. Click **OK** to complete the configuration and click **Save** in the auxiliary area to save such configuration.

6. When you need to configure the VLAN port member, click the **Edit** button, select the port member required to join the VLAN in the port panel, and click the **OK** button to complete the operation.

Figure 3-3 Create VLAN



Configuration

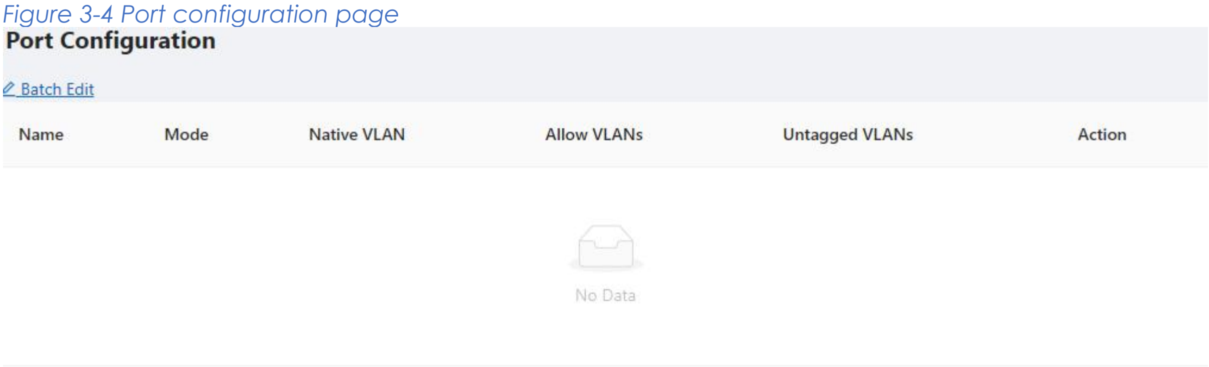
* ID:

Name:

3.1.2.2 Configure Port

1. Select **Configuration** > **VLAN** in the navigation area to enter the VLAN page as shown in Figure 3-4. Table 3-3 describes the configuration items of configuring a port.

Figure 3-4 Port configuration page



Port Configuration

Batch Edit

Name	Mode	Native VLAN	Allow VLANs	Untagged VLANs	Action

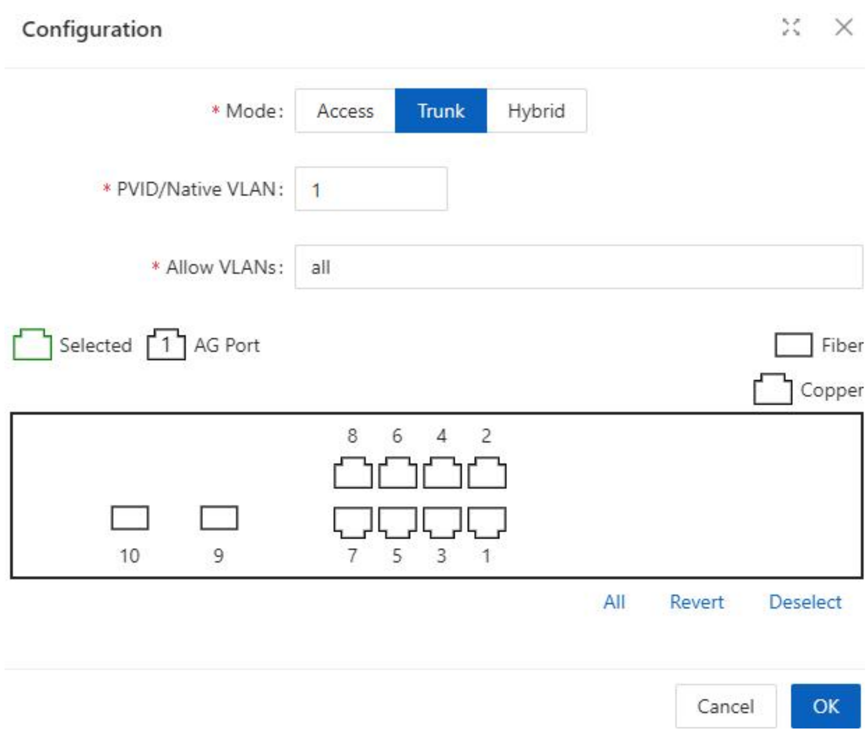
No Data

2. Click **Batch Edit** button below Port Configuration to enter the Port Configuration page, as shown in Figure 3-5. Table 3-3 describes the configuration items of configuring a VLAN.

Table3-3 The description of the trunk configuration

Item		Description
Mode	Access	Set the port’s VLAN Mode to access
	Trunk	Set the port’s VLAN Mode to trunk
	Hybrid	Set the port’s VLAN Mode to hybrid
PVID		Set the port’s default VLAN ID, only exist in access mode. The trunk ports at the two ends of a link must have the same PVID. Otherwise, the link cannot properly transmit packets
Native VLAN		VLAN（Native VLAN）, only exist in Trunk mode.
Allow VLANs		Select the VLANs that are allowed through the port.

Figure 3-5 Interface configuration page



Configuration

* Mode: Access | **Trunk** | Hybrid

* PVID/Native VLAN: 1

* Allow VLANs: all

3. Select the VLAN Mode, type VLAN number in PVID and Allow VLANs box, click **OK** button to complete the configuration.

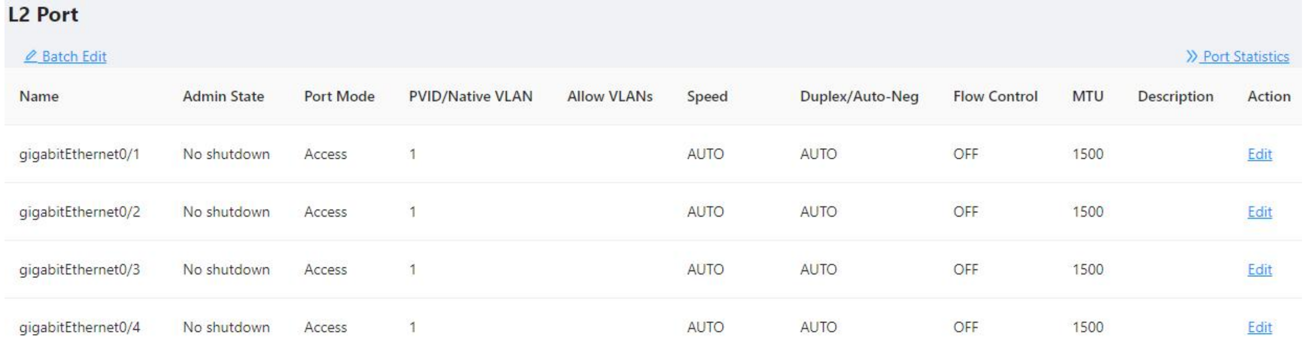
4. Click the **Save** in the auxiliary area to save the configuration.

3.2 Port

3.2.1 Port Configuration

The user can use the interface management feature to view interface information, create/remove logical interfaces, change interface status, and reset interface parameters, as shown in Figure 3-6.

Figure 3-6 Port configuration page



L2 Port

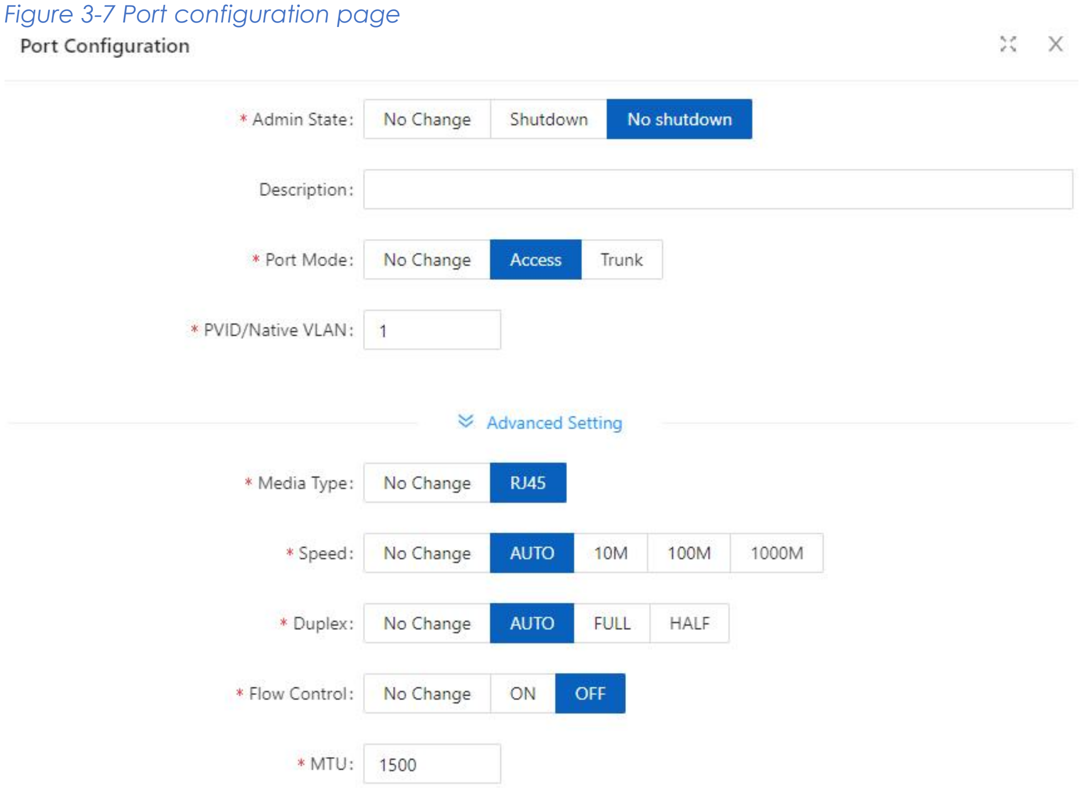
Name	Admin State	Port Mode	PVID/Native VLAN	Allow VLANs	Speed	Duplex/Auto-Neg	Flow Control	MTU	Description	Action
gigabitEthernet0/1	No shutdown	Access	1		AUTO	AUTO	OFF	1500		Edit
gigabitEthernet0/2	No shutdown	Access	1		AUTO	AUTO	OFF	1500		Edit
gigabitEthernet0/3	No shutdown	Access	1		AUTO	AUTO	OFF	1500		Edit
gigabitEthernet0/4	No shutdown	Access	1		AUTO	AUTO	OFF	1500		Edit

Configuring Interface Management

1. Select **Configuration** > **Port** > **Port Configuration** in the navigation area to enter the Port Configuration page as shown in Figure 3-6.

2. Select the ports to be configured, click **Edit** button to enter the page for configuring an interface, as shown in Figure 3-7. Table 3-4 describes the configuration items of configuring an interface.

Figure 3-7 Port configuration page



Port Configuration

* Admin State: No Change Shutdown [✓ No shutdown]

Description:

* Port Mode: No Change [✓ Access] Trunk

* PVID/Native VLAN: 1

Advanced Setting

* Media Type: No Change [✓ RJ45]

* Speed: No Change [✓ AUTO] 10M 100M 1000M

* Duplex: No Change [✓ AUTO] FULL HALF

* Flow Control: No Change ON [✓ OFF]

* MTU: 1500

Table 3-4 Configuration items of ports

Item	Description
Admin State	Shutdown/no shutdown the port.
Description	Set the description of a logical interface.
Port Mode	Set the port's vlan mode, Access or Trunk
PVID/Native VLAN	Set the port's PVID or Native VLAN.
Medium type	Set the medium type of the Combo ports • RJ45：the mode of port is 10/100/1000BASE-T • SFP：the mode of port is 1000BASE-X Note: only for combo ports.
Speed(copper)	Set the port's transmission rate: • 10: indicate 10 Mbps • 100M：indicate 100 Mbps • 1000M：indicate 1000 Mbps • Auto: indicate auto-negotiation Note: only for copper ports.

Duplex(copper)	Set the port's duplex mode: • AUTO：indicate auto-negotiation • FULL：indicate full duplex • HALF：indicate half duplex Note: only for copper ports.
Speed(fiber)	Set the port's mode • 100BASE-FX：indicate the port mode is 100BASE-FX. • 1000BASE-X：indicate the port mode is 1000BASE-X. • 2500BASE-X：indicate the port mode is 2.5G BASE-X. • 10G BASE-X: indicate the port mode is 10G BASE-X. Note: only for fiber ports.
Autoneg(fiber)	Enable or disable port's autoneg. Display The auto-negotiation function needs to be enabled or disabled at the same time as the peer end, otherwise a link failure will occur. Note: only for fiber ports.
Flow control	Enable or disable port's Flow control.
MTU	Allow or forbid jumbo frames to pass through the port. Default length of packets is 46-1500 bytes.
Admin Shutdown	Shutdown/no shutdown the port.

3.2.2 Port Extension

3.2.2.1 Rate Limiting

Port-based rate limiting allows the user to limit the speed at which network traffic is sent or received by a device that is connected to a port on the switch. Unlike 802.1p Quality of Service (QoS), port-based rate limiting does not prioritize information based on type. Rate limiting simply means that the switch will slow down traffic on a port to keep it from exceeding the limit that you set. If you set the rate limit on a port too low, you might see degraded video stream quality, sluggish response times during online activity, and other problems.

The best use of rate limiting is to keep low-priority devices that are connected to the switch from using too much of the bandwidth and slowing down your other connected devices. A combination of rate limiting and QoS can help the user maximize your network's efficiency and prioritize devices and activities.

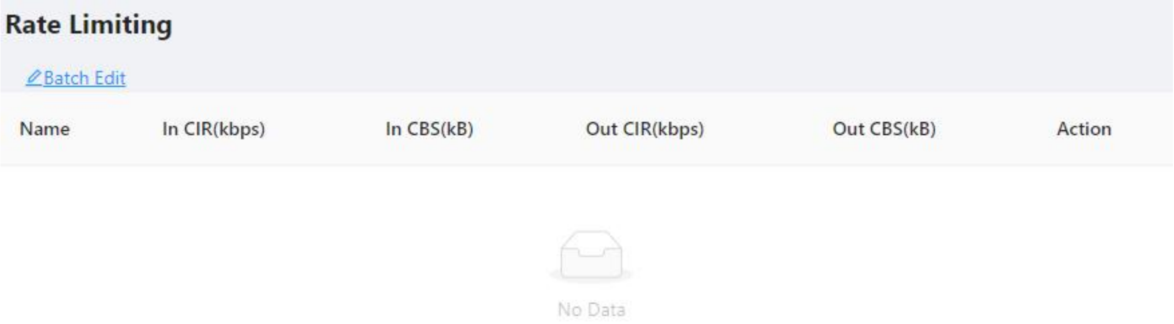
Configure Port Ratelimit

1. Select **Configuration** > **Port** > **Port Extension** in the navigation area to enter the Port Ratelimit module as shown in Figure 3-8.

2. Click the **Batch Edit** button below Rate Limiting to enter the Configure Rate Limiting page, as shown in Figure 3-9, and type the parameter in the modal. Table 3-5 describes the items of configuring such a function.

3. Click the **OK** button.
4. Click the **Save** button in the auxiliary area.

Figure 3-8 Port ratelimit page



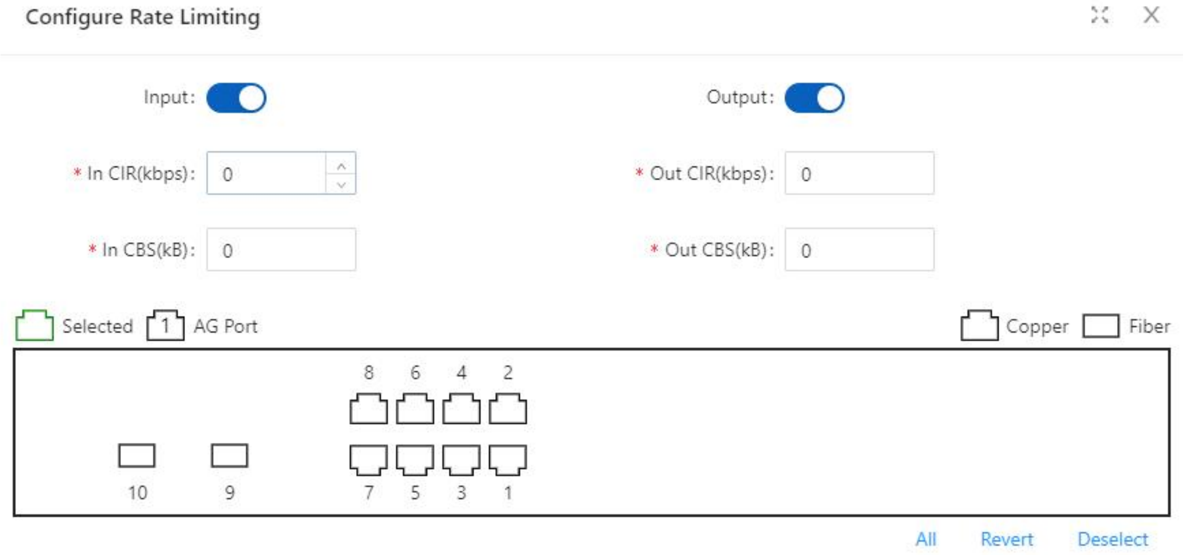
Rate Limiting

Batch Edit

Name	In CIR(kbps)	In CBS(kB)	Out CIR(kbps)	Out CBS(kB)	Action

No Data

Figure 3-9 Port ratelimit configuration



Configure Rate Limiting

Input: ● Output: ●

* In CIR(kbps): 0 * Out CIR(kbps): 0

* In CBS(kB): 0 * Out CBS(kB): 0

NOTE:

- CBS embodies a rate-limit feature for policing traffic. When policing traffic with CBS, here recommends the burst value 4 times of the limit value. If the burst values are too low, then the achieved rate is often much lower than the configured rate.

Table 3-5 Port ratelimit configuration items

Item	Description
In CIR (kbps)	Specify the rate limit in the inbound direction (KBits).
In CBS (KB)	Specify the burst size in the inbound direction (KBits).
Out CIR (kbps)	Specify the rate limit in the outbound direction (KBits).
Out CBS (KB)	Specify the burst size in the outbound direction (KBits).

3.2.2.2 Storm Control

A traffic storm occurs when a large amount of broadcast, multicast, or unicast packets congest a network.

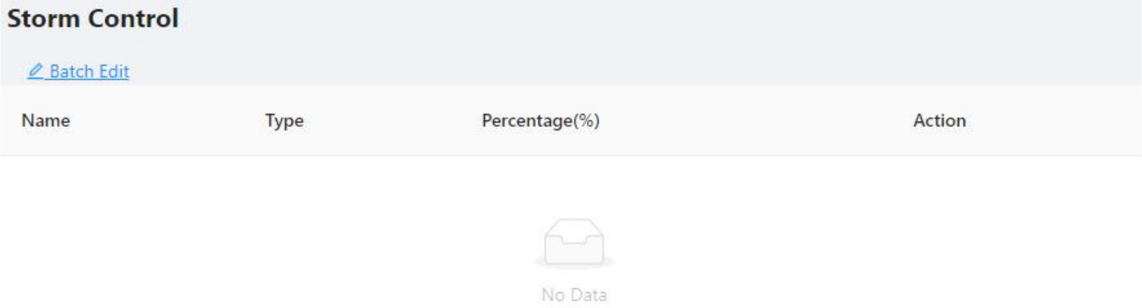
The user can use the storm suppression function to limit the size of a particular type of traffic (currently broadcast, multicast and unknown unicast traffic) on a per-interface basis in Ethernet port view or port group view.

In the port or port group view, the user set the maximum broadcast, multicast or unknown unicast traffic allowed to pass through a port or each port in a group. When the broadcast, multicast, or unknown unicast traffic on the interface exceeds the threshold, the system discards packets until the traffic drops below the threshold.

Configure the Storm Control

1. Select **Configuration** > **Port** > **Port Extension** in the navigation area to enter the Storm Control section as shown in Figure 3-10.

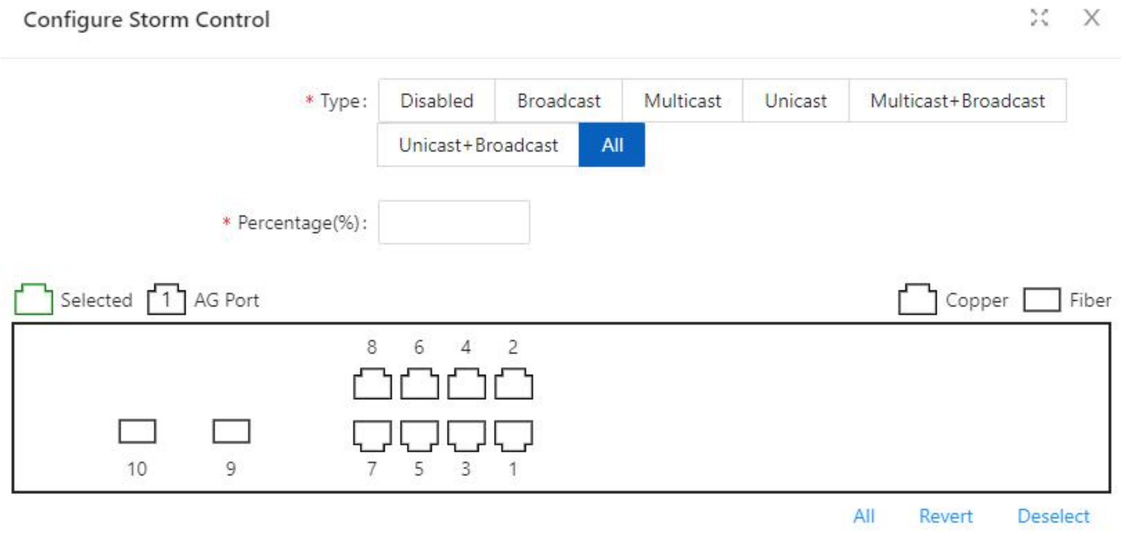
Figure 3-10 Strom Control page



Storm Control

2. Select the type, input the Percentage, and select the port in the port panel, as shown in Figure 3-11. Table 3-6 describes the items of configuring storm control.
3. Click the **OK** button to complete the configuration.
4. Click the **Save** in the auxiliary area to save such configuration.

Figure 3-11 Storm control configuration



Configure Storm Control

* Type: Disabled | Broadcast | Multicast | Unicast | Multicast+Broadcast | Unicast+Broadcast | All

* Percentage(%):

Table 3-6 Items of the storm control

Item	Description

Type	Disabled	Disable storm control
	Broadcast	Select the parameter used in broadcast suppression and set its value in the percentage box.
	Multicast	Select the parameter used in multicast suppression and set its value in the percentage box.
	Unicast	Select the parameter used in unicast suppression and set its value in the percentage box.
	Multicast-broadcast	Select the parameter used in multicast and broadcast suppression and set its value in the percentage box.
	Unicast-broadcast	Select the parameter used in unicast and broadcast, suppression and set its value in the percentage box.
	All	Select the parameter used in unicast and unicast, broadcast, suppression and set its value in the percentage box.
Percentage (%)		Indicate the maximum percentage of traffic to the total transmission capability of an Ethernet interface.

3.2.2.1 Isolation

Usually, Layer 2 traffic isolation is achieved by assigning ports to different VLANs. To save VLAN resources, port isolation is introduced to isolate ports within a VLAN, allowing for great flexibility and security.

1. The switch support multiple isolation groups which can be configured manually. These devices are referred to as multiple-isolation-group devices.

2. There is no restriction on the number of ports assigned to an isolation group.

3. Within the same VLAN, Layer 2 data transmission between ports within and outside the isolation group is supported.

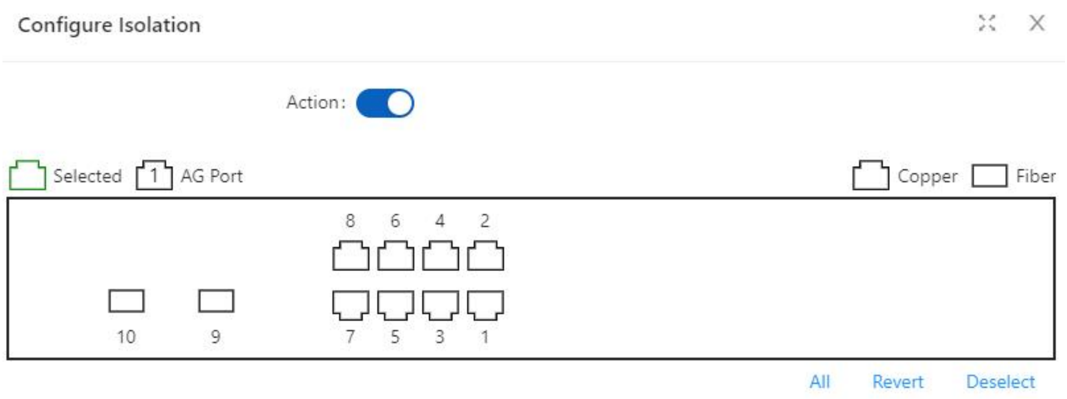
Configure an Isolation Group

1. Select **Configuration** > **Port** > **Port Extension** in the navigation area to enter the Port Isolate section as shown in Figure 3-12.

2. Select the port to be isolated, click **OK** button.

3. Click **Save** in the auxiliary area.

Figure 3-12 Port isolate modal



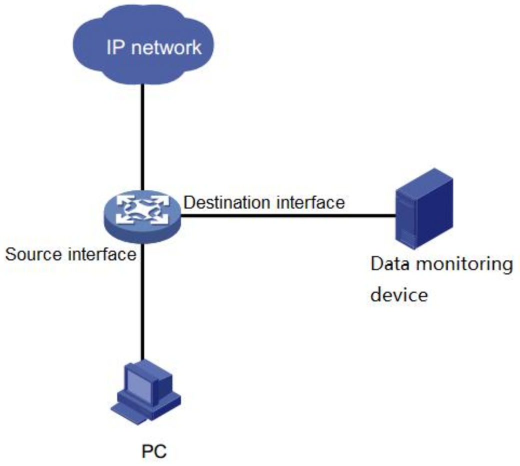
Configure Isolation

Action: ●

3.2.3 Port Mirroring

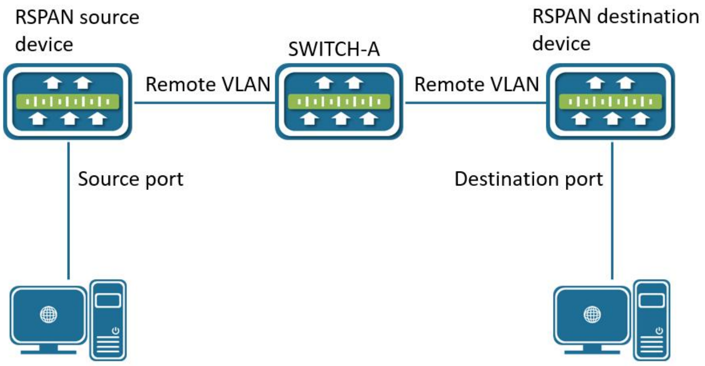
Port mirroring (SPAN) is to copy the packets passing through one or multiple ports (called source interface) to a port (called the destination interface) on the local device. The source interface is connected with a monitoring device. By analyzing on the monitoring device, the packets mirrored to the destination interface, the user can monitor the network and troubleshoot possible network problems.

Figure3-13 A port mirroring implementation



The Remote Switch Port Analyzer (RSPAN) is an extension of the SPAN. Between the remote mirror source port and the destination port, the user can span multiple network devices. The principle of RSPAN is that the original device, the intermediate one and the destination one create a Remote VLAN to which all the ports participating in the session are added. The mirror message is broadcast in the Remote VLAN so that it is transmitted from the source port of the source device to the destination port of the destination device, as shown in Figure 3-14.

Figure3-14 Remote port mirror



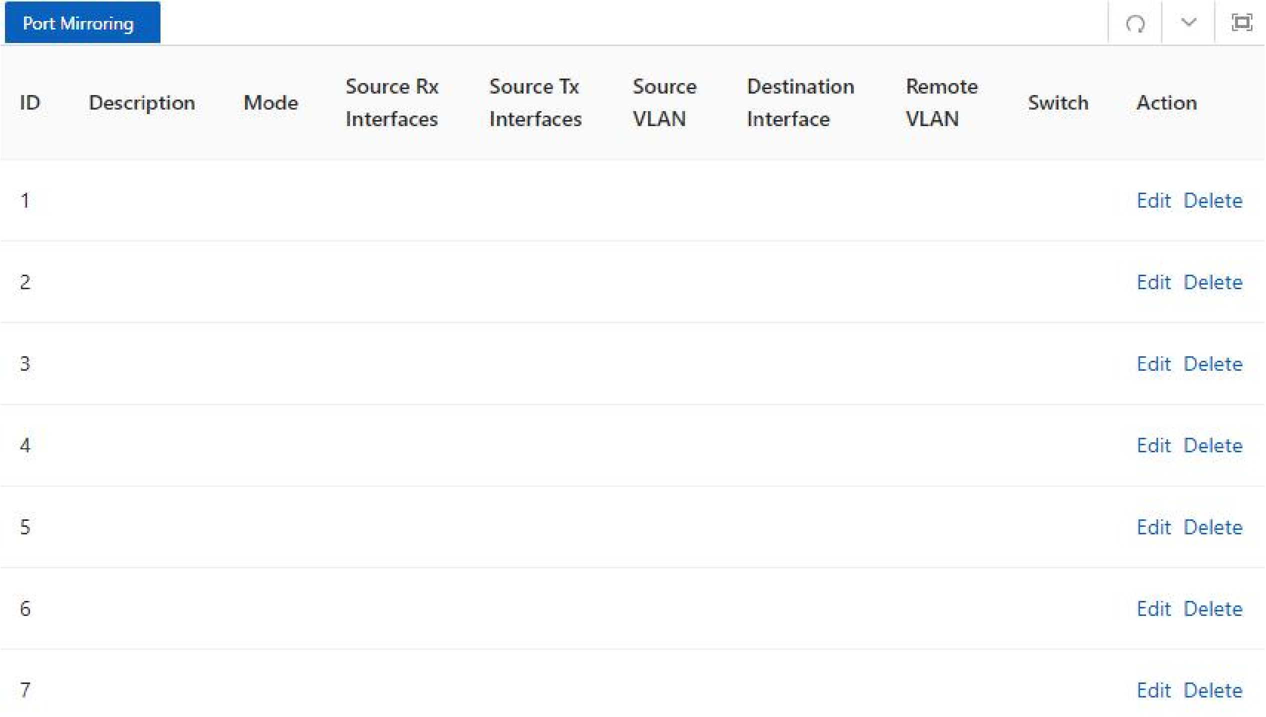
SPAN/RSPAN does not affect the packet exchange of the source port but only copies all the input and output packets of the source port to the destination one. When the mirror traffic of the source port surpasses the bandwidth of the destination one, for instance, the 100Mbps destination port monitors the traffic of the 1000Mbps source port which may cause the message to be discarded.

SPAN/RSPAN based on session management in where the user can configure the source port and the destination one. In one session, there can only be one destination port, while multiple source ports can be configured simultaneously.

Create a Mirroring Group

1. Select **Configuration** > **Port** > **Port Mirroring** in the navigation area to enter the Port mirror page as shown in Figure 3-15.

Figure 3-15 Port mirror page



Port Mirroring

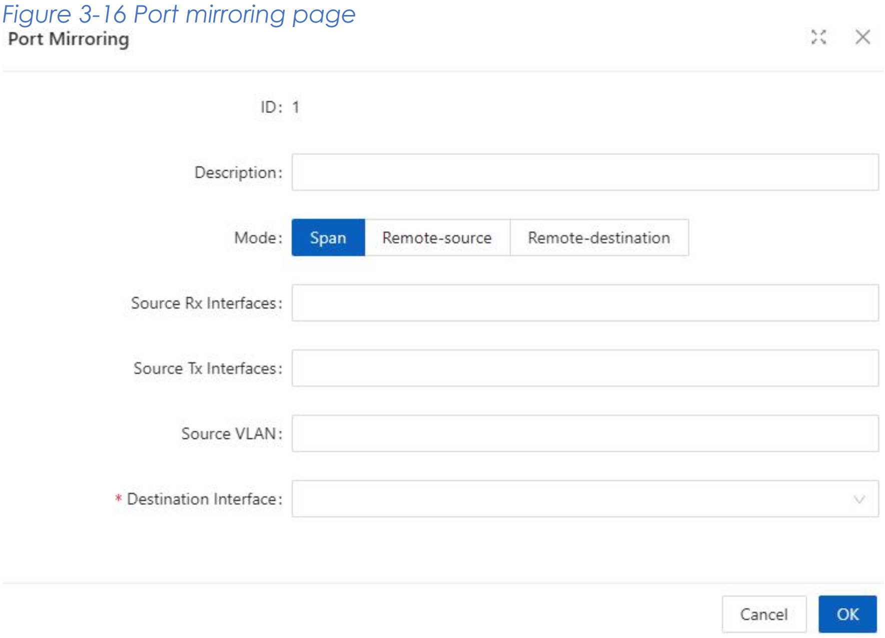
ID	Description	Mode	Source Rx Interfaces	Source Tx Interfaces	Source VLAN	Destination Interface	Remote VLAN	Switch	Action
1									Edit Delete
2									Edit Delete
3									Edit Delete
4									Edit Delete
5									Edit Delete
6									Edit Delete
7									Edit Delete

2. Click the **Edit** button for the corresponding ID to enter the Port Mirroring Configuration modal as shown in Figure 3-16 and the specific parameters are described in Table 3-7.

Table 3-7 Configuration items of creating a mirroring group

Item	Description
ID	ID of the mirroring group to be created
Description	The mirror group descriptors that have created
Mode	The mode of mirror group, default to local mirror
Source Rx Interfaces	Select the mirror source rx port, allowing multiple source rx ports to exist simultaneously
Source Tx Interfaces	Select the mirror source tx port, allowing multiple source ts ports to exist simultaneously
Source VLAN	Create/delete SPAN source VLAN which supports range mode. Source VLAN can only support one session and it can't coexist with source port.
Destination Interfaces	Select the mirroring destination port, and only one destination port is allowed for each session
Switch	Whether the destination port of SPAN is involved in the exchange
Remote VLAN	Create/delete RSPAN source VLAN which supports range mode. Source VLAN can only support one session and it can't coexist with source port.

Figure 3-16 Port mirroring page


Port Mirroring

ID: 1

Description:

Mode: Span | Remote-source | Remote-destination

Source Rx Interfaces:

Source Tx Interfaces:

Source VLAN:

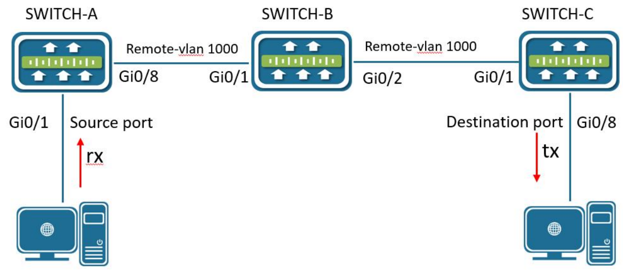
* Destination Interface:

3. Fill in the parameters according to the requirements, and click the **OK** button to complete the configuration.
4. Click **Save** in the auxiliary area.

A Configuration Example

Case requirement: Using port gigabitEthernet0/8 of remote device SWITCH-C to monitor the rx message of the port gigabitEthernet0/1 in local device SWITCH-A and the Remote VLAN is 1000, in the meantime, the intermediate device supports VLAN 1000 message broadcast. The name of this monitoring session is set to TRAFFIC_MONITOR_REMOTE. Such network is shown in below Figure 3-17.

Figure 3-17 Network topology

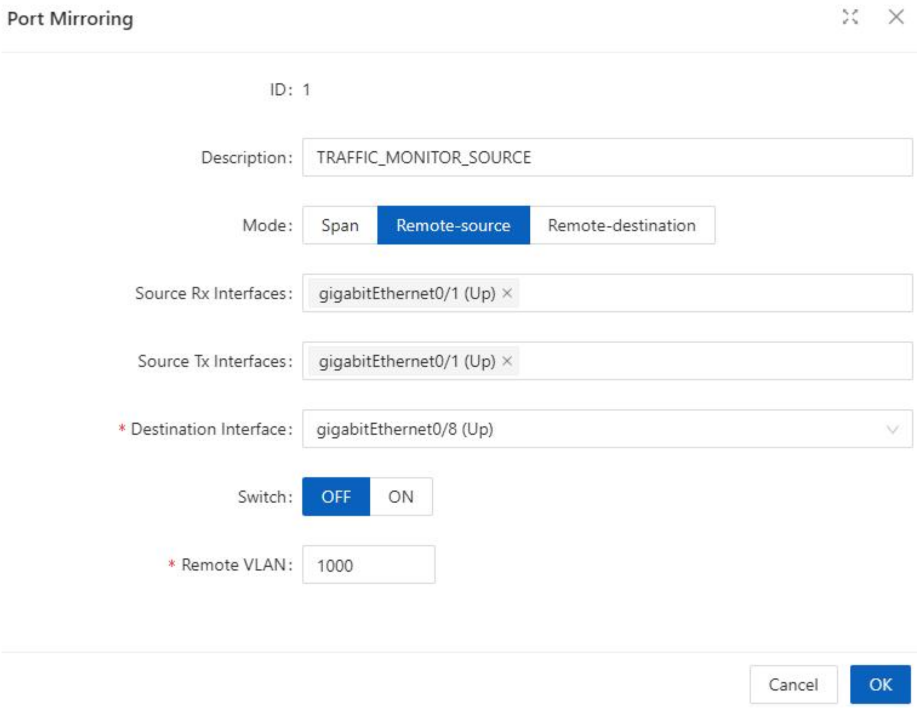


Switch A Configuration:

Step 1: Select **Configuration** > **Port** > **Port Mirroring** in the navigation area to enter the Port Mirror page.

Step 2: Click the **Edit** button corresponding to session 1, fill in the parameters as Figure 3-18, then click **OK**.

Figure 3-18 Port mirroring configuration page in Switch A



Port Mirroring

ID: 1

Description: TRAFFIC_MONITOR_SOURCE

Mode: Span | **Remote-source** | Remote-destination

Source Rx Interfaces: gigabitEthernet0/1 (Up) ×

Source Tx Interfaces: gigabitEthernet0/1 (Up) ×

* Destination Interface: gigabitEthernet0/8 (Up)

Switch: **OFF** | ON

* Remote VLAN: 1000

Step 3: Click **Save** button in the auxiliary area.

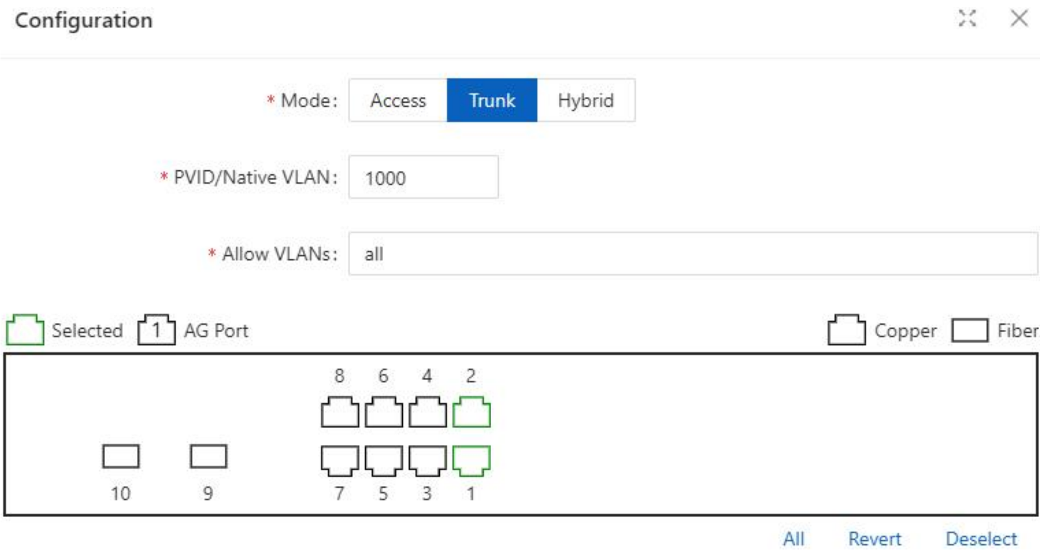
Switch B Configuration:

Step 1: Select **Configuration** > **VLAN** in the navigation area to enter the VLAN Configuration page.

Step 2: Click the **+Add** button under VLAN Configuration to configure gigabitEthernet0/1 and gigabitEthernet0/2 as trunk port whose VLAN is 1000, as shown in Figure 3-19.

Step 3: Click **Save** button in the auxiliary area.

Figure 3-19 VLAN configuration page in Switch B



Configuration

* Mode: Access [✓ Trunk] Hybrid

* PVID/Native VLAN: 1000

* Allow VLANs: all

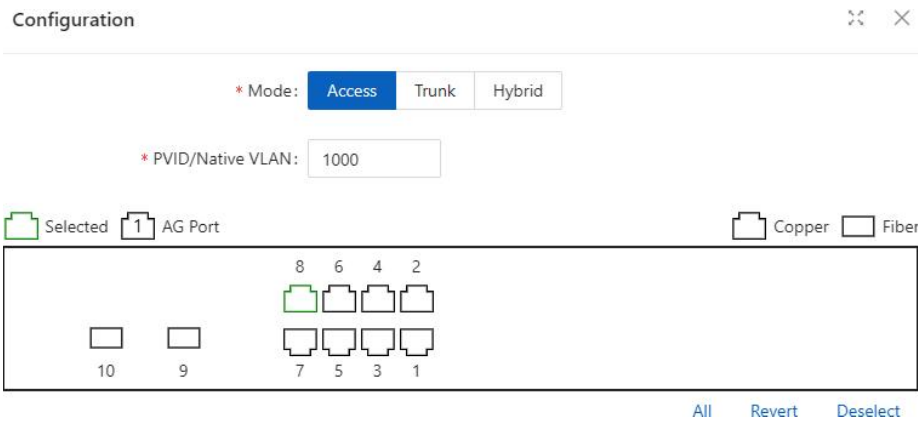
Switch C Configuration:

Step 1: Select **Configuration** > **VLAN** in the navigation area to enter the VLAN Configuration page.

Step 2: Click the **+Add** button under VLAN Configuration to create VLAN 1000.

Step 3: As shown in Figure 3-20, configure the gigabitEthernet0/8 as the access port and the port VLAN as 1000.

Figure 3-20 VLAN configuration page in Switch C



Configuration

* Mode: [✓ Access] Trunk Hybrid

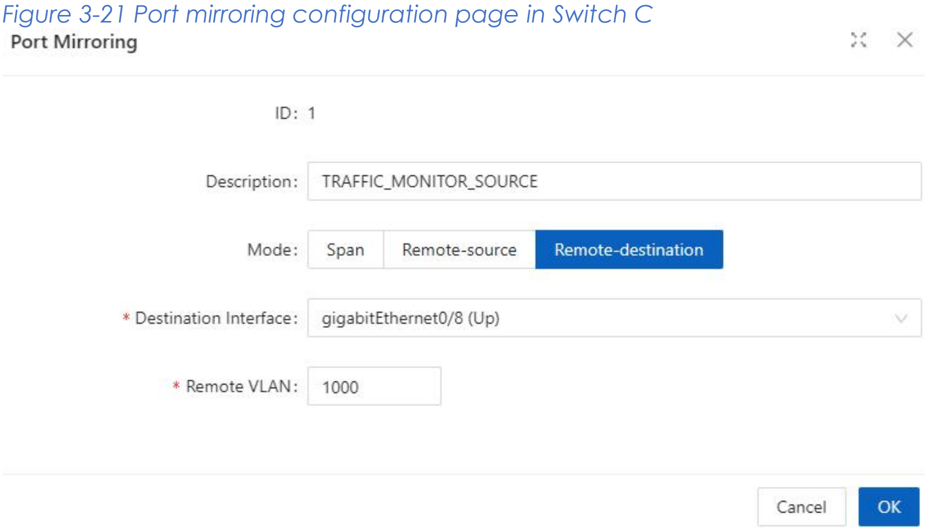
* PVID/Native VLAN: 1000

Step 4: Select **Configuration** > **Port** > **Port Mirroring** in the navigation area to enter the Port Mirror page.

Step 5: Click the **Edit** button corresponding to session 1, fill in the parameters as Figure 3-21, then click **OK**.

Step 6: Click **Save** button in the auxiliary area.

Figure 3-21 Port mirroring configuration page in Switch C



Port Mirroring

ID: 1

Description: TRAFFIC_MONITOR_SOURCE

Mode: Span | Remote-source | Remote-destination

* Destination Interface: gigabitEthernet0/8 (Up)

* Remote VLAN: 1000

3.2.4 Port Aggregation

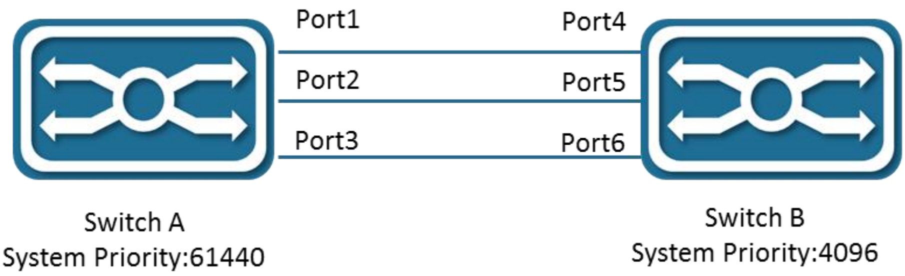
3.2.4.1 Overview

Link Aggregation

Ethernet link aggregation, most often simply called link aggregation, aggregates multiple physical Ethernet links into one logical link to increase link bandwidth beyond the limits of any one single link. This logical link is called an aggregate link. It allows for link redundancy because the member physical links dynamically back up one another.

As shown in Figure 3-22, Switch A and Switch B are connected with three physical Ethernet links. These physical Ethernet links are aggregated into an aggregate link, Link aggregation 1. The bandwidth of this aggregate link can be as high as the total bandwidth of these three physical Ethernet links.

Figure 3-22 Port isolate page



LACP

The IEEE 802.3ad Link Aggregation Control Protocol (LACP) enables dynamic aggregation of physical links. It uses link aggregation control protocol data units (LACPDUs) for exchanging aggregation information between LACP enabled devices.

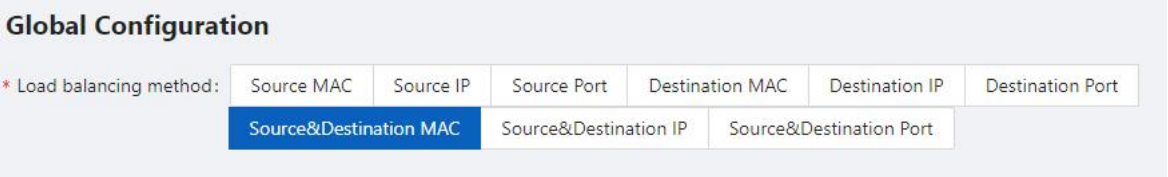
There are two link aggregation modes: dynamic and static. Dynamic link aggregation uses LACP while static link aggregation does not. A link aggregation group operating in static mode is called a static link aggregation group, while a link aggregation group operating in dynamic mode is called a dynamic link aggregation group.

3.2.4.2 Configure an Aggregation Group

Configuration Procedure:

1. Select **Configuration** > **Port** > **Port Aggregation** in the navigation area to enter the Link Aggregation page as shown in Figure 3-23. The description of the link aggregation is described in Table 3-8.

Figure 3-23 Global configuration page



Global Configuration

* Load balancing method: Source MAC | Source IP | Source Port | Destination MAC | Destination IP | Destination Port | [✓ Source&Destination MAC] | Source&Destination IP | Source&Destination Port

Table 3-8 Description of global configuration items

Item	Description	
Load balancing method	Dst-mac	Equalize according to the destination MAC address
	Src-mac	Equalize according to the source MAC address
	Src-dst-mac	Equalize according to the destination MAC address and source MAC address
	Dst-ip	Equalize according to the destination IP address
	Srt-ip	Equalize according to the source IP address
	Src-dst-ip	Equalize according to the destination IP address and source IP address
	Dst-port	Equalize according to the L4 TCP/UDP destination port number
	Src-port	Equalize according to the L4 TCP/UDP source port number
	Src-dst-port	Equalize according to the L4 TCP/UDP destination port number and source port number

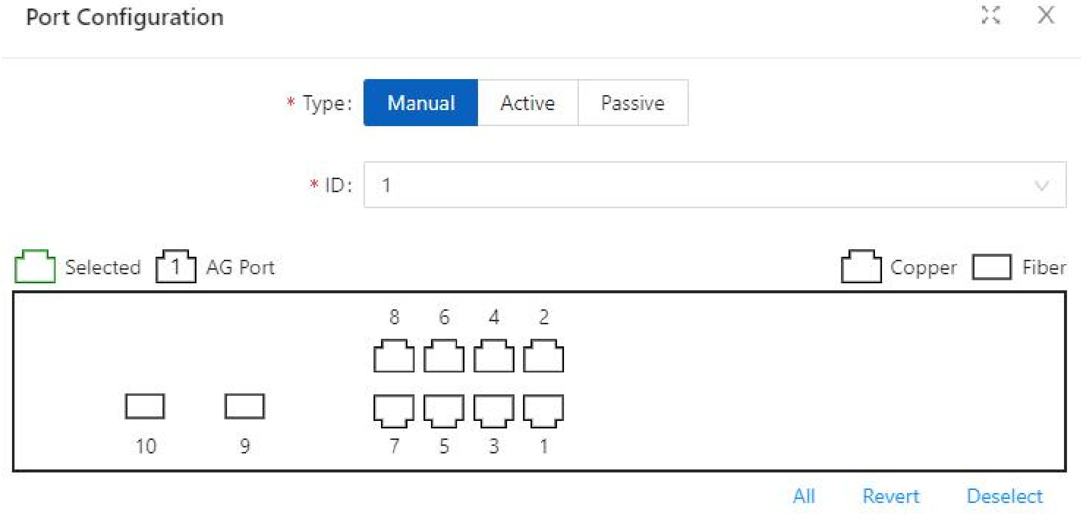
2. In the Aggregate Ports Configure page, click **+Add** button to enter Port Configuration page, as shown in Figure 3-24. The description of the link aggregation is described in Table 3-9.

Table 3-9 Description of aggregation member

Item		Description	
Port Configuration	ID	The ID of the Aggregation Member	
	Type	Manual	Manual mode
		Active	In this mode, the ports send LACP packets at regular

			intervals to the partner ports
		Passive	In this mode, the ports do not send LACP packets until the partner port sends LACP packets. After receiving the LACP packets from the partner port, the ports send LACP packets to the partner port.

Figure 3-24 Aggregation port configuration page



Port Configuration

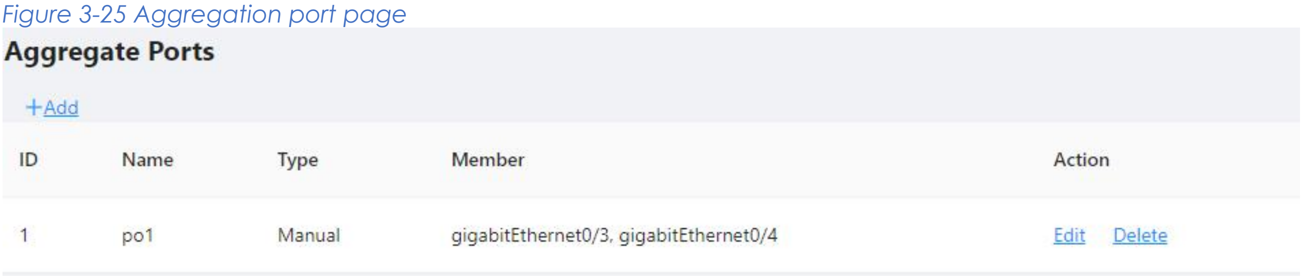
* Type: Manual | Active | Passive

* ID: 1

Select the type of aggregation, text the ID box, select the port in the port panel, click OK button to complete the configuration.

After the configuration is completed, the aggregation port created is displayed on the Aggregation Port page, as shown in Figure 3-25. The description of Aggregation Port is described in Table 3-10.

Figure 3-25 Aggregation port page



Aggregate Ports

+Add

ID	Name	Type	Member	Action
1	po1	Manual	gigabitEthernet0/3, gigabitEthernet0/4	Edit Delete

Table 3-10 Description of aggregation port

Item		Description
Aggregation Port	ID	The ID of the Aggregation Port
	Name	The name of the Aggregation Port
	Type	The mode of the Aggregation Port
	Member	The member ports of the Aggregation Port

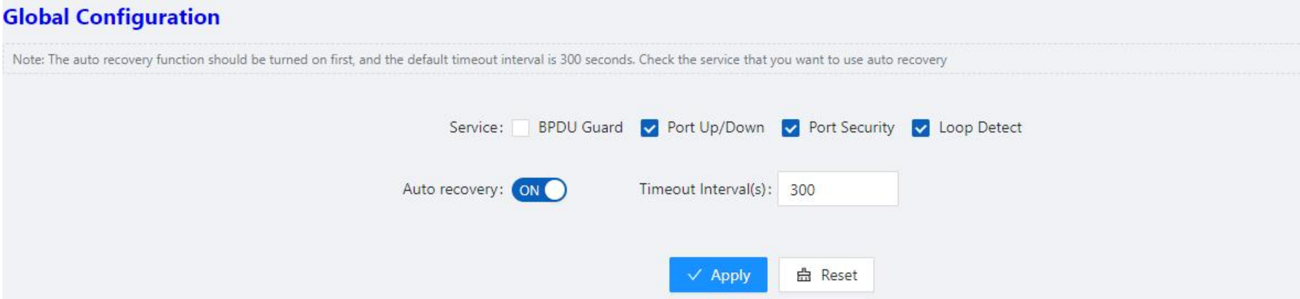
3.2.5 Port Violation

During the use of the device, active or passive violations may occur on the switch port, such as port security violations, port flapping violations, port loop detection violations, etc. The port violation module is used to configure the recovery enablement and recovery time of the violating port, and displays the port's violation behavior.

Configuration Procedure:

Select **Configuration** > **Port** > **Port Violation** in the navigation bar to enter the Port Violation Global Configuration interface, check the service that needs to be violated, turn on the automatic recovery button and configure the recovery time, click the **Apply** button to complete the configuration, such as Figure 3-26 is shown, and the global configuration parameters are shown in Table 3-11.

Figure 3-26 Global configuration page



Global Configuration

Note: The auto recovery function should be turned on first, and the default timeout interval is 300 seconds. Check the service that you want to use auto recovery

Service: □ BPDU Guard ☑ Port Up/Down ☑ Port Security ☑ Loop Detect

Auto recovery: ON

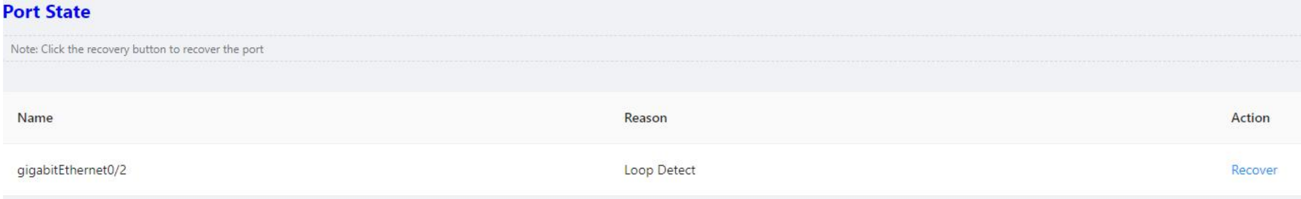
Timeout Interval(s): 300

Table 3-11 Description of global configuration

Item		Description
Service	BPDU Guard	Violations caused by port BPDU protection
	Port Up/Down	Violations caused by frequent port Up/Down
	Port Security	Violations caused by illegal port security
	Loop Detect	Violations caused by a loop in the device downstream of the port
Auto recovery		Enable/disable automatic recovery of violating ports
Timeout interval		Configure the recovery time of the violating port, in seconds

When you need to manually restore the violating port, select the port that needs to be restored and click the **Reset** button to restore the port function.

Figure 3-27 Port state



Port State

Note: Click the recovery button to recover the port

Name	Reason	Action
gigabitEthernet0/2	Loop Detect	Recover

3.3 Spanning Tree

3.3.1 Overview

Spanning Tree Protocol (STP) is a Layer-2 management protocol. It cannot only selectively block redundant links to eliminate Layer-2 loops but also can back up links.

Like many protocols, STP is continuously updated from Rapid Spanning Tree Protocol (RSTP) to Multiple Spanning Tree Protocol (MSTP) as the network develops.

For the Layer-2 Ethernet, only one active link can exist between two local area networks (LANs). Otherwise, a broadcast storm will occur. To enhance the reliability of a LAN, it is necessary to establish a redundant link and keep some paths in backup state. If the network is faulty and a link fails, you must switch the redundant link to the active state. STP can automatically activate the redundant link without any manual operations. STP enables devices on a LAN to:

- Discover and start the best tree topology on the LAN.
- Troubleshoot a fault and automatically update the network topology so that the possible best tree topology is always selected.

The LAN topology is automatically calculated based on a set of bridge parameters configured by the administrator. The best topology tree can be obtained by properly configuring these parameters.

RSTP is completely compatible with 802.1D STP. Like traditional STP, RSTP provides loop-free and redundancy services. It is characterized by rapid speed. If all bridges in a LAN support RSTP and are properly configured by the administrator, it takes less than 1 second (about 50 seconds if traditional STP is used) to re-generate a topology tree after the network topology changes.

STP and RSTP have the following defects:

- STP migration is slow. Even on point-to-point links or edge ports, it still takes two times of the forward delay for ports to switch to the forwarding state.
- RSTP can rapidly converge but has the same defect with STP: Since all VLANs in a LAN share the same spanning tree, packets of all VLANs are forwarded along this spanning tree. Therefore, redundant links cannot be blocked according to specific VLANs and data traffic cannot be balanced among VLANs.
- MSTP, defined by the IEEE in 802.1s, resolves defects of STP and RSTP. It cannot only rapidly converge but also can enable traffic of different VLANs to be forwarded along respective paths, thereby providing a better load balancing mechanism for redundant links.

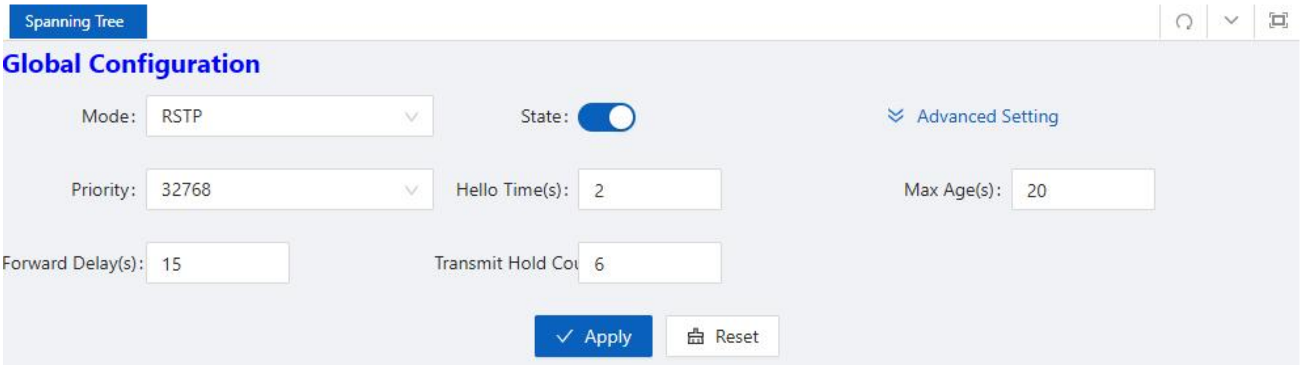
  In general, STP/RSTP works based on ports while MSTP works based on instances. An instance is a set of multiple VLANs. Binding multiple VLANs to one instance can reduce the communication overhead and resource utilization.

3.3.2 Spanning Tree Configuring

Global Configuration of the Spanning Tree

Select **Configuration** > **Spanning Tree** in the navigation area to enter the Global Configuration section, as shown in Figure 3-28. Table 3-12 describes the Spanning Tree Global Configuration items.

Figure 3-28 Spanning tree global configuration



Spanning Tree

Global Configuration

Mode: RSTP

State: ●

Advanced Setting

Priority: 32768

Hello Time(s): 2

Max Age(s): 20

Forward Delay(s): 15

Transmit Hold Cou 6

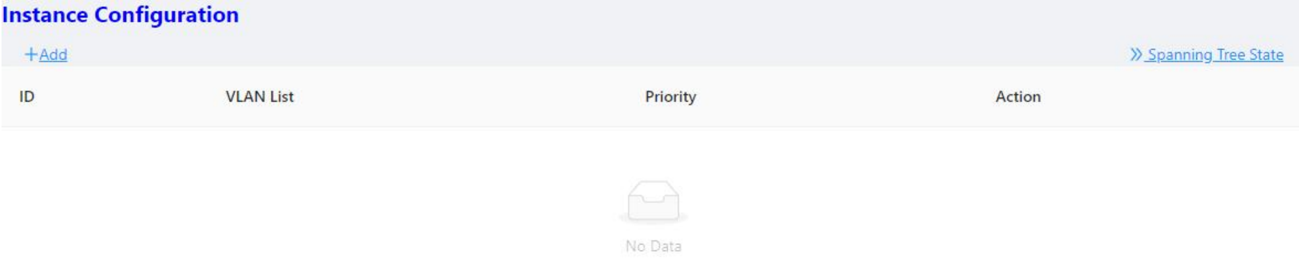
Table 3-12 Spanning tree global configuration items

Item		Description
Global Configuration	Mode	Set the working mode of STP, including STP, RSTP, and MSTP. STP: In STP mode, each port of the device sends STP BPDUs. RSTP: In RSTP mode, each port of the device will send out RSTP BPDUs. When it is connected to the device running STP, the port will automatically migrate to STP mode. MSTP: In MSTP mode, each port of the device sends MSTP BPDUs. When it is connected to the device running STP, the port is automatically migrated to work in STP mode.
	State	Enable STP.
	Hello Time(s)	Hello timer interval
	Priority	Bridge priority
	Forward Delay(s)	Set the delay time before an interface change to forwarding
	Transmit Hold Count	Maximum number of BPDUs sent by the bridge per second
	Max Age(s)	Set the maximum duration that messages are saved in the device

Configure the Instance

Select **Configuration** > **Spanning Tree** in the navigation area to enter the Instance Configuration part, as shown in Figure 3-29. Table 3-13 describes the instance configuration items.

Figure 3-29 Spanning tree instance configuration



Instance Configuration

+Add

» Spanning Tree State

ID	VLAN List	Priority	Action

No Data

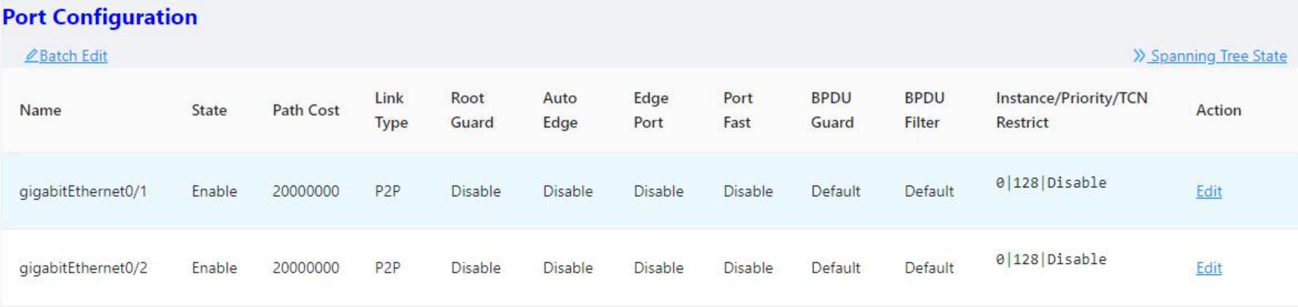
Table 3-13 Spanning tree instance items

Item		Description
Instance Configuration	ID	Instance ID
	VLAN List	Instance associated VLAN list
	Priority	Bridge priority in this instance
	Action	Click to delete this entry

Configure the Ports

Select **Configuration** > **Spanning Tree** in the navigation area to enter the Port Configuration page, as shown in Figure 3-30. Table 3-14 describes the port configuration items.

Figure 3-30 Spanning tree port configuration



Port Configuration

Batch Edit

Spanning Tree State

Name	State	Path Cost	Link Type	Root Guard	Auto Edge	Edge Port	Port Fast	BPDU Guard	BPDU Filter	Instance/Priority/TCN Restrict	Action
gigabitEthernet0/1	Enable	20000000	P2P	Disable	Disable	Disable	Disable	Default	Default	0|128|Disable	Edit
gigabitEthernet0/2	Enable	20000000	P2P	Disable	Disable	Disable	Disable	Default	Default	0|128|Disable	Edit

Table 3-14 Spanning tree port configuration items

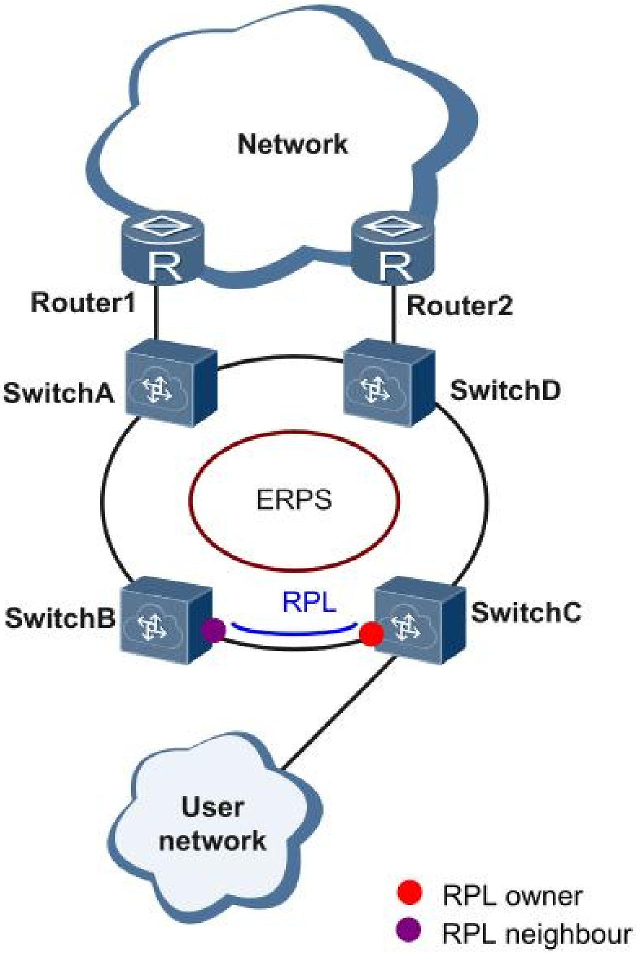
Item		Description
Port Configuration	Name	Interface name
	State	STP status
	Path Cost	Configure interface path cost
	Link Type	Configure interface link type
	Root Guard	Configure the interface to enable root protection.
	Auto Edge	Configure the interface to automatically recognize the function of the edge port.
	Edge Port	Configure the interface as an edge port.
	Port Fast	Configure the interface as a fast port.
	BPDU Filter	Configure the interface to enable BPDU filtering.
	BPDU Guard	Configure the interface to enable BPDU protection.
	Instance/Priority/TCN restrict	Configure the instance, Priority, and TCN restrict.

3.4 ERPS

3.4.1 Overview

The ITU-T G.8032 ERPS feature implements protection switching mechanisms for the Ethernet layer ring topology. This feature uses the G.8032 Ethernet Ring Protection (ERP) protocol, defined in ITU-T G.8032, to provide protection for Ethernet traffic in a ring topology, while ensuring that no loops are within the ring at the Ethernet layer. The loops are prevented by blocking traffic on either a predetermined link or a failed link.

Figure 3-31 Network topology



Initial State

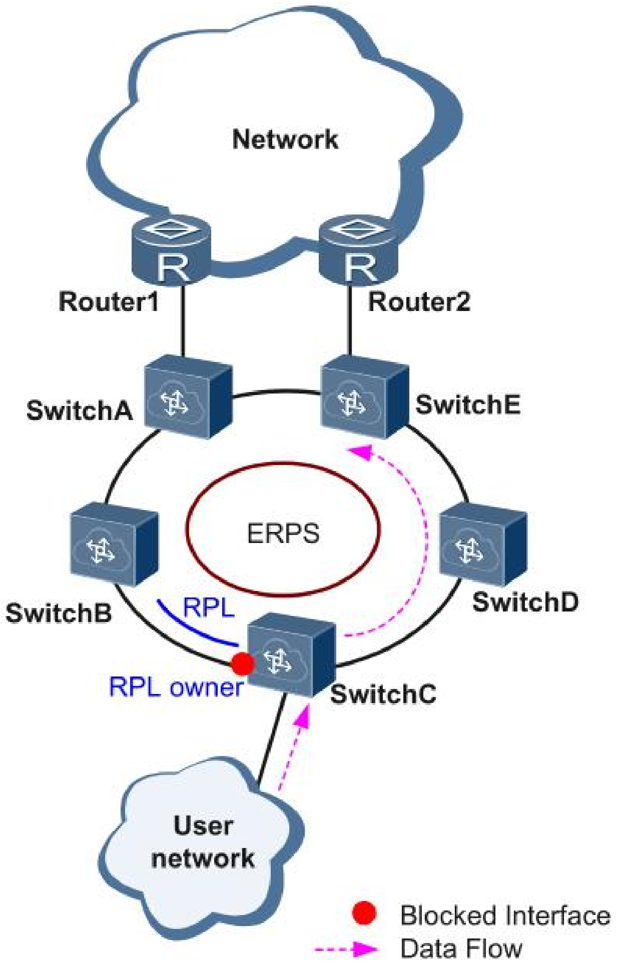
As the following figure, the devices on the ring have been configured, and all the link status is up.

The RPL owner interface will be blocked by ERPS protocol to prevent loops. If a RPL neighbor interface is configured, it will also be blocked. Other interfaces are under the forwarding state, can forward the traffic.

Link Failure

When there is a link failure between Switch D and Switch E, the two interfaces on the link will be blocked by ERPS protocol, the RPL owner interface will be forwarded.

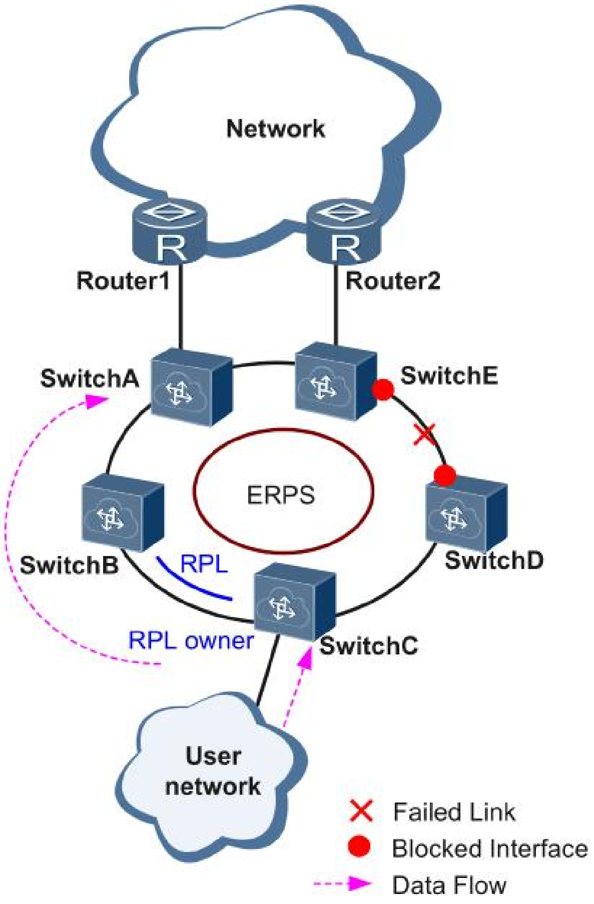
Figure 3-32 Link failure



Link Restores

When the failure link is restored. When the ERPS ring is configured to revertive mode, the RPL owner interface will be blocked by ERPS protocol, the restored link will be configured to forwarding state to forward traffic.

Figure 3-33 Link restores



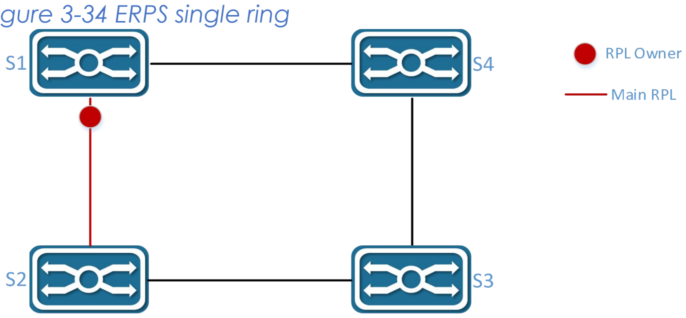
Single-Ring：

Only one ring in a network topology needs to be protected.

In Figure 3-34, the network topology has only one ring, only one ring protection link (RPL) owner node, and only one RPL. All nodes must belong to the same ring automatic protection switching (R-APS) virtual local area network (VLAN).

- All devices in the ring network must support ERPS.
- The links between devices in the ring network must be directly connected, and there must be no intermediate devices.

Figure 3-34 ERPS single ring



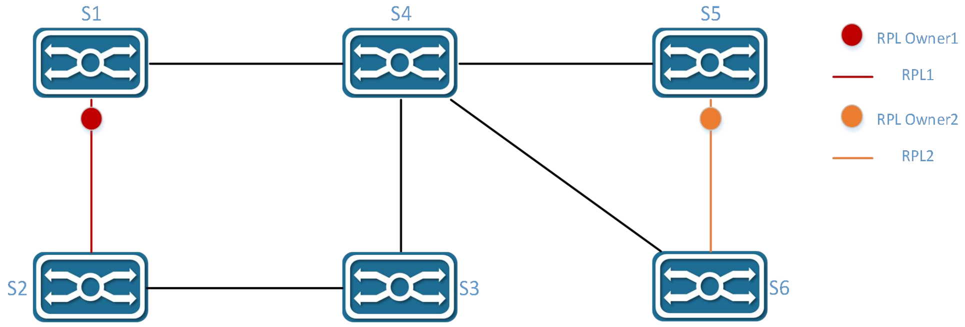
Tangent Rings：

The two rings in a network topology that share one device need to be protected.

In Figure 3-35, the two rings in the network topology share one device. Each ring has only one PRL owner node and only one RPL. The two rings belong to different R-APS VLANs.

- All devices in the ring network need to support ERPS.
- The links between devices in the ring network must be directly connected, and there must be no intermediate devices.

Figure 3-35 ERPS tangent rings



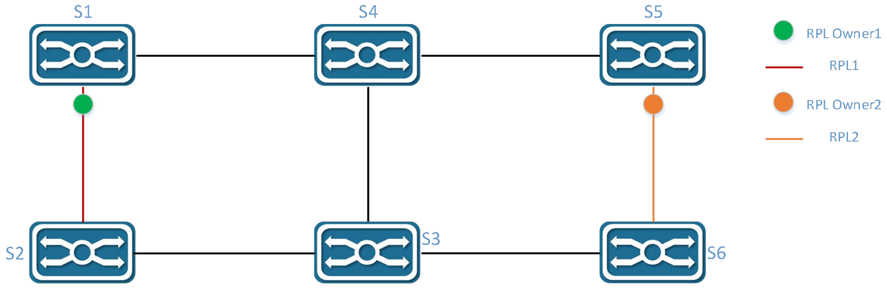
Intersecting Rings:

Two or more rings in a network topology share one link. (Each link between intersecting nodes must be a direct link without any intermediate node.)

In Figure 3-36, four rings exist in the network topology. Each ring has only one PRL owner node and only one RPL. The four rings belong to different R-APS VLANs.

- All devices in the ring network need to support ERPS.
- The links between devices in the ring network must be directly connected, and there must be no intermediate devices.

Figure 3-36 ERPS intersecting rings

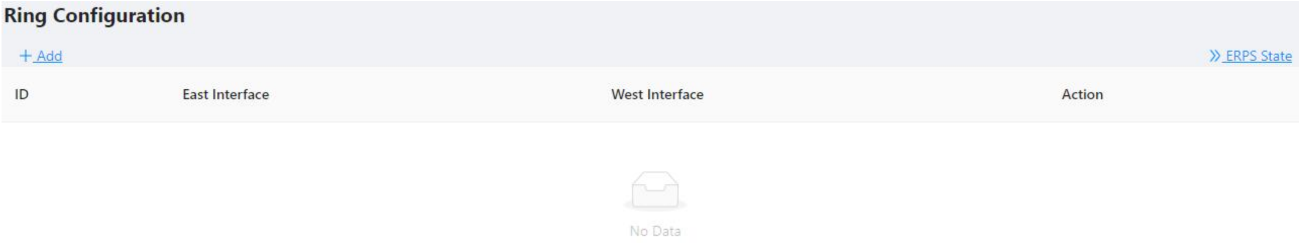


3.4.2 Configure the ERPS

Ring Configuration

Select **Configuration** > **ERPS > Ring Configuration** in the navigation area to enter the ERPS Ring Configuration page as shown in Figure 3-37, The description of the ERPS ring configuration is described in Table 3-15.

Figure 3-37 ERPS ring configuration


Ring Configuration

ID	East Interface	West Interface	Action

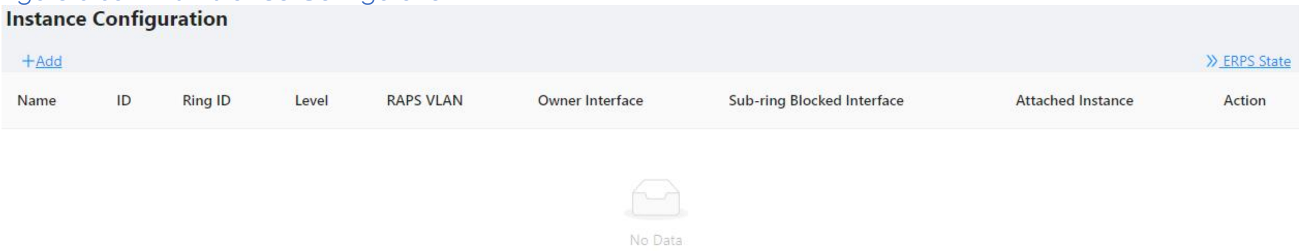
Table 3-15 Ring configuration description

Item	Description
Ring ID	Can be any number. The ring number of each ERPS ring must be unique.
East Interface	The east interface of the ERPS ring
West Interface	The west interface of the ERPS ring
Action	Delete ERPS Ring

ERPS Instance Configuration

Select **Configuration > ERPS > Instance Configuration** to enter the ERPS Instance Configuration page, as shown in Figure 3-38.

Figure 3-38 ERPS Instance Configuration


Instance Configuration

Name	ID	Ring ID	Level	RAPS VLAN	Owner Interface	Sub-ring Blocked Interface	Attached Instance	Action

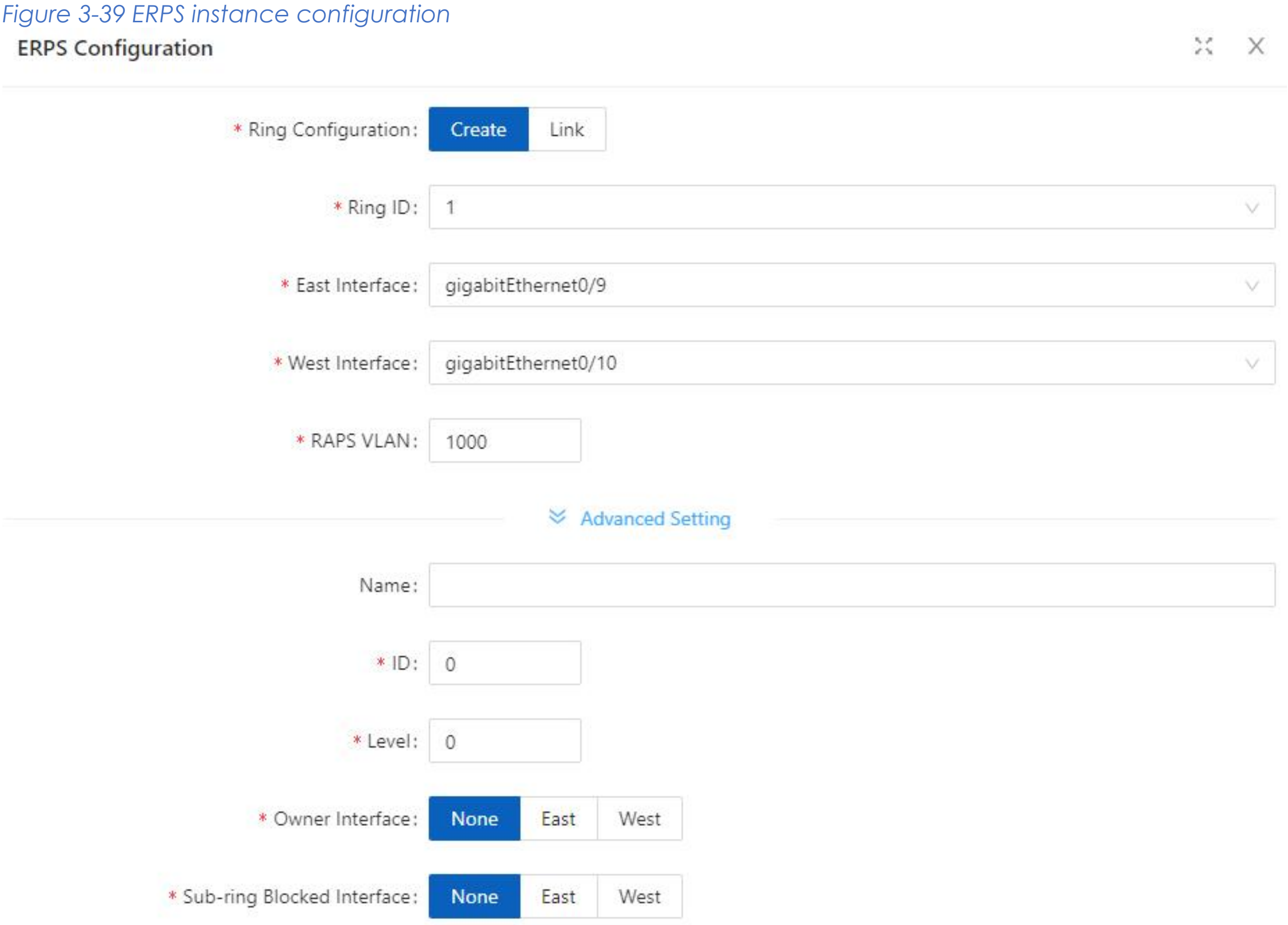
Click **+Add** button below Instance Configuration to create an ERPS instance, as shown in Figure 3-39. The description of the ERPS Instance Configuration Summary is described in Table 3-16.

Table 3-16 Description of the ERPS instance configuration

Item	Description
Ring Configuration	Create a new one or Link to a ERPS ring which has been created
Ring ID	The associated ring ID must be the ring that has been created.
East Interface	The east interface of the ERPS ring
West Interface	The west interface of the ERPS ring
RAPS VLAN	Each switch in the same ring must be configured with the same RAPS management VLAN for transmitting ERPS protocol packets. The RAPS management VLAN can be a virtual VLAN and needs to be distinguished from the data VLAN. * It does not need to be created in 6&8 series switch, as it is created by default.
Owner interface	ERPS Owner interface can select either the east interface or the west interface as the Owner node. Each ERPS ring has one and only one interface configured as an RPL owner interface

	that controls the ports that need to be blocked.
Sub-ring Block Interface	The subring 's blocked interface, one subring has only one blocking port. You can choose east or west. This parameter needs to be configured only for the tangent ring. The sub-rings of the two devices with tangent to the ring must be configured with the sub-ring blocking port.
Attached Instance	It only needs to be set when the sub-ring blocking port needs to be configured, and is set to the ring ID that is tangent to the current sub-ring.

Figure 3-39 ERPS instance configuration



ERPS Configuration

* Ring Configuration: Create | Link
* Ring ID: 1
* East Interface: gigabitEthernet0/9
* West Interface: gigabitEthernet0/10
* RAPS VLAN: 1000

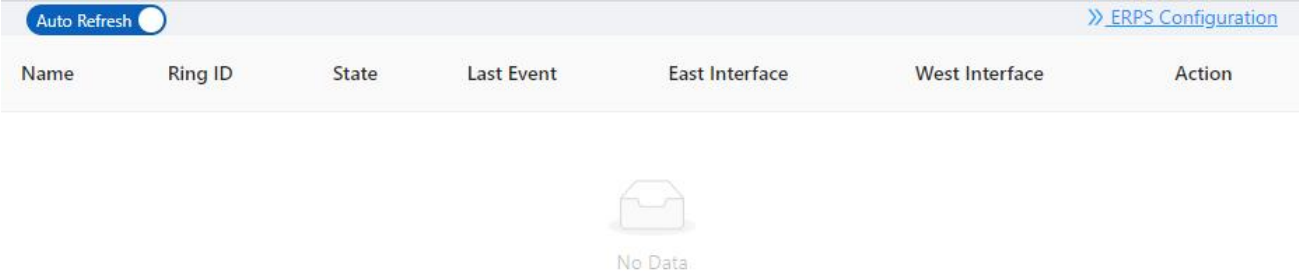
Advanced Setting

Name:
* ID: 0
* Level: 0
* Owner Interface: None | East | West
* Sub-ring Blocked Interface: None | East | West

View ERPS State

Click **ERPS State** button to enter the ERPS State page, as shown in Figure 3-40. The description of the ERPS State summary is described in Table 3-17.

Figure 3-40 ERPS state



Name	Ring ID	State	Last Event	East Interface	West Interface	Action

No Data

Table 3-17 ERPS state description

Item	Description
Name	The name of the ERPS ring
Ring ID	The number of the ERPS ring
State	ERPS ring status, include： Idle： Stable state when all non-RPL links are available. In this state, the owner node blocks the RPL port and periodically sends NR-RB packets. The neighbor node blocks the RPL port. All nodes enter the idle state after the owner node enters the idle state. Pending： Transient state between the previous states Protection： State when a non-RPL link is faulty. In this state, the RPL link is unblocked to forward traffic. All nodes enter the protection state after a node enters the protection state.
Last Event	Recent state event RAPS-NR：remote failure recovery RAPS-NR-RB: remote switchback RAPS-SF：remote fault LOCAL-SF：local fault LOCAL-CLEAR-SF：local failure recovery WTR-EXP：local switchback
East Interface	The east interface of the ERPS ring
West Interface	The west interface of the ERPS ring
Action	When the faulty link is restored, you can choose to manually revert immediately, otherwise the system will automatically revert after 5 minutes.

3.5 PoE Management

3.5.1 PoE Overview

Power over Ethernet (PoE) means that power sourcing equipment (PSE) supplies power to powered devices (PDs) from Ethernet interfaces through twisted pair cables.

3.5.2 PoE Configuration

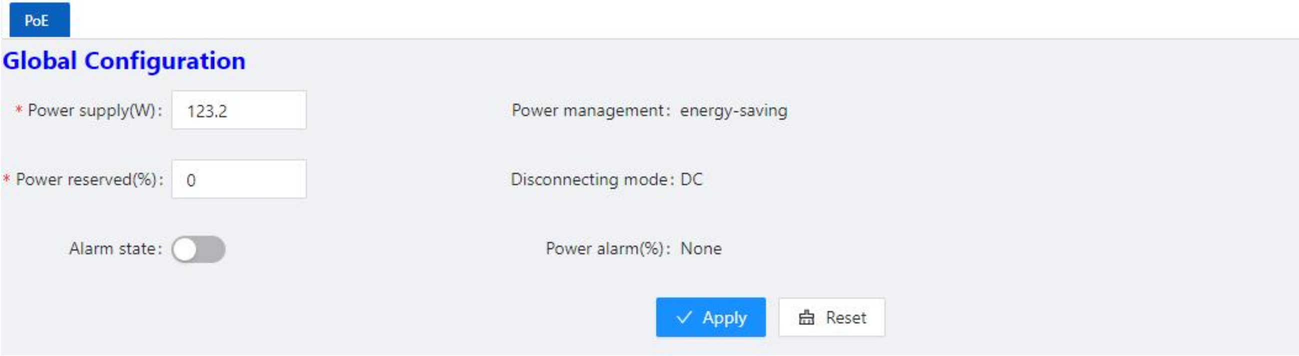
NOTE:

- 1. Before configure PoE, make sure that the PoE power supply and PSE are operating normally; otherwise, you cannot configure PoE or the configured PoE function does not take effect.
- 2. For switches with external power supply, the input voltage range is 44-57 V. In order to obtain a more stable power supply, it is recommended that the power supply voltage of AT equipment be greater than 50V, and that of BT equipment be greater than 53V.

1. Select **Configuration** > **PoE** in the navigation area to enter the PoE Management page as shown in Figure 3-41, the Table 3-18 describes the items of PoE global configuration.

2. Type the Power supply and Power reserved boxes, and click **Apply** button.

Figure 3-41 PoE global configuration



PoE

Global Configuration

* Power supply(W): 123.2

Power management: energy-saving

* Power reserved(%): 0

Disconnecting mode: DC

Alarm state: ○

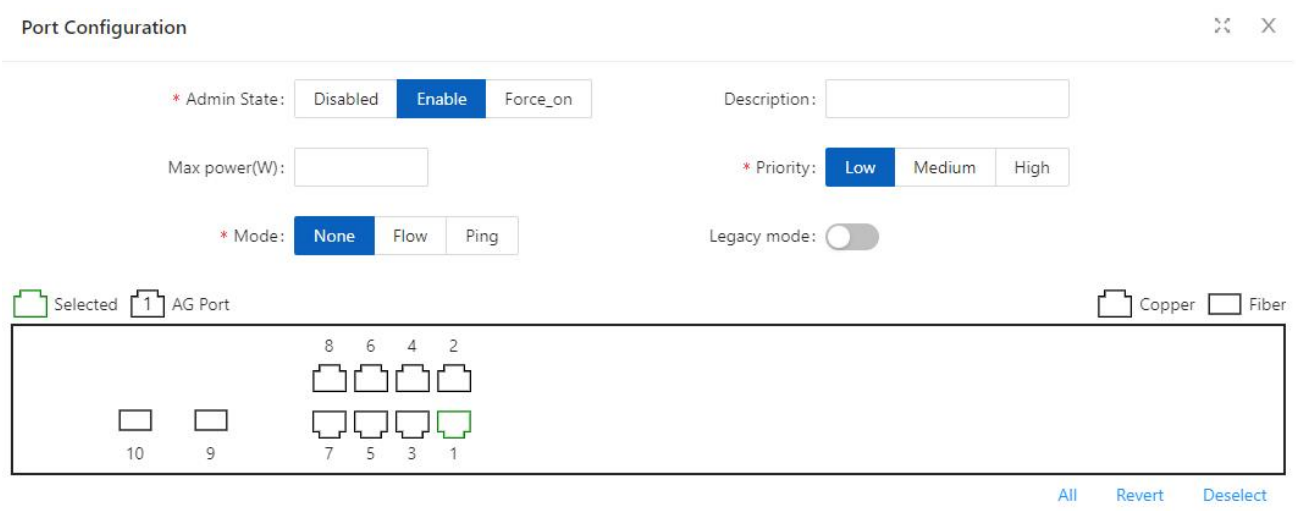
Power alarm(%): None

Table 3-18 Descriptions of PoE global configuration

Item	Description
Power supply (w)	By default, the default power provided by the device is 15.4W*port number, for example, the maximum power provided by an 8-port device is 123.2W • For devices with external power supply, please fill in this parameter according to the actual configured power supply • For devices with built-in power supply, please refer to the description of PoE power in the product manual for this parameter
Power reserved (%)	Reserved power set against power fluctuations • For devices with external power supply, it is recommended to fill in the power consumption of the main board • For devices with built-in power supply, this parameter can be set 0 by default
Power management	Display the mode of power management is energy-saving. In this mode, the power requested and allocated to the port is based on the actual port's (real time) power consumption.
Disconnect mode	Display the mode of disconnection is DC disconnect
Alarm state	Turn on/off the log alarm when the power is insufficient
Power alarm (%)	Alarm power limit setting, when the PoE power consumption exceeds this value, the system will automatically output a log alarm

3. Click **Batch Edit** below Port Configuration to enter PoE Port Configuration page, Select the port to be configured, as shown in Figure 3-42.

Figure 3-42 PoE configuration page



Port Configuration

* Admin State: Disabled [✓ Enable] Force_on

Description:

Max power(W):

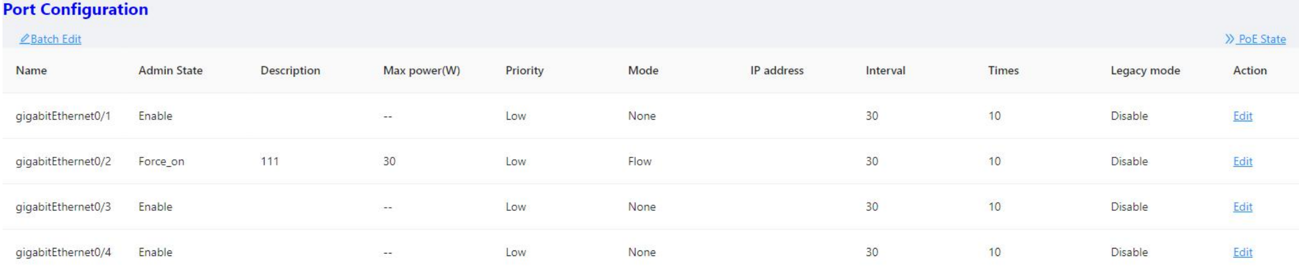
* Priority: [✓ Low] Medium High

* Mode: [✓ None] Flow Ping

Legacy mode: ○

4. Click the **OK** to complete the operation, and then the page will return to the PoE Interface Configuration page, as shown in Figure 3-43. the Table 3-19 describes the items of the PoE interface configuration.

Figure 3-43 PoE configuration page



Port Configuration

Name	Admin State	Description	Max power(W)	Priority	Mode	IP address	Interval	Times	Legacy mode	Action
gigabitEthernet0/1	Enable		--	Low	None		30	10	Disable	Edit
gigabitEthernet0/2	Force_on	111	30	Low	Flow		30	10	Disable	Edit
gigabitEthernet0/3	Enable		--	Low	None		30	10	Disable	Edit
gigabitEthernet0/4	Enable		--	Low	None		30	10	Disable	Edit

5. Click the **Save** in the navigation area to save the configuration.

Table 3-19 The items of the PoE interface configuration

Item	Description
Name	Indication panel port number
Admin State	Enable/disable PoE for the PoE Interface. Disable: Disable the PoE power supply of the port Enable: Enable the Po E power supply of the port Force_on: Forcibly turn on the PoE power supply of the port. This function is implemented by skipping the PD valid detection and PD classification detection, and directly supply power to the PD load. In this mode, the default maximum load power is 15w, if you need to power the device above 15w, the maximum power parameter needs to be configured at the same time.
Description	Description of PoE port
Max Power (W)	Configure the maximum power for this port. For AF/AT ports, the maximum port power range is 1-30 For BT ports, the port maximum power range is 1-90 In default mode, the port will perform power management according to PD class.
Priority	Configuring the port's priority

	Users can configure the interface power supply priority of the PoE switch. The priority from high to low is: high, medium, and low. When the overall power of the PoE switch is insufficient, the ports with lower priority will be powered off first. The port priorities of the same priority are arranged in the order of the port number, and the priority of the port with the smaller port number is higher. For example, the priority of port 0/1 is higher than ports 0/2 and 0/3. Newly inserted ports will not affect the power supply of PDs that are already powered which has the same priority. Newly inserted ports which have higher priority will preempt low- priority ports.
Mode	None: Disable the PD alive detection function Flow: Enable the PD alvie detection function in Flow mode. This function is realized by monitoring the port counter, if the port packets counter does not change, it is judged that the PD device connected to the port is in abnormal state, and then turn off the power supply for a few seconds and then turn on. Ping: Enable the PD alive detection function in Ping mode. This function is realized by continuously pinging the PD load, if a period of time the ping packet fails during the interval, it is judged that the PD device connected to the port is in abnormal state, and the power supply is turned off for a few seconds and then turned on again. It is recommended to use the switch **diagnostics network tool→ ping** to test whether the ping packet of the PD device can be used before enabling this function.
IP address	Ping mode, the IP address of the PD load requires that the switch and the PD load be in the same network segment.
Interval	The detection time interval
Times	The detection times PD start up time must be less than the interval * times, otherwise the PD load will always be in the power- off and start -up state.
Legacy mode	ON/OFF, the default is OFF. OFF: Only standard PD devices are supported, the detection resistance is between 19k-26.5k, and the detection capacitance is less than 150nF. ON: Support non-standard PD devices, and can supply power to some PD devices whose detection resistance and capacitance values exceed the standard values.

3.6 Security

3.6.1 Port Security

3.6.1.1 Overview

The Port Security function restricts the number of valid MAC addresses on the port to limit the access of illegal users to the port. The illegal MAC packets will be directly discarded.

The legal MAC can be generated statically or dynamically. The static legal MAC is generated through user command line configuration; the dynamic legal MAC is dynamically generated through the MAC address learning function.

When the number of secure addresses on the port has reached the configured value of the maximum number of secure addresses, the new MAC access port will be recognized as an illegal MAC and a violation event will be generated. The user can configure the actions to be taken when the violation event occurs, respectively restrict or shutdown the port.

Restrict: Prohibit illegal MAC data from passing, and generate alarm log prompt information. Illegal MAC will prohibit access to the port within the MAC address aging time. It can be restored through shutdown and no shutdown ports.

Shutdown: The port is forced to be down, and the port recovery time can be configured. The port will automatically recover when the time is up; it can also be recovered by the shutdown, no shutdown command.

If you want to convert a dynamic security user to a static security user, you can enable the sticky function on the port. When the sticky function is enabled on the port, the dynamic users learned on the port will exist as static users. If the configuration is saved, the device will still exist after restarting the device.

NOTE:

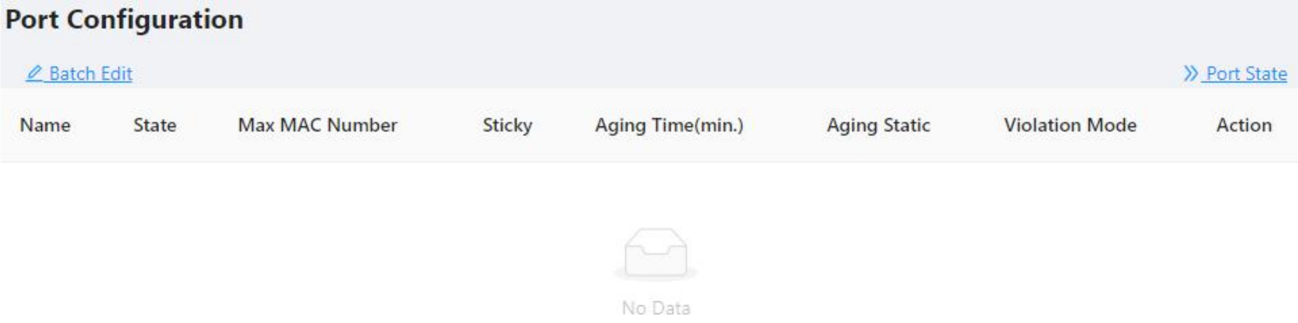
- Only support L2 port configuration port security, such as ordinary physical port, aggregation port.
- Only support port security configuration in access mode.
- Does not support aggregation port member ports to configure port security functions.
- Does not support SPAN destination port configuration port security function.
- Does not support configuring port security functions on ports that have been configured with static MAC addresses.

3.6.1.2 Configuring Port Security

Port Configuration

Select **Configuration > Security > Port security** in the navigation area to enter the Port Security page as shown in Figure 3-44.

Figure 3-44 Port security statistic page

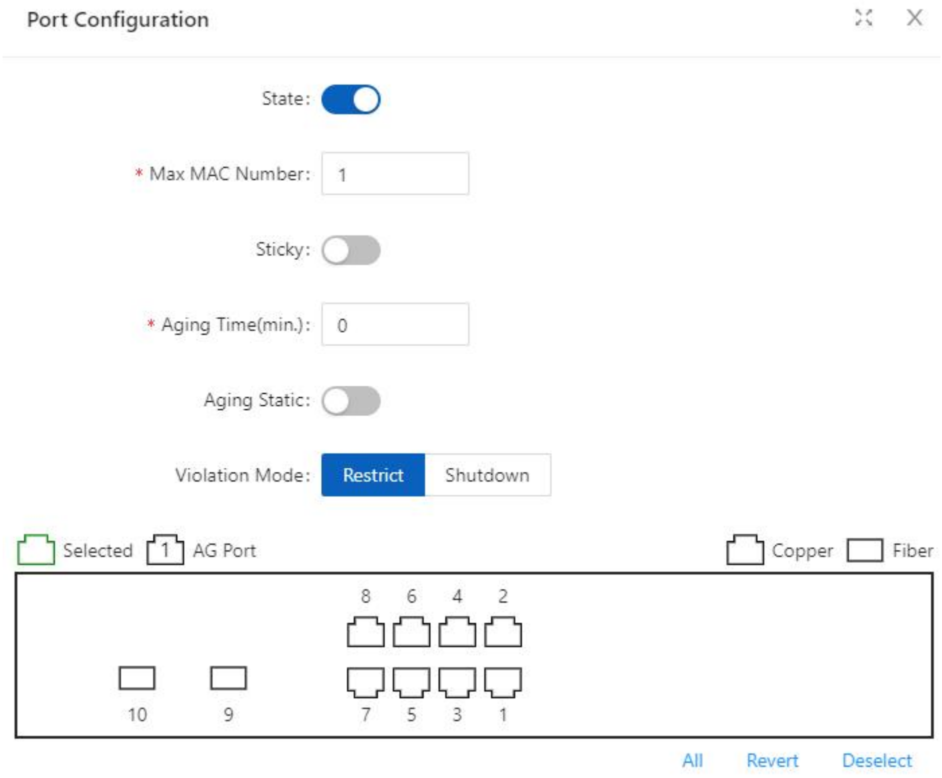


Port Configuration

Name	State	Max MAC Number	Sticky	Aging Time(min.)	Aging Static	Violation Mode	Action

Click the **Batch Edit** button below Port Configuration to enter the Port Configuration page, as shown in Figure 3-45. The items of the port configuration are described in Table 3-20.

Figure 3-45 Port security configuration page



Port Configuration

State: On

* Max MAC Number: 1

Sticky: Off

* Aging Time(min.): 0

Aging Static: Off

Violation Mode: Restrict | Shutdown

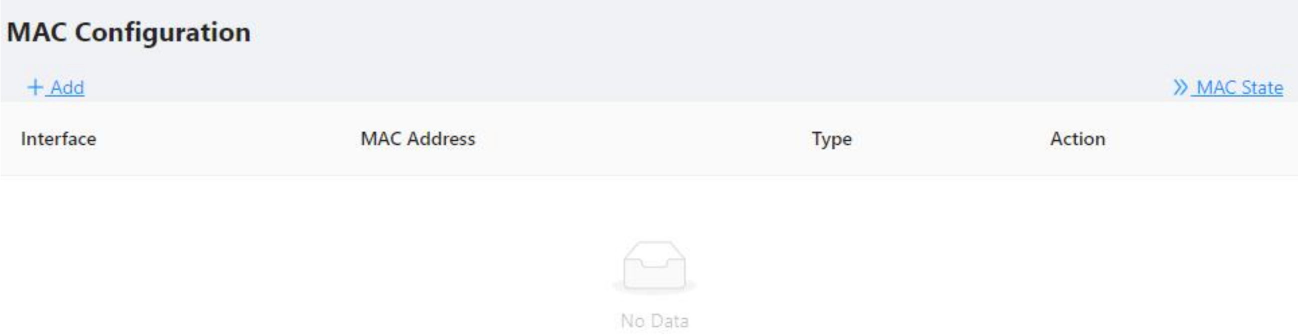
Table 3-20 The items of the port security configuration

Item		Description
Port Configuration	State	Enable/disable port Security of the interface.
	Max MAC Number	Configure the maximum number of secure MAC addresses for the port, the default maximum number of secure addresses is 1, the range is <1-1024>
	Sticky	Turn on/off the Sticky function.
	Aging Time(min)	Configure the security address aging time, in minutes. The default aging time is 0, which means that the aging function is turned off. Aging time range <0-1440> The default aging function only takes effect for dynamic and sticky security addresses.
	Aging Static	Enable the static security address aging function.
	Violation Mode	Configure port security violation handling, default violation mode is Restrict. Restrict：Prohibit illegal user data from passing, and log prompt Shutdown：shutdown interface，and resume passing after errdisable recovery time.

MAC Configuration

Select **Configuration** > **Security** > **MAC Configuration** in the navigation area to enter the MAC Configuration page as shown in Figure 3-46.

Figure 3-46 MAC configuration summary

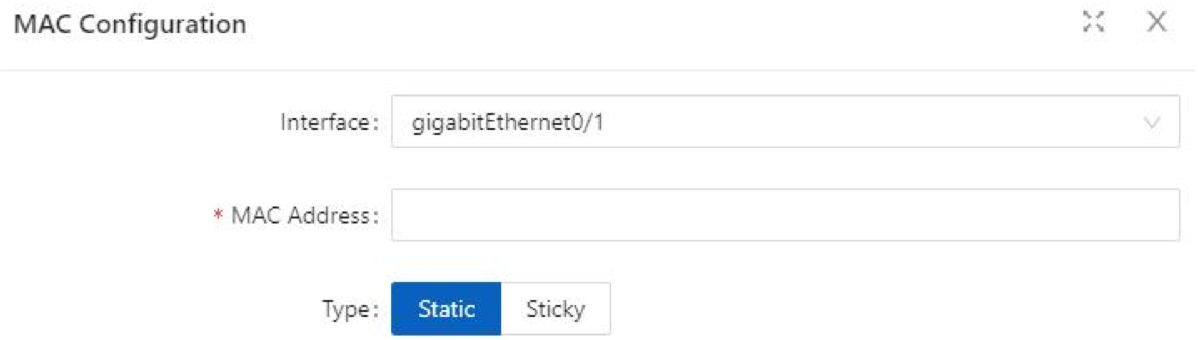


MAC Configuration

Interface	MAC Address	Type	Action

Click **+Add** to enter the MAC Configuration page as shown in Figure 3-47. The items of the mac configuration are described in Table 3-21.

Figure 3-47 MAC configuration page



MAC Configuration

Interface: gigabitEthernet0/1

* MAC Address:

Type: Static Sticky

Table 3-21 The items of the MAC configuration

Item		Description
MAC Configuration	Interface	Select the interface to be configured.
	MAC Address	Configure a static security address, the format of the security address: XXXX.XXXX.XXXX The security address cannot be a broadcast or multicast Address.
	Type	Configure the MAC address as dynamic or static.

3.6.2 IP Source Guard

3.6.2.1 Overview

IP Source Guard:

The IP Source Guard binding function allows IP packets conforming to the IP+MAC binding to pass through the port, and non-conforming packets are directly discarded, thereby achieving the purpose of preventing IP/MAC spoofing attacks.

The binding entries of IP Source Guard mainly come from two sources: user static configuration and dynamic acquisition in the IP DHCP snooping environment.

User static configuration: mainly for host users whose IP addresses are statically configured in the local area network.

IP DHCP snooping dynamic acquisition: mainly respond to the host users who dynamically acquire the IP address through DHCP in the local area network.

IP/MAC spoofing attack: Illegal MAC users send IP packets with legal source IP to realize the legalization of access identity.

ARP Check:

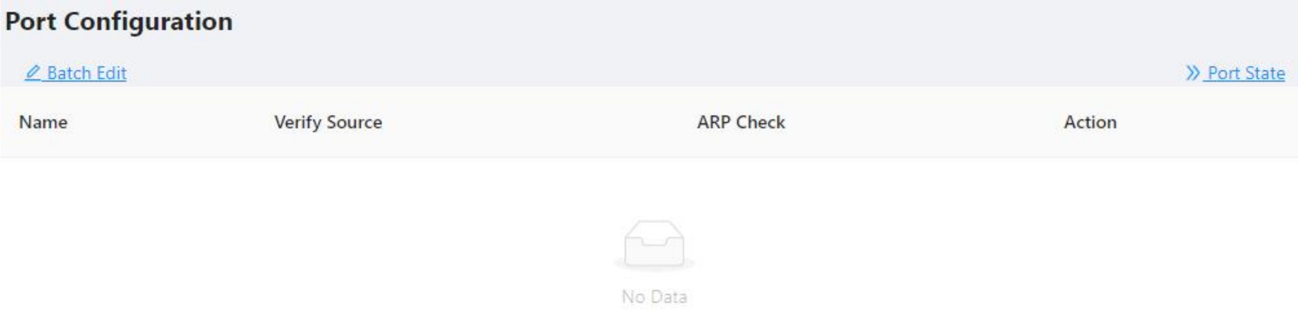
The ARP-check (ARP packet check) function filters all ARP packets under the port and discards all illegal ARP packets, which can effectively prevent ARP spoofing in the network and improve the stability of the network.

In the device that supports the ARP-check function, the ARP-check function can generate corresponding ARP filtering information based on the legal user information (IP+MAC) generated by the security application modules such as IP Source Guard, so as to realize the illegal ARP packets filtering in the network.

3.6.2.2 Configuring IP Source Guard

1. Select **Configuration** > **Security** > **IP Source Guard** in the navigation area to enter the IP Source Guard Summary page as shown in Figure 3-48.

Figure 3-48 IP source guard summary



Port Configuration

Batch Edit

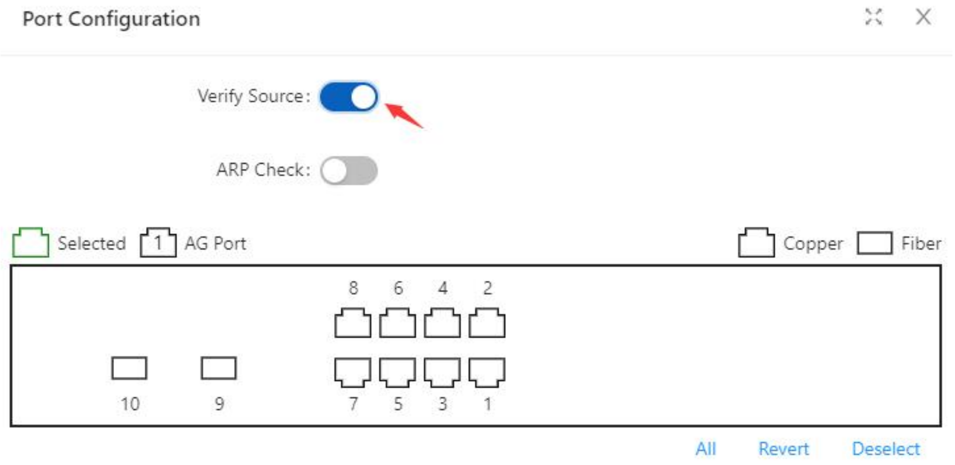
Port State

Name	Verify Source	ARP Check	Action

No Data

2. Click **Batch Edit** button below Port Configuration in the current page, select the interface to be configured in the port panel, click **Verify Source** button, as shown in Figure 3-49.

Figure 3-49 IP source guard port configuration



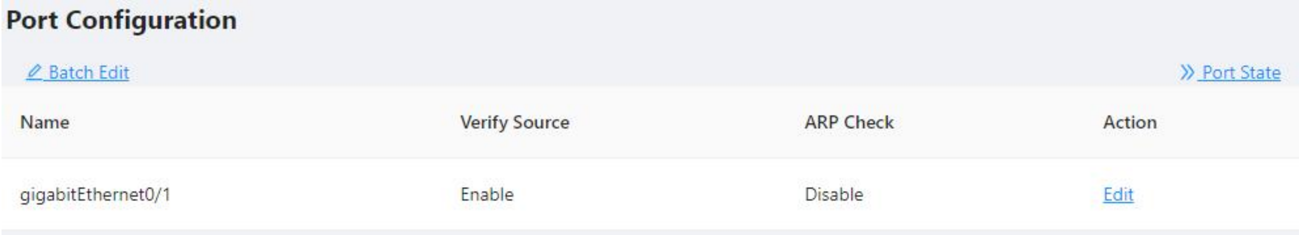
Port Configuration

Verify Source: ●

ARP Check: ○

3. Click **OK** button, the rules created were displayed in summary page as shown in Figure 3-50.

Figure 3-50 Port configuration



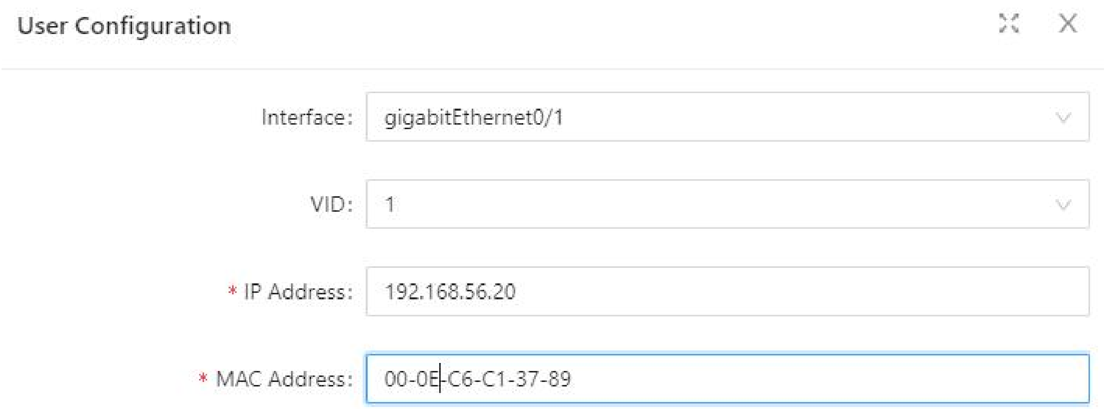
Port Configuration

Batch Edit | Port State

Name	Verify Source	ARP Check	Action
gigabitEthernet0/1	Enable	Disable	Edit

4. Click **+Add** button below User Configuration in current page, to enter the User Configuration page, Select the port in the interface box, text VID, IP Address, MAC Address, as shown in Figure 3-51.

Figure 3-51 IP source guard user configuration



User Configuration

Interface: gigabitEthernet0/1

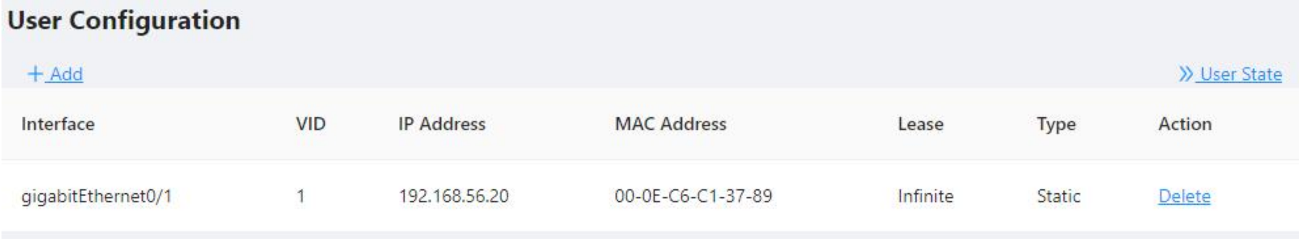
VID: 1

* IP Address: 192.168.56.20

* MAC Address: 00-0E-C6-C1-37-89

5. Click **OK** button, the rules created were displayed in summary page as shown in Figure 3-52.

Figure 3-52 IP source guard rules summary



User Configuration

+ Add | User State

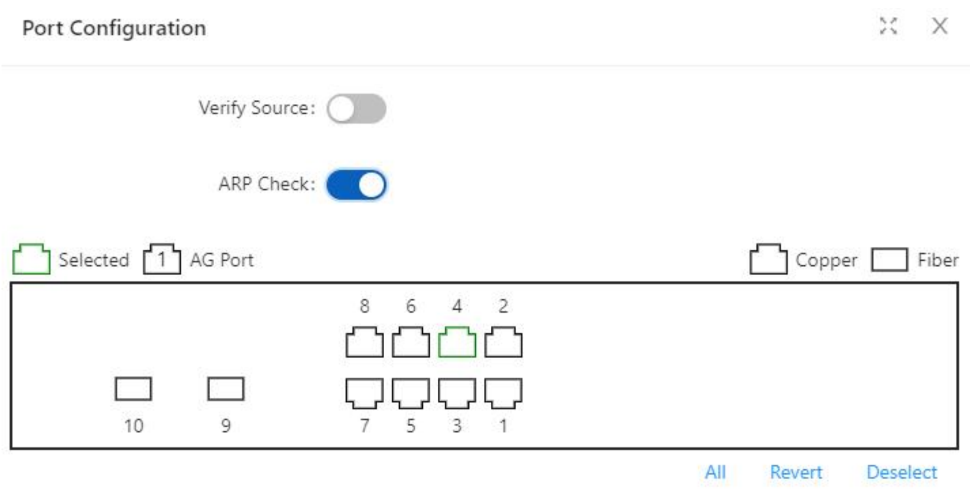
Interface	VID	IP Address	MAC Address	Lease	Type	Action
gigabitEthernet0/1	1	192.168.56.20	00-0E-C6-C1-37-89	Infinite	Static	Delete

3.6.2.3 Configuring ARP Check

1. Select **Configuration** > **Security** > **IP Source Guard** in the navigation area to enter the IP Source Guard Summary page as shown in Figure 3-48.

2. Click **Batch Edit** button below Port Configuration in the current page, select the interface to be configured in the port panel, click **ARP Check** button, as shown in Figure 3-53.

Figure 3-53 IP source guard ARP check

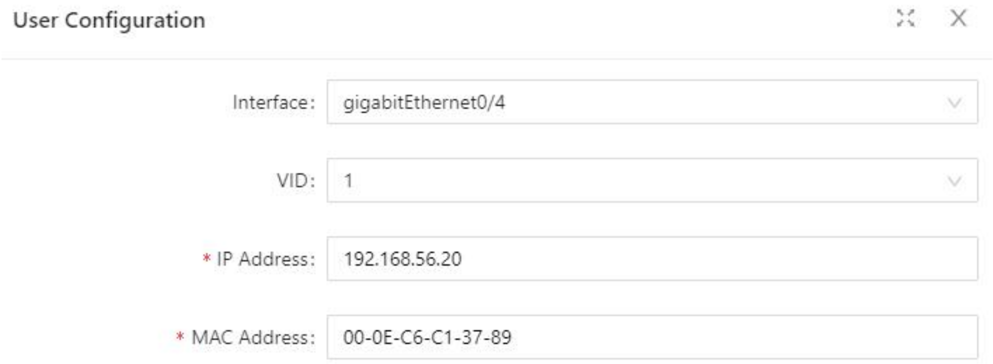

Port Configuration

Verify Source: ○

ARP Check: ●

3. Click **+Add** button below User Configuration in current page, to enter the User Configuration page, as shown in Figure 3-54.

Figure 3-54 IP source guard user configuration


User Configuration

Interface: gigabitEthernet0/4

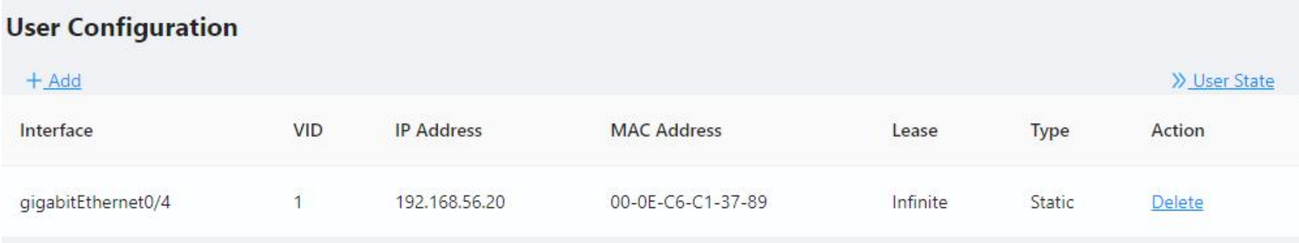
VID: 1

* IP Address: 192.168.56.20

* MAC Address: 00-0E-C6-C1-37-89

4. Click **OK** button, the rules created were displayed in summary page as shown in Figure 3-55.

Figure 3-55 ARP check rules


User Configuration

Interface	VID	IP Address	MAC Address	Lease	Type	Action
gigabitEthernet0/4	1	192.168.56.20	00-0E-C6-C1-37-89	Infinite	Static	Delete

3.6.3 Dot1X

3.6.3.1 Overview

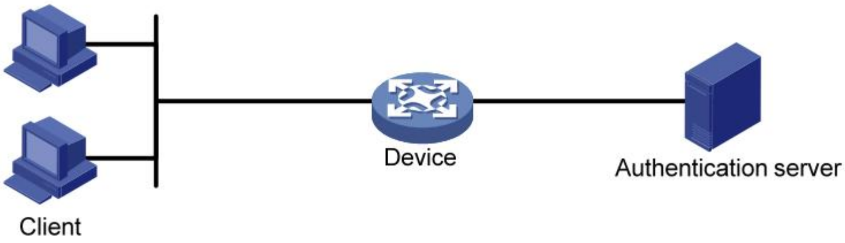
The 802.1X (Dot1X) protocol was proposed by the IEEE 802 LAN/WAN committee for security of wireless LANs (WLAN). It has been widely used on Ethernet as a common port access control mechanism.

As a port-based access control protocol, 802.1X authenticates and controls accessing devices at the port level. A device connected to an 802.1X-enabled port of an access control device can access the resources on the LAN only after passing authentication.

Architecture of 802.1X

802.1X operates in the typical client/server model and defines three entities: Client, Device, and Server, as shown in below.

Figure 3-56 802.1X



- Client is an entity seeking access to the LAN. It resides at one end of a LAN segment and is authenticated by Device at the other end of the LAN segment. Client is usually a user-end device such as a PC. 802.1X authentication is triggered when an 802.1X-capable client program is launched on Client. The client program must support Extensible Authentication Protocol over LAN (EAPOL).
- Device, residing at the other end of the LAN segment, authenticates connected clients. Device is usually an 802.1X-enabled network device and provides access ports (physical or logical) for clients to access the LAN.
- Server is the entity that provides authentication services to Device. Server, normally running RADIUS (Remote Authentication Dial-in User Service), serves to perform authentication, authorization, and accounting services for users.

Authentication Modes of 802.1x

The 802.1X authentication system employs the Extensible Authentication Protocol (EAP) to exchange authentication information between the client, device, and authentication server. Client Device Server

- Between the client and the device, EAP protocol packets are encapsulated using EAPOL to be transferred on the LAN.
- Between the device and the RADIUS server, EAP protocol packets can be exchanged in two modes: EAP relay and EAP termination. In EAP relay mode, EAP packets are encapsulated in EAP over RADIUS (EAPOR) packets on the device, and then relayed by device to the RADIUS server. In EAP termination mode, EAP packets are terminated at the device, converted to RADIUS packets either with the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) attribute, and then transferred to the RADIUS server.

Basic Concepts of 802.1x

These basic concepts are involved in 802.1X: controlled port/uncontrolled port, authorized state/unauthorized state, and control direction.

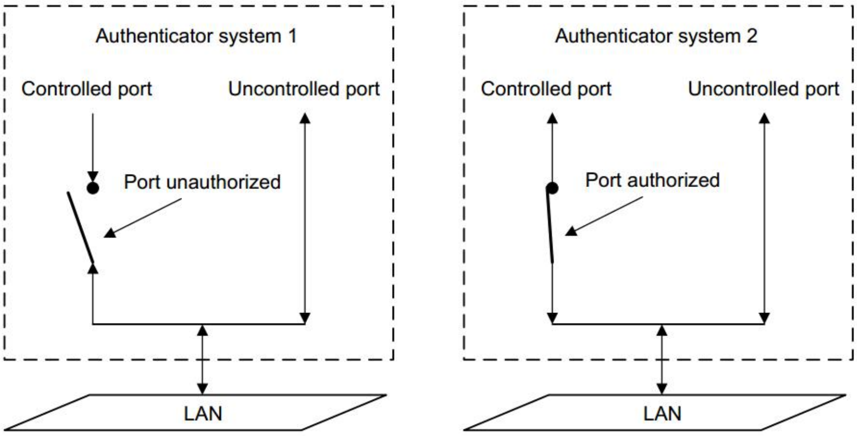
Controlled Port and Uncontrolled Port

A device provides ports for clients to access the LAN. Each port can be regarded as a unity of two logical ports: a controlled port and an uncontrolled port. Any packets arriving at the port are visible to both logical ports.

- The uncontrolled port is always open in both the inbound and outbound directions to allow EAPOL protocol packets to pass, guaranteeing that the client can always send and receive authentication packets.
- The controlled port is open to allow data traffic to pass only when it is in the authorized state.

Authorized State and Unauthorized State

Figure 3-57 Authorized/unauthorized state of a controlled port



A controlled port can be in either authorized state or unauthorized state, which depends on the authentication result, as shown in Figure 3-57.

You can control the port authorization status of a port by setting port authorization mode to one of the following:

- Force-Authorized: Places the port in authorized state, allowing users of the port to access the network without authentication.
- Force-Unauthorized: Places the port in unauthorized state, denying any access requests from users of the port.
- Auto: Places the port in the unauthorized state initially to allow only EAPOL packets to pass, and turns the port into the authorized state to allow access to the network after the users pass authentication. This is the most common choice.

Control Direction

In the unauthorized state, the controlled port can be set to deny traffic to and from the client or just the traffic from the client.

802.1X Authentication Triggering

802.1X authentication can be initiated by either a client or the device.

Unsolicited Triggering of A Client

A client can initiate authentication unsolicitedly by sending an EAPOL-Start packet to the device. The destination address of the packet is 01-80-C2-00-00-03, the multicast address specified by the IEEE 802.1X protocol.

Some devices in the network may not support multicast packets with the above destination address, and unable to receive authentication requests of clients as a result. To solve this problem, the device also supports EAPOL-Start packets using a broadcast MAC address as the destination address.

Unsolicited Triggering of the Device

The device can trigger authentication by sending EAP-Request/Identity packets to unauthenticated clients periodically (every 30 seconds by default). This method can be used to authenticate clients that cannot send EAPOL-Start packets unsolicitedly to trigger authentication, for example, a client running the 802.1X client application provided by Windows XP.

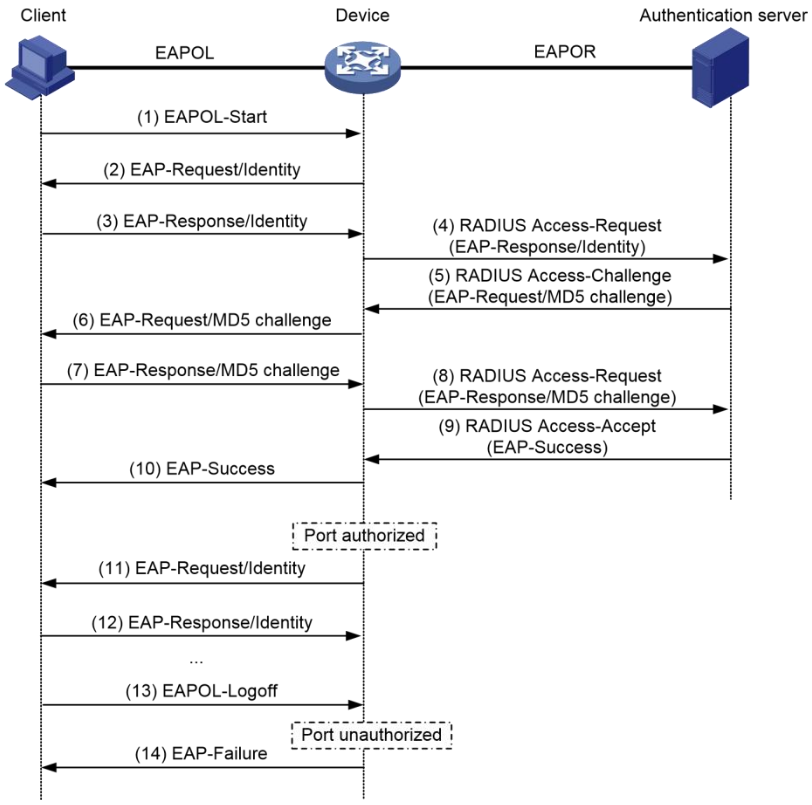
Authentication Process of 802.1x

An 802.1X device communicates with a remote RADIUS server in two modes: EAP relay and EAP termination. The following describes the 802.1X authentication procedure in the two modes, which is triggered by the client in the examples.

EAP Relay

EAP relay is defined in IEEE 802.1X. In this mode, EAP packets are carried in an upper layer protocol, such as RADIUS, so that they can go through complex networks and reach the authentication server. Generally, relaying EAP requires that the RADIUS server support the EAP attributes of EAP-Message and Message-Authenticator, which are used to encapsulate EAP packets and protect RADIUS packets carrying the EAP-Message attribute respectively.

Figure 3-58 Show the message exchange procedure with EAP-MD5


Client
Device
Authentication server
EAPOL
EAPOR
(1) EAPOL-Start
(2) EAP-Request/Identity
(3) EAP-Response/Identity
(4) RADIUS Access-Request (EAP-Response/Identity)
(5) RADIUS Access-Challenge (EAP-Request/MD5 challenge)
(6) EAP-Request/MD5 challenge
(7) EAP-Response/MD5 challenge
(8) RADIUS Access-Request (EAP-Response/MD5 challenge)
(9) RADIUS Access-Accept (EAP-Success)
(10) EAP-Success
Port authorized
(11) EAP-Request/Identity
(12) EAP-Response/Identity
...
(13) EAPOL-Logoff
Port unauthorized
(14) EAP-Failure

1. When a user launches the 802.1X client software and enters the registered username and password, the 802.1X client software generates an EAPOL-Start frame and sends it to the device to initiate an authentication process.
2. Upon receiving the EAPOL-Start frame, the device responds with an EAP-Request/Identity packet for the username of the client.
3. When the client receives the EAP-Request/Identity packet, it encapsulates the username in an EAP-Response/Identity packet and sends the packet to the device.
4. Upon receiving the EAP-Response/Identity packet, the device relays the packet in a RADIUS Access-Request packet to the authentication server.
5. When receiving the RADIUS Access-Request packet, the RADIUS server compares the identify information against its user information table to obtain the corresponding password information. Then, it encrypts the password information using a randomly generated challenge, and sends the challenge information through a RADIUS Access-Challenge packet to the device.
6. After receiving the RADIUS Access-Challenge packet, the device relays the contained EAP-Request/MD5 Challenge packet to the client.
7. When receiving the EAP-Request/MD5 Challenge packet, the client uses the offered challenge to encrypt the password part (this process is not reversible), creates an EAP-Response/MD5 Challenge packet, and then sends the packet to the device.
8. After receiving the EAP-Response/MD5 Challenge packet, the device relays the packet through a RADIUS Access-Request packet to the authentication server.

9. When receiving the RADIUS Access-Request packet, the RADIUS server compares the password information encapsulated in the packet with that generated by itself. If the two are identical, the authentication server considers the user valid and sends to the device a RADIUS Access-Accept packet.

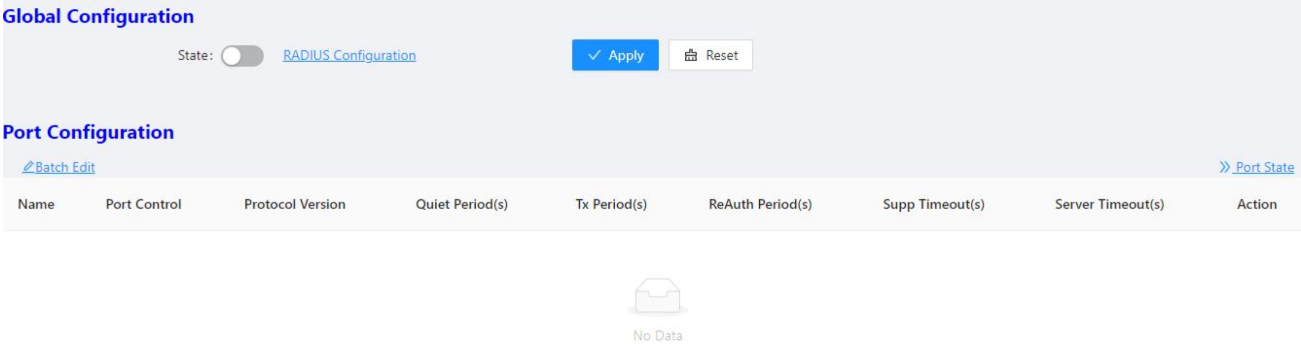
10. Upon receiving the RADIUS Access-Accept packet, the device opens the port to grant the access request of the client. After the client gets online, the device periodically sends handshake requests to the client to check whether the client is still online. By default, if two consecutive handshake attempts end up with failure, the device concludes that the client has gone offline and performs the necessary operations, guaranteeing that the device always knows when a client goes offline.

11. The client can also send an EAPOL-Logoff frame to the device to go offline unsolicitedly. In this case, the device changes the status of the port from authorized to unauthorized and sends an EAP-Failure packet to the client.

3.6.3.2 Configuring Dot1X

Select **Security** > **Dot1x**> **Configuration** from the navigation area. The system automatically displays the 802.1X Global Configuration and Port Configuration, as shown in Figure 3-59 and Figure 3-60. Table 3-22 and Table 3-23 separately describe the global configuration and port configuration items.

Figure 3-59 802.1X global configuration



Global Configuration

State: RADIUS Configuration

Port Configuration

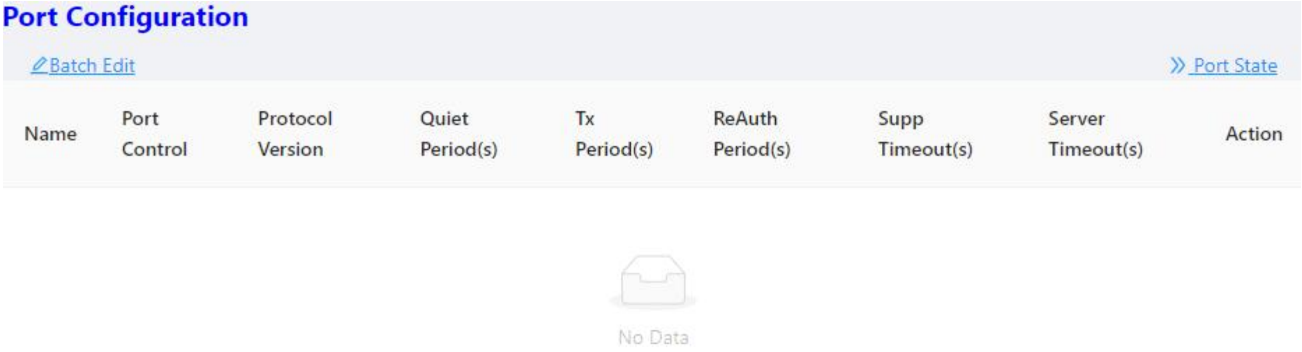
Name	Port Control	Protocol Version	Quiet Period(s)	Tx Period(s)	ReAuth Period(s)	Supp Timeout(s)	Server Timeout(s)	Action

No Data

Table 3-22 The 802.1X configuration items

Item		Description
Global Configuration	State	Enables the 802.1X feature on your switch.
	RADIUS Configuration	Click to jump to the RADIUS configuration interface

Figure 3-60 802.1X port configuration


Port Configuration

Name	Port Control	Protocol Version	Quiet Period(s)	Tx Period(s)	ReAuth Period(s)	Supp Timeout(s)	Server Timeout(s)	Action

Table 3-23 The 802.1X port configuration items

Item		Description
Port Configuration	Name	Physical interface name
	Port Control	Port control mode
	Protocol Version	Eapol protocol version, default version 2
	Quiet Period(s)	Sets the number of seconds that the switch remains in the quiet-period following a failed authentication exchange with the client. The range is 0 to 65,535 seconds; the default is 60. When the switch cannot authenticate the client, the switch remains idle for a set period, and then tries again. The idle time is determined by the quiet-period value.
	Tx Period(s)	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65,535 seconds; the default is 30.
	ReAuth Enabled	Enables periodic reauthentication of the client
	ReAuth Period(s)	Specifies the number of seconds between reauthentication attempts or have the switch use a RADIUS-provided session timeout. The range is 1 to 65,535; the default is 3600 seconds. This command affects the behavior of the switch only if periodic reauthentication is enabled.
	Supp Timeout(s)	Sets the number of seconds that the switch waits for a response to an EAP-Request/MD5 Challenge frame from the client before retransmitting the request. The range is 1 to 65,535 seconds; the default is 30.
	Server Timeout(s)	Sets the number of seconds that the switch waits for a response to a RADIUS Access-Request packet from the server. The range is 1 to 65,535 seconds; the default is 30.

3.6.4 MAC Auth

3.6.4.1 Overview

Authentication of MAC addresses is supported using a RADIUS server that contains a database of all valid users.

When the MAC-auth option is enabled on any interface, all source MAC addresses from any incoming frame are sent for authentication. If the username and password of the source address are configured in the RADIUS server, then authentication succeeds, otherwise it fails. When authentication succeeds, the source MAC is added to the forwarding table with forwarding enabled. In the case of failure, the source MAC either is added to the forwarding table as discarded or is added to a restricted VLAN.

NOTE:

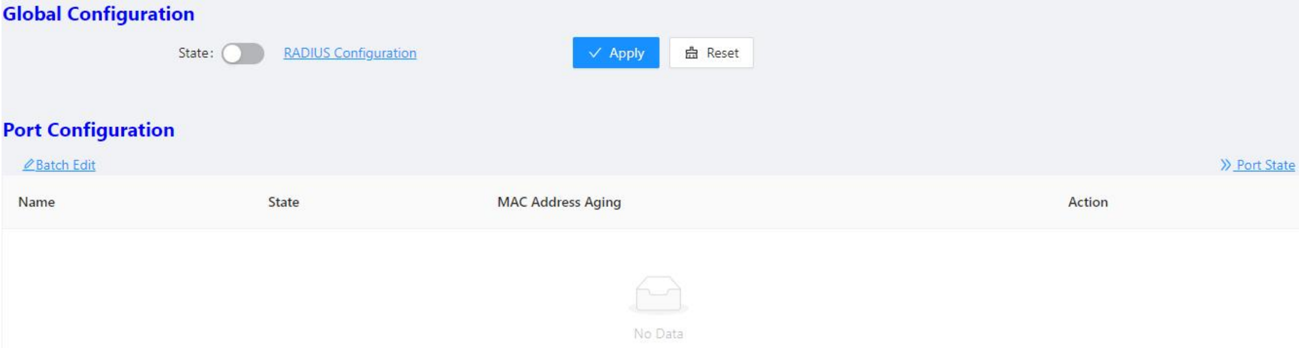
- If the configured static MAC is the same as the silent MAC, the MAC silent function after the MAC address authentication fails will be invalid.

3.6.4.2 Configuring MAC Authentication

Displaying MAC Authentication Summary

Select **Configuration > Security > MAC Authentication** from the navigation area. The system automatically displays the MAC Authentication summary, as shown in Figure 3-61. Table 3-24 describes the MAC Authentication Summary items.

Figure 3-61 The MAC authentication summary



Global Configuration

State: RADIUS Configuration

Port Configuration

Name	State	MAC Address Aging	Action

No Data

Table 3-24 The MAC authentication summary items

Item		Description
Global Configuration	State	Enables the 802.1X feature on your switch.
	RADIUS Configuration	Click to jump to the RADIUS configuration interface
Port Configuration	Name	Physical interface name
	State	Display the state of MAC Auth
	MAC Address Aging	Display the state of MAC Address Aging
	Action	Click to Edit the rule

Configuring MAC Authentication

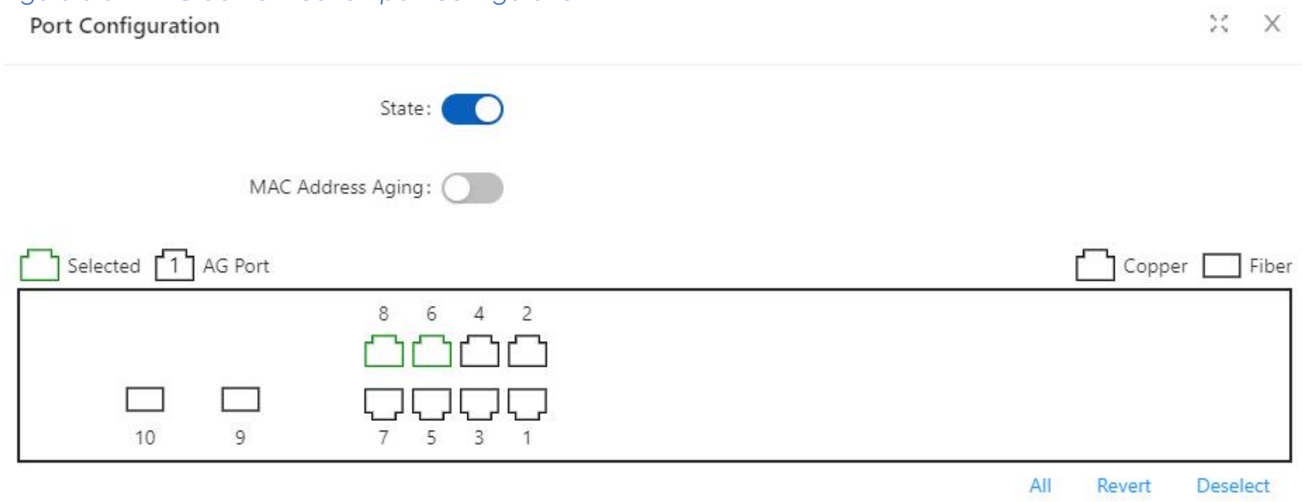
1. Enable MAC Auth

Select **Configuration** > **Security** > **MAC Authentication** from the navigation area. Click **State** button in Global Configuration, click **Apply** button to enable the MAC auth function.

2. Configuring Port

Click **Batch Edit** button below Port Configuration to enter the Port Configuration page, as shown in Figure 3-62. Click **State** button, select the port to be configured in port panel, click **OK** button.

Figure 3-62 MAC authentication port configuration



Port Configuration

State: on

MAC Address Aging: off

3.6.5 RADIUS

3.6.5.1 Overview

Remote Authentication Dial-In User Service (RADIUS) is protocol for implementing Authentication, Authorization, and Accounting (AAA).

RADIUS is a distributed information interaction protocol using the client/server model. RADIUS can protect networks against unauthorized access and is often used in network environments where both high security and remote user access are required. RADIUS uses UDP, and its packet format and message transfer mechanism are based on UDP. It uses UDP port 1812 for authentication and 1813 for accounting.

RADIUS was originally designed for dial-in user access. With the diversification of access methods, RADIUS has been extended to support more access methods, for example, Ethernet access and ADSL access. It uses authentication and authorization in providing access services and uses accounting to collect and record usage information of network resources.

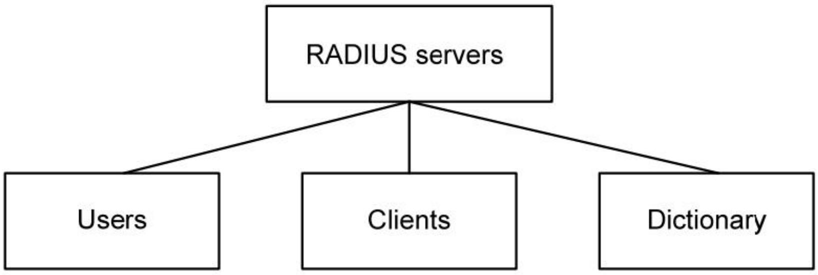
Client/server Model

- Client: The RADIUS client runs on the NASs located throughout the network. It passes user information to designated RADIUS servers and acts on the responses (for example, rejects or accepts user access requests).

- Server: The RADIUS server runs on the computer or workstation at the network center and maintains information related to user authentication and network service access. It listens to connection requests, authenticates users, and returns the processing results (for example, rejecting or accepting the user access request) to the clients.

  In general, the RADIUS server maintains three databases: Users, Clients, and Dictionary, as shown in Figure 3-63.

Figure 3-63 RADIUS server components



- Users: Stores user information such as the usernames, passwords, applied protocols, and IP addresses.
- Clients: Stores information about RADIUS clients, such as the shared keys and IP addresses.
- Dictionary: Stores information about the meanings of RADIUS protocol attributes and their values.

Security and Authentication Mechanisms

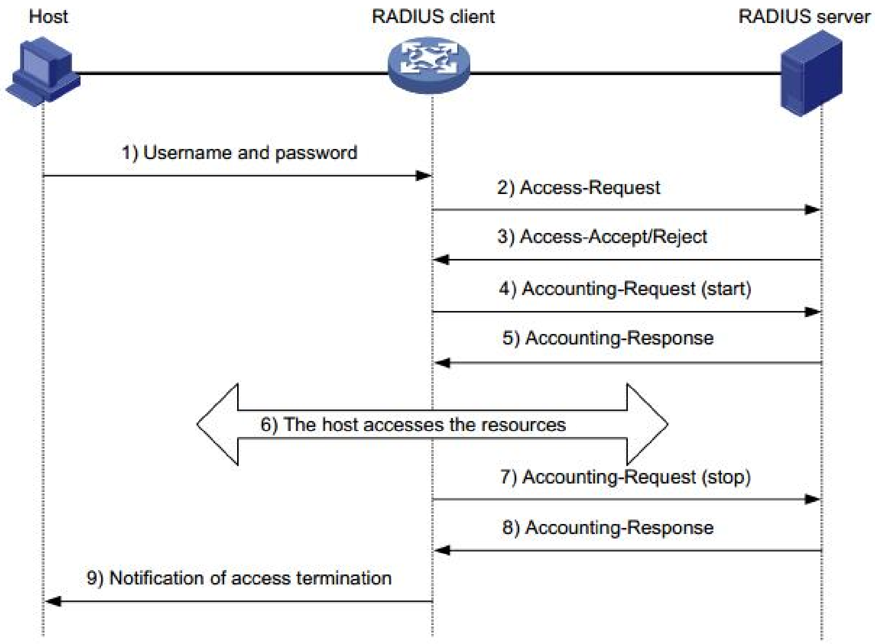
Information exchanged between a RADIUS client and the RADIUS server is authenticated with a shared key, which is never transmitted over the network. This enhances the information exchange security. In addition, to prevent user passwords from being intercepted on insecure networks, RADIUS encrypts passwords before transmitting them.

A RADIUS server supports multiple user authentication methods, for example, the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) of the Point-to-Point Protocol (PPP). Moreover, a RADIUS server can act as the client of another AAA server to provide authentication proxy services.

Basic Message Exchange Process of RADIUS

Figure 3-64 illustrates the interaction of the host, the RADIUS client, and the RADIUS server.

Figure 3-64 Basic message exchange process of RADIUS



The following is how RADIUS operates:

1. The host initiates a connection request carrying the username and password to the RADIUS client.
2. Having received the username and password, the RADIUS client sends an authentication request (Access-Request) to the RADIUS server, with the user password encrypted by using the Message-Digest 5 (MD5) algorithm and the shared key.
3. The RADIUS server authenticates the username and password. If the authentication succeeds, it sends back an Access-Accept message containing the user 's authorization information. If the authentication fails, it returns an Access-Reject message.
4. The RADIUS client permits or denies the user according to the returned authentication result. If it permits the user, it sends a start-accounting request (Accounting-Request) to the RADIUS server.
5. The RADIUS server returns a start-accounting response (Accounting-Response) and starts accounting.
6. The user accesses the network resources.
7. The host requests the RADIUS client to tear down the connection and the RADIUS client sends a stop-accounting request (Accounting-Request) to the RADIUS server.
8. The RADIUS server returns a stop-accounting response (Accounting-Response) and stops accounting for the user.
9. The user stops access to network resources

NOTE:

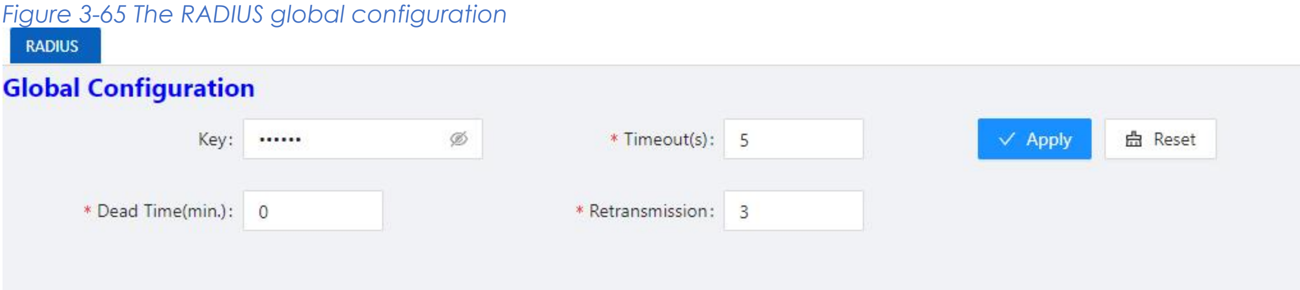
- Do not support RADIUS accounting function

3.6.5.2 Configuring RADIUS

RADIUS Global Configuration

Select **Configuration > Security > RADIUS** from the navigation area. The system automatically displays the RADIUS Global Configuration, as shown in Figure 3-65. Table 3-25 describes the RADIUS global configuration items.

Figure 3-65 The RADIUS global configuration



Key: ••••••
* Timeout(s): 5
* Dead Time(min.): 0
* Retransmission: 3

Table 3-25 The RADIUS global configuration items

Item		Description
Global Configuration	Key	Global default password configuration; configurable, unreadable; optional configuration
	Timeout	Global server timeout; optional configuration
	Retransmission	Global server retransmissions; optional configuration
	Dead Time	Server death duration; optional configuration; default 0, indicating that the server will be revived immediately after death

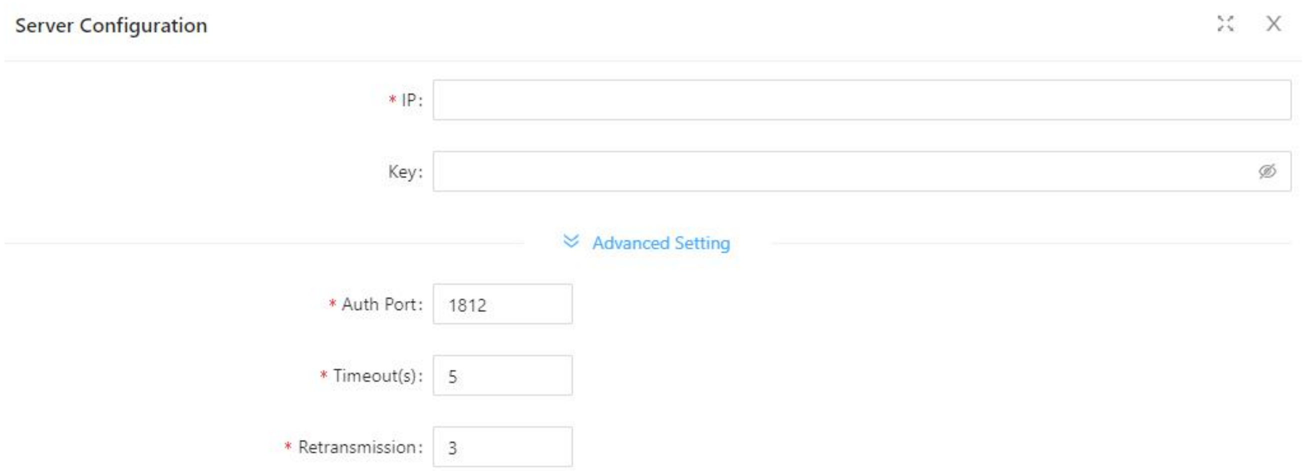
RADIU Server Configuration

Click **+Add** button below Server Configuration in current page to enter the Configuration page, as shown in Figure 3-66. Table 3-26 describes the RADIUS Server Configuration items.

Table 3-26 The RADIUS server configuration items

Item	Description
IP	Server IP address
Auth Port	Server authentication port number; default 1812
Key	Server key; global configuration when not configured
Timeout	Server timeout; default 5s
Retransmission	Server retransmission times, default 3 times

Figure 3-66 The RADIUS server configuration



Server Configuration

* IP:

Key:

Advanced Setting

* Auth Port: 1812

* Timeout(s): 5

* Retransmission: 3

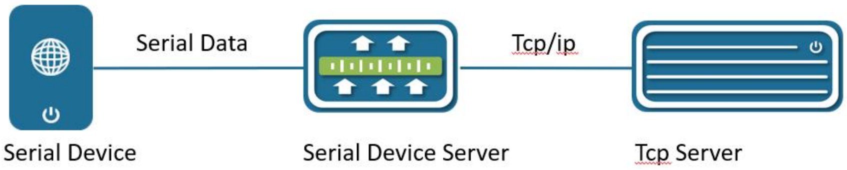
3.7 Control

3.7.1 Serial Servers

3.7.1.1 Overview

The serial device server is used to connect serial devices to the Ethernet. The serial device server supports bidirectional conversion and transmission of network data and serial data. Serial device server work in tcp-client mode, as shown in Figure 3-67.

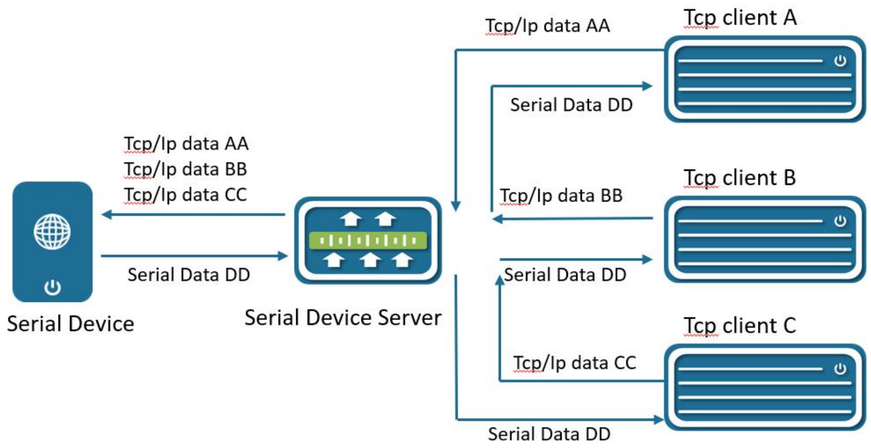
Figure 3-67 Serial device server work in tcp-client mode



Serial device server in tcp-client mode provides client connections for TCP network servers. it actively initiates a connection and connect to the server to realize the interaction between serial device and TCP server. The TCP/IP and serial data are transparently transmitted in both directions. The serial device server supports to establish multiple TCP Clients to connect to different TCP Server. Serial device server work in tcp-server mode, as show in Figure 3-68.

In TCP Server mode, the module monitors the local port, accepts and establishes a connection for data communication when a connection request is sent. Used for communication with TCP clients within a local area network. It is suitable for scenarios where there is no server in the LAN and there are multiple computers or mobile phones requesting data from the module.

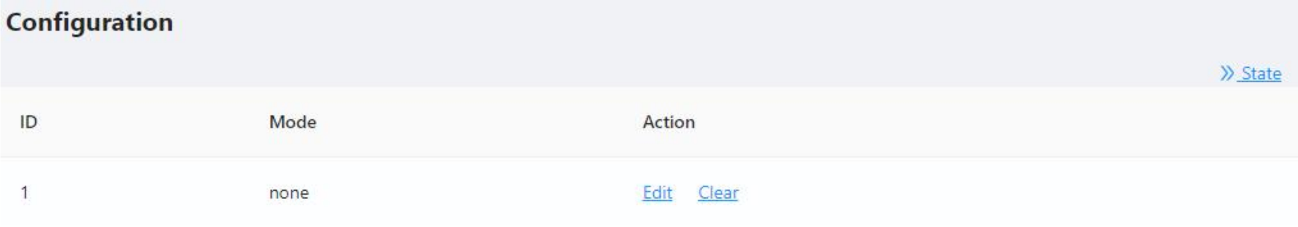
Figure 3-68 Serial device server work in tcp-server mode



3.7.1.2 Configuring Serial Server

Select **Configuration** > **Control** > **Serial Server** from the navigation area. The system automatically displays the Serial Server Configuration page, as shown in Figure 3-69.

Figure 3-69 Serial server configuration summary



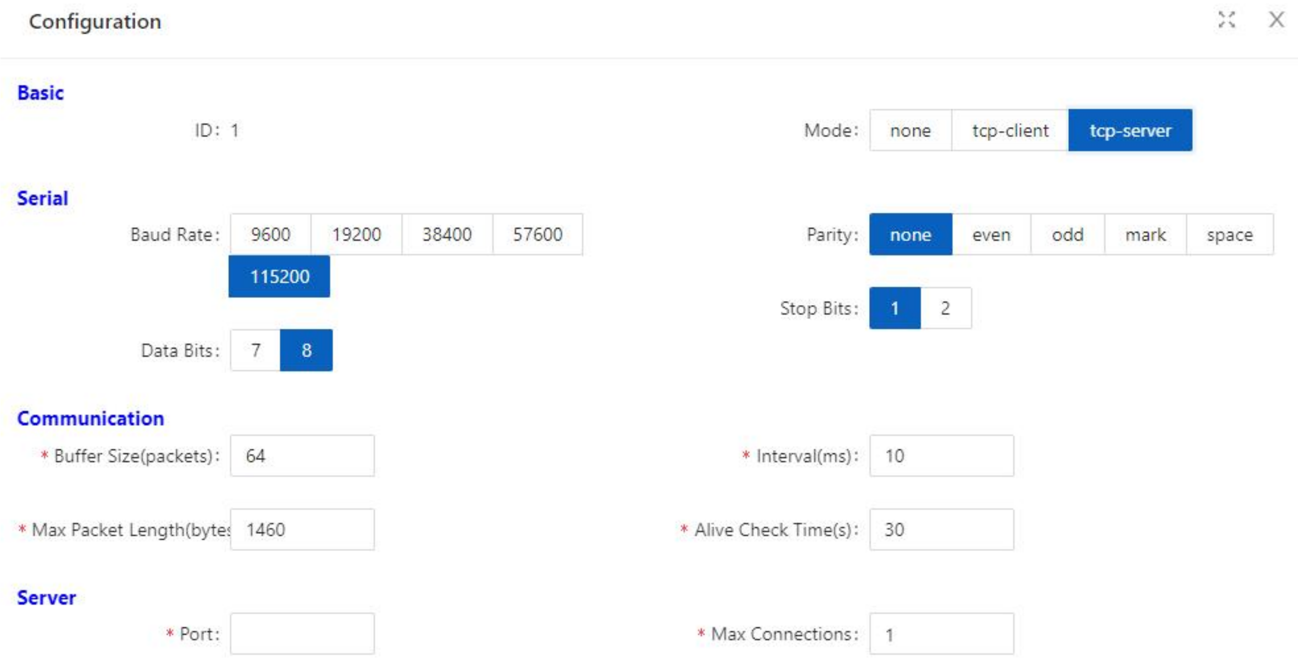
Configuration

» State

ID	Mode	Action
1	none	Edit Clear

Click **Edit** button to enter Serial Server Configuration page, as shown in Figure 3-70. Table 3-27 describes the serial server configuration items.

Figure 3-70 Serial server configuration



Configuration

Basic

ID: 1

Mode: none | tcp-client | [✓ tcp-server]

Serial

Baud Rate: 9600 | 19200 | 38400 | 57600 | [✓ 115200]

Parity: [✓ none] | even | odd | mark | space

Stop Bits: [✓ 1] | 2

Data Bits: 7 | [✓ 8]

Communication

* Buffer Size(packets): 64

* Interval(ms): 10

* Max Packet Length(bytes: 1460

* Alive Check Time(s): 30

Server

* Port:

* Max Connections: 1

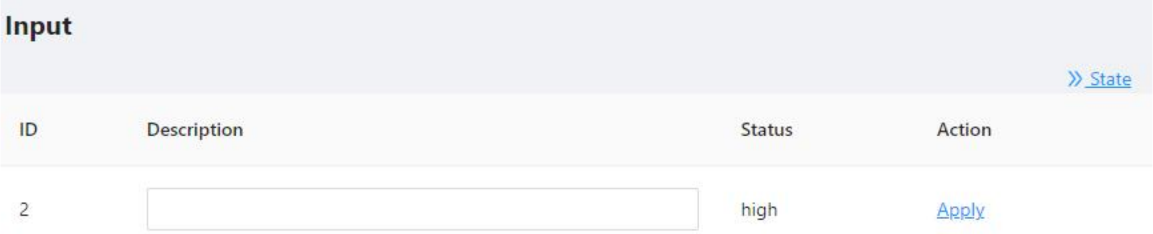
Table 3-27 Serial server configuration items

Item		Description
Basic	ID	Serial port number
Mode	None	Shut down the serial port server
	tcp-client	Configure the working mode to tcp-client
	tcp-server	Configure the working mode to tcp-server
Serial	Baud Rate	The baud rate of the serial port is configured, and there are five kinds of options: 9600, 19200, 38400, 57600, and 115200
	Data Bits	The data bits of the serial port are configured, and there are two kinds of options: 7 and 8
	Parity	There are five types of configuration checksum methods: none, even, odd, mark, and space
	Stop Bits	There are two options for configuring the stop bit, 1 and 2
Communication	Buffer size	Serial port data bits are transmitted at low speed, and the data is transferred from the network end to the serial port side to increase the fifo, improve the forwarding ability, the range < 0-128>, the default 64
	Max packet Length	The length of the serial port data packet, beyond the LEGGTH value, the packet is forwarded to the network end, the range <0-1460>, the default is 1460
	Interval	If the interval between the bytes before and after the serial port data exceeds MILLISECONDS, the post-byte data is recognized as the new message header byte The range < 1-1000 >, the default is 10ms
	Alive check time	Configure the serial port server to keep alive, during which there is no data interaction, then active detection is initiated
Client	Remote IP	Configure the remote connection IP address
	Remote port	Configure the port number for the remote connection, ranging from < 1-65535>
	Local port	For optional configurations, the default system is automatically assigned
Server	Port	Configure the tcp-server port number, which < range from 1-65535>
	Max connections	The maximum number of connections in tcp-server mode, ranging from 1 to 65535 >

3.7.2 IO Control

IO control module is divided into DI, DO two parts. In current software, DO only supports simple manual control relay (DO) ON/OFF switching function, as shown in Figure 3-71. DI only supports input level high and low judgment, as shown in Figure 3-72.

Figure 3-71 DI configuration page

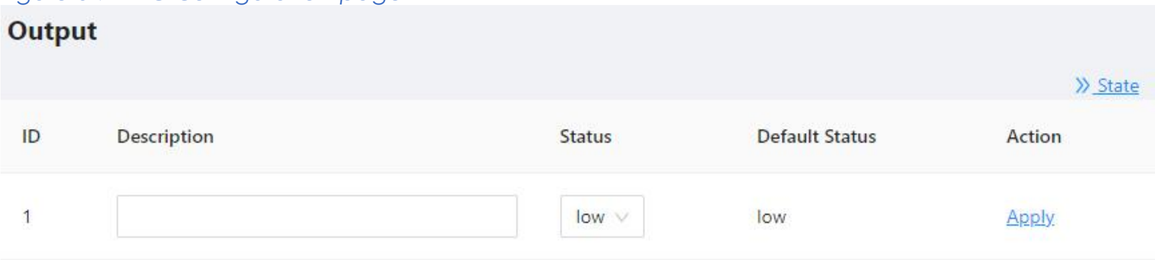


Input

» State

ID	Description	Status	Action
2		high	Apply

Figure 3-72 DO configuration page



Output

» State

ID	Description	Status	Default Status	Action
1		low	low	Apply

3.8 LoopDetect

3.8.1 Overview

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

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

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

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

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

3.8.2 Configuring LoopDetect

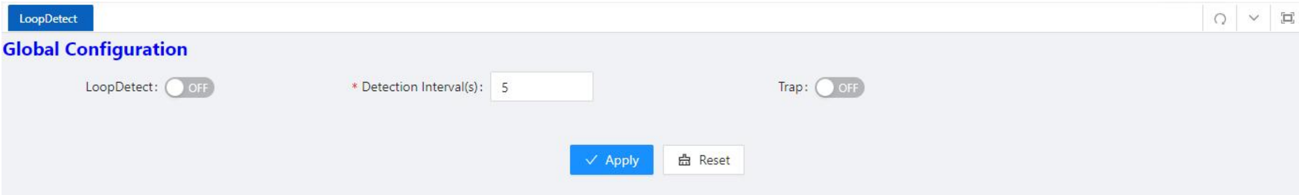
LoopDetect Configuration

1. Select **Configuration** > **LoopDetect** in the navigation area to enter the LoopDetect page. This page contains two parts: Global Configuration and Port Configuration.

2. Turn on the loop detection switch in the global configuration page, configure the detection

interval, turn on the Trap switch (optional), and click the **Apply** button to complete the configuration, as shown in Figure 3-73, the Table 3-28 describes the items of PoE global configuration.

Figure 3-73 LoopDetect global configuration



LoopDetect

Global Configuration

LoopDetect: OFF

* Detection Interval(s): 5

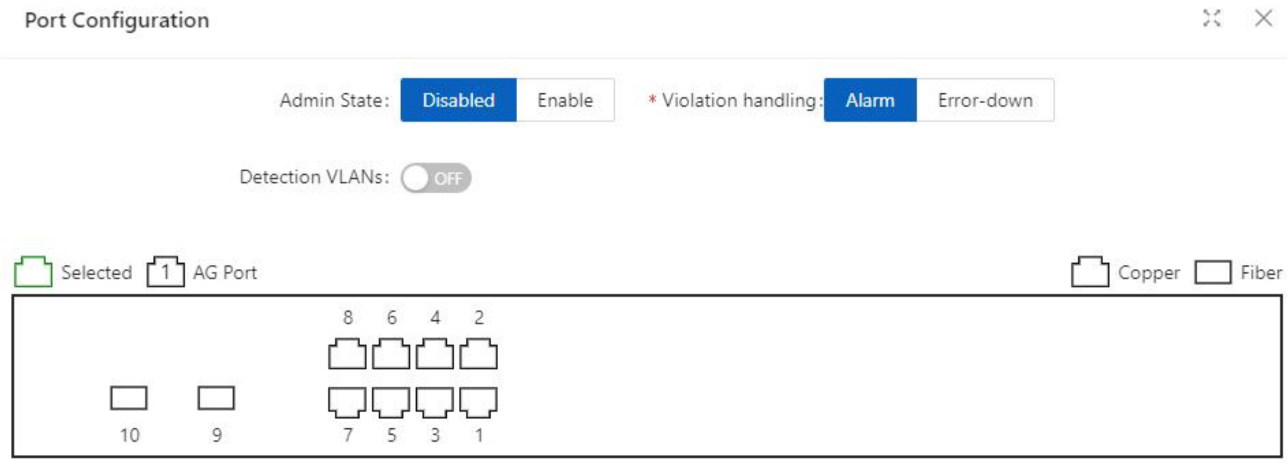
Trap: OFF

Table 3-28 Loop detection global configuration items

Item	Description
Loop detection	Turn on/off the loop detection function. The default is to turn off globally and the port.
Detection interval	Configure loop detection interval, range 5-300 seconds, default 5 seconds
Trap	Enable/disable loop fault trap alarm

3. Click the **Batch Edit** button under Port Configuration or the **Edit** button behind the port that needs to be configured to enter the loop detection port configuration interface, configure the management status, violation handling method, VLAN domain detection, and select the required. The port that enables this function is shown in Figure 3-74, and the parameter description is shown in Table 3-29.

Figure 3-74 LoopDetect port configuration



Port Configuration

Admin State: Disabled Enable

* Violation handling: Alarm Error-down

Detection VLANs: OFF

Table 3-29 Loop detection port configuration items

Item	Description
Admin State	Enable: Enable the loop detection function of the port Disabled: Turn off the loop detection function of the port
Violation handling	Alarm: Trap alarm when a loop occurs Error-down: When a loop occurs, shut down the loop port.
Detection VLANs	Detect whether a data path loop occurs within the specified VLAN domain

4 Advance

4.1 LLDP

4.1.1 Overview

In a heterogeneous network, a standard configuration exchange platform ensures that different types of network devices from different vendors can discover one another and exchange configuration.

The Link Layer Discovery Protocol (LLDP) is specified in IEEE 802.1AB. The protocol operates on the data link layer to exchange device information between directly connected devices. With LLDP, a device sends local device information as TLV (type, length, and value) triplets in LLDP Data Units (LLDPDUs) to the directly connected devices. Local device information includes its system capabilities, management IP address, device ID, port ID, and so on. The device stores the device information in LLDPDUs from the LLDP neighbors in a standard MIB. LLDP enables a network management system to quickly detect and identify Layer 2 network topology changes.

NOTE:

- TLV for PoE-related sections is not supported.

4.1.2 Configuring LLDP

LLDP Global Configuration

Select **Advance** > **Layer2** > **LLDP Configuration** in the navigation area to enter the Global Configuration page, as shown in Figure 4-1. Table 4-1 describes the Global Configuration items.

1. Click enable button ● behind **Status**.

2. Type the boxes behind of the **System Name** and **Description**.

3. Click **Apply** button to enable LLDP Configuration.

Figure 4-1 LLDP global configuration

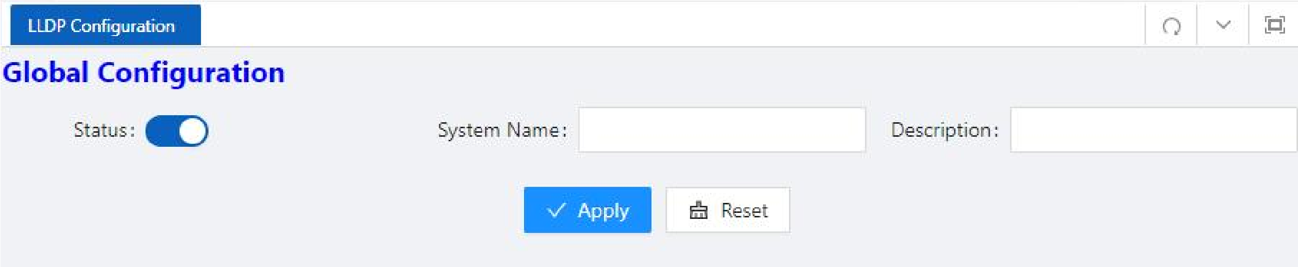


Table 4-1 LLDP global configuration items

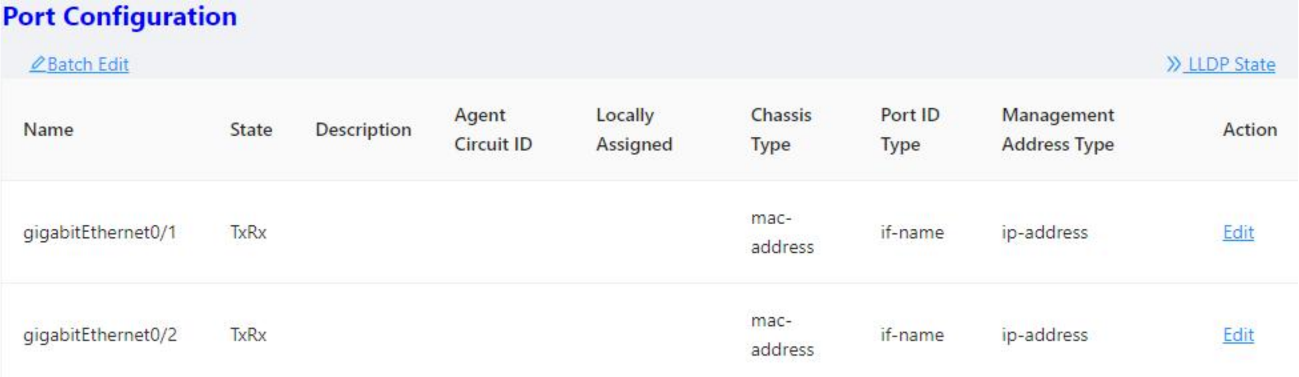
Item	Description
Status	Disable: global disable Enable: global enable
System Name	The name of the device, can be empty

Description	Description of the system, can be empty
Apply	Click to enable

LLDP Port Setting

1. The LLDP Port Configuration page appears after global configuration is enabled, as shown in Figure 4-2.

Figure 4-2 LLDP port configuration status



Port Configuration

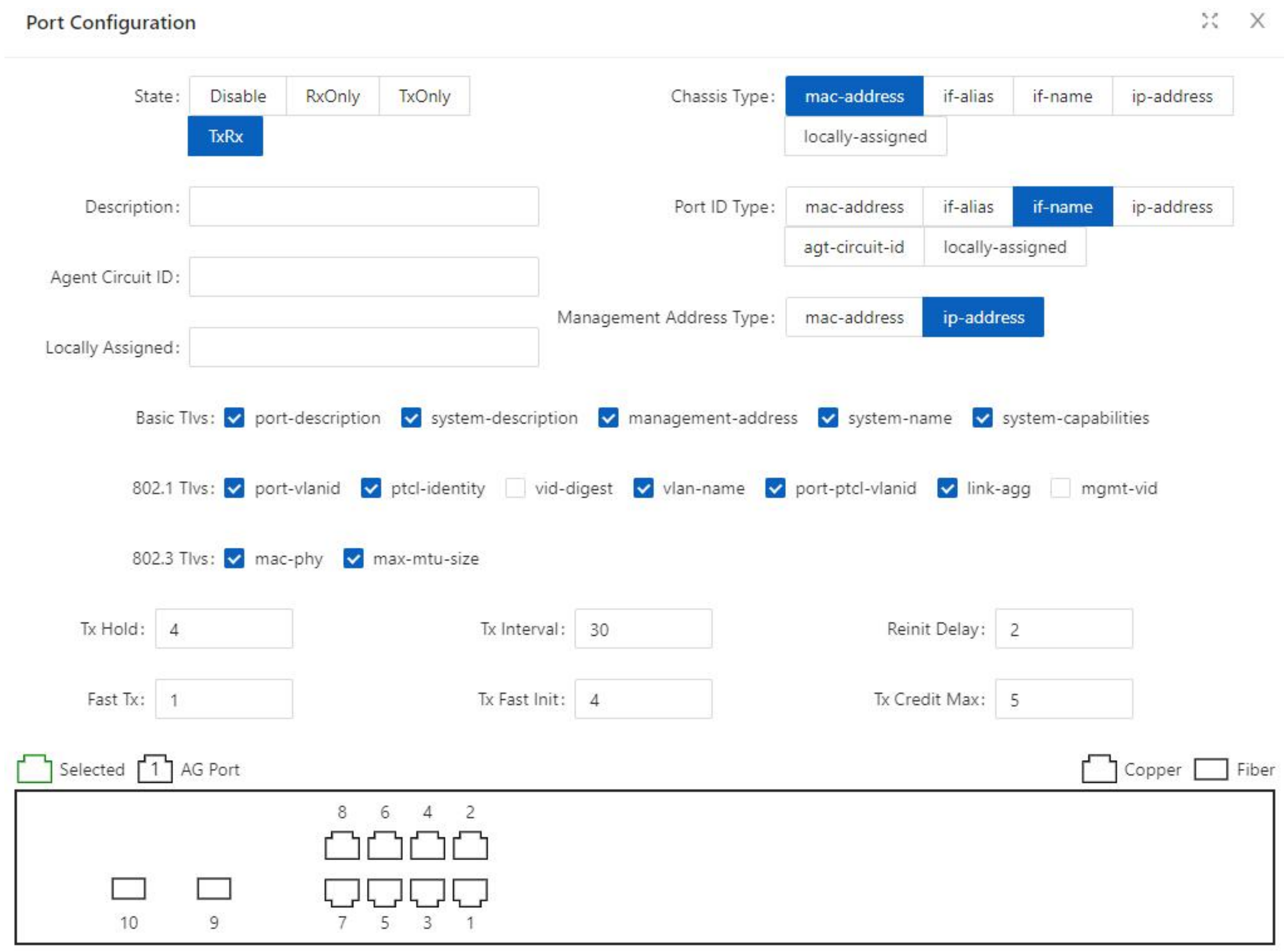
Batch Edit

LLDP State

Name	State	Description	Agent Circuit ID	Locally Assigned	Chassis Type	Port ID Type	Management Address Type	Action
gigabitEthernet0/1	TxRx				mac-address	if-name	ip-address	Edit
gigabitEthernet0/2	TxRx				mac-address	if-name	ip-address	Edit

2. Click **Batch Edit** button below Port Configuration or **Edit** button correspond of the port to enter the page for configuring ports, as shown in Figure 4-3. Table 4-2 describes the configuration items of configuring ports.

Figure 4-3 LLDP port status



Port Configuration

State: Disable | RxOnly | TxOnly | [✓ TxRx]

Chassis Type: [✓ mac-address] | if-alias | if-name | ip-address | locally-assigned

Description:

Port ID Type: mac-address | if-alias | [✓ if-name] | ip-address | agt-circuit-id | locally-assigned

Agent Circuit ID:

Management Address Type: mac-address | [✓ ip-address]

Locally Assigned:

Basic Tlvs: ☑ port-description ☑ system-description ☑ management-address ☑ system-name ☑ system-capabilities

802.1 Tlvs: ☑ port-vlanid ☑ ptcl-identity □ vid-digest ☑ vlan-name ☑ port-ptcl-vlanid ☑ link-agg □ mgmt-vid

802.3 Tlvs: ☑ mac-phy ☑ max-mtu-size

Tx Hold: 4
Tx Interval: 30
Reinit Delay: 2

Fast Tx: 1
Tx Fast Init: 4
Tx Credit Max: 5

Table 4-2 LLDP port configuration items

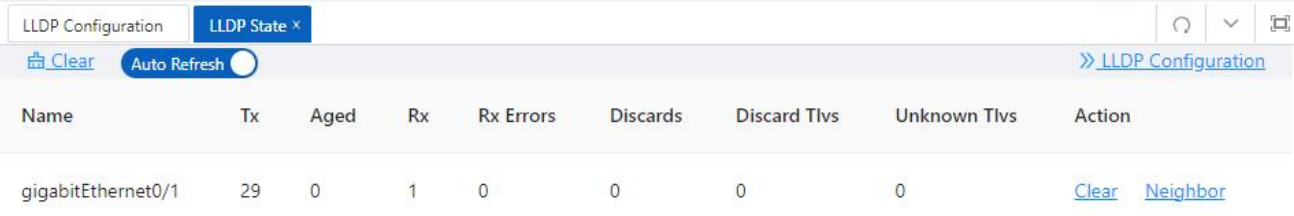
Item	Description
Description	Description of the currently configured LLDP port
Agent Circuit ID	Agent circuit identification. Can be used as a value for port-id-tlv
Locally Assigned	Locally Assigned
Admin Status	Disabled: No LLDP packets are sent/receive on the interface TxOnly: LLDP packets are sent on the interface RxOnly: LLDP packets are received on the interface TxRx: LLDP packets are sent/receive on the interface
Chassis 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 Locally-assigned: indicates 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 agt-circuit-id

	Locally-assigned: indicates locally-assigned value
Management Address Subtype	Mac-address: Device MAC address IP-address: Device IP address
Basic Tlvs	port-description: port descriptor system-description: system descriptor management-address: management address system-name: system name system-capabilities: system capabilities
802.1 Tlvs	port-vlanid: port's vlanid ptcl -identity: protocol id vid-digest: vid digest vlan-name: vlan name port-ptcl - vlanid: port protocol vlanid link- agg mgmt -vid: Link Aggregation Management vid
802.3 Tlvs	mac-phy: The rate and duplex status supported by the port, whether it supports port rate auto-negotiation, whether the auto-negotiation function is enabled, and the current rate and duplex status max - mtu -size: maximum mtu value
Tx hold	Transmission hold, the default value txFastInit is 4, used for packet TTL calculation; TTL= msgTxInterval * msgTxHold + 1
Tx interval	Transfer intervals, default is 30 s; admin can change this value to any value between5and 300.
Reinit delay	Indicates the amount of delay between when adminStatus becomes ' disabled' and when reinitialization is attempted. The default value of reinitDelay is 2 s.
Fast tx	Defines the time interval for the timer interval between two transfers within a fast transfer period (ie txFast is not zero). The default value for msgFastTx is 1; administrators can change this value to any value between 1 and 3600.
Tx fast init	This variable is used as the initial value of the txFast variable. This value determines the number of LLDPDUs transmitted during the fast transmission period.
Tx credit max	Configure the maximum value of txCredit. The default value is 5. Administrators can change this value to any value in the range 1 to 10.

View LLDP State

In the current page, click the **LLDP State** button on the right to enter the LLDP State page, as shown in Figure 4-4, and the specific parameters are described as described in Table 4-3.

Figure 4-4 LLDP port statistics



Name	Tx	Aged	Rx	Rx Errors	Discards	Discard Tlvs	Unknown Tlvs	Action
gigabitEthernet0/1	29	0	1	0	0	0	0	Clear Neighbor

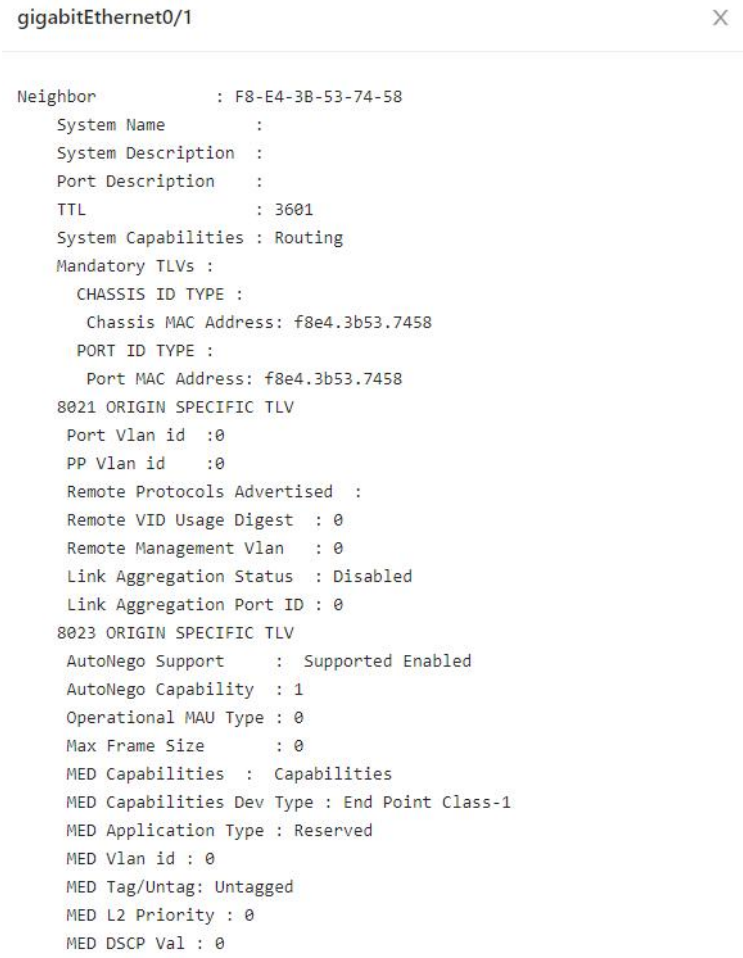
Table 4-3 LLDP port configuration items

Item	Description
Name	Description of the currently configured LLDP port
Tx	The number of packets sent on the interface
Aged	The number of packets aged on the interface
Rx	The number of packets received on the interface
Rx Errors	The number of error packets received on the interface
Discards	The number of packets discarded on the interface
Discard Tlvs	The number of Tlv packets of discarded on the interface
Unknown Tlvs	The number of unknown Tlvs packets on the interface
CLEAR	Clear counters on the current interface

View Neighbor Information

On the current LLDP State page, click the **Neighbor** button of the corresponding port to enter the Neighbor Information view interface.

Figure 4-5 LLDP neighbor information



gigabitEthernet0/1

```
Neighbor            : F8-E4-3B-53-74-58
    System Name         :
    System Description  :
    Port Description    :
    TTL                 : 3601
    System Capabilities : Routing
    Mandatory TLVs :
      CHASSIS ID TYPE :
       Chassis MAC Address: f8e4.3b53.7458
      PORT ID TYPE :
       Port MAC Address: f8e4.3b53.7458
    8021 ORIGIN SPECIFIC TLV
     Port Vlan id   :0
     PP Vlan id     :0
     Remote Protocols Advertised   :
     Remote VID Usage Digest   : 0
     Remote Management Vlan    : 0
     Link Aggregation Status   : Disabled
     Link Aggregation Port ID : 0
    8023 ORIGIN SPECIFIC TLV
     AutoNego Support      :  Supported Enabled
     AutoNego Capability   : 1
     Operational MAU Type : 0
     Max Frame Size        : 0
     MED Capabilities   :  Capabilities
     MED Capabilities Dev Type : End Point Class-1
     MED Application Type : Reserved
     MED Vlan id : 0
     MED Tag/Untag: Untagged
     MED L2 Priority : 0
     MED DSCP Val : 0
```

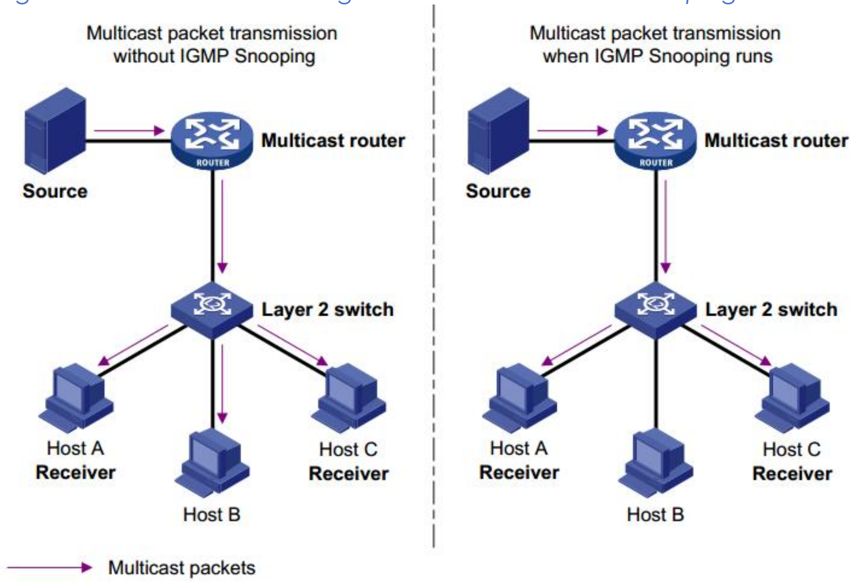
4.2 IGMP Snooping

Internet Group Management Protocol Snooping (IGMP snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

4.2.1 Principle of IGMP Snooping

By analyzing received IGMP messages, a Layer 2 device running IGMP snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings. As shown in Figure 4-6, when IGMP snooping is not running on the switch, multicast packets are flooded to all devices at Layer 2. However, when IGMP snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2.

Figure 4-6 Multicast forwarding before and after IGMP snooping runs



4.2.2 Configure the IGMP Snooping

4.2.2.1 Global Configuration

Select **Advance** > **Layer2** > **IGMP Snooping Configuration** in the navigation area to enter the Global Configuration page, as shown in Figure 4-7. Table 4-4 describes the IGMP snooping configuration items.

Figure 4-7 IGMP global configuration

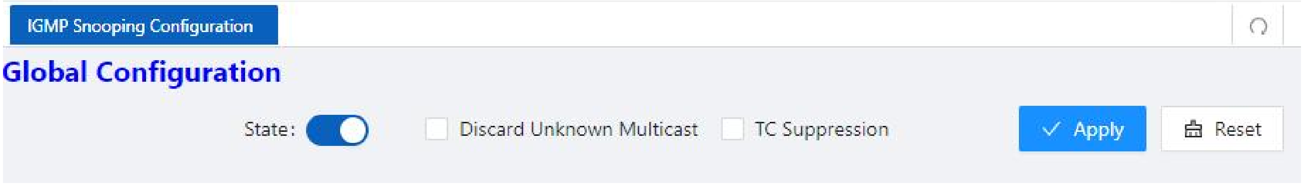


Table 4-4 IGMP snooping summary items

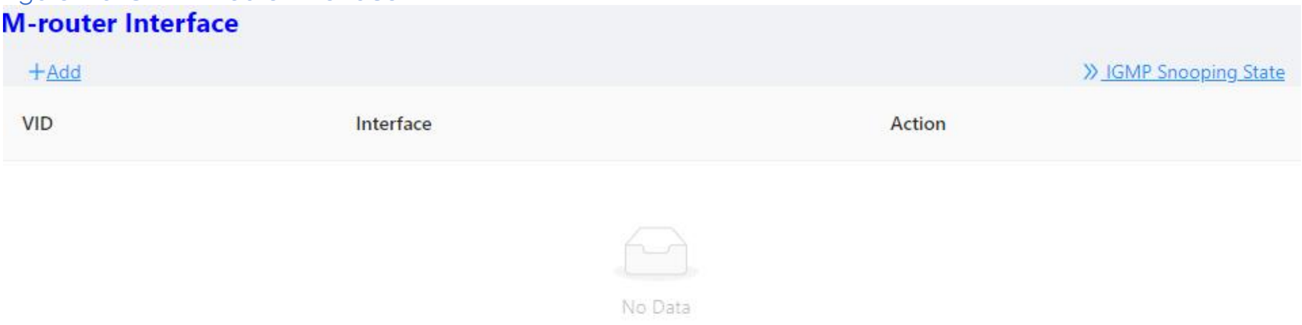
Item		Description
Global Configuration	State	Disabled: global disable Enabled: global enable
	Discard Unknown Multicast	If this option is enabled, unknown multicast traffic will be dropped by switch.

	TC Suppression	If this option is enabled, topology change event will be ignored by switch

4.2.2.2 IGMP Mrouter Interface Configuration

1. Select **Advance** > **Layer2** > **IGMP Snooping Configuration** in the navigation area to enter the IGMP M-router Interface section as shown in Figure 4-8. Table 4-5 describes the IGMP M-router Interface configuration items.

Figure 4-8 IGMP M-router interface



M-router Interface

+Add

» IGMP Snooping State

VID	Interface	Action

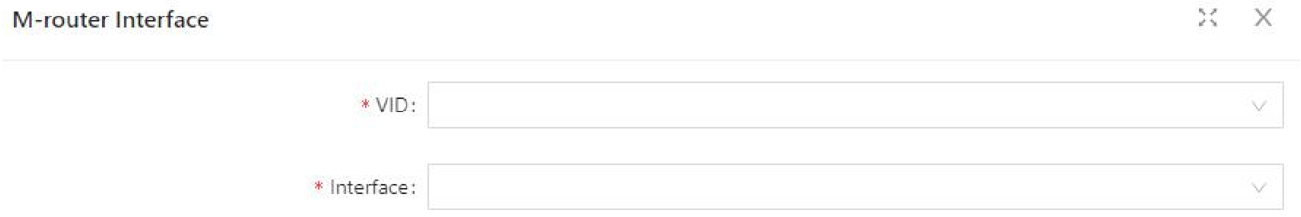
No Data

Table 4-5 IGMP M-router interface items

Item		Description
IGMP M-router Interface	VID	VLAN ID
	Interface	Interface Name.
	Delete	Click to delete this entry.

2. Click the **+Add** button to create an IGMP M-router Interface, as shown in Figure 4-9. Configure VID and Interface,then click **OK**.

Figure 4-9 Creating IGMP M-router interface



M-router Interface

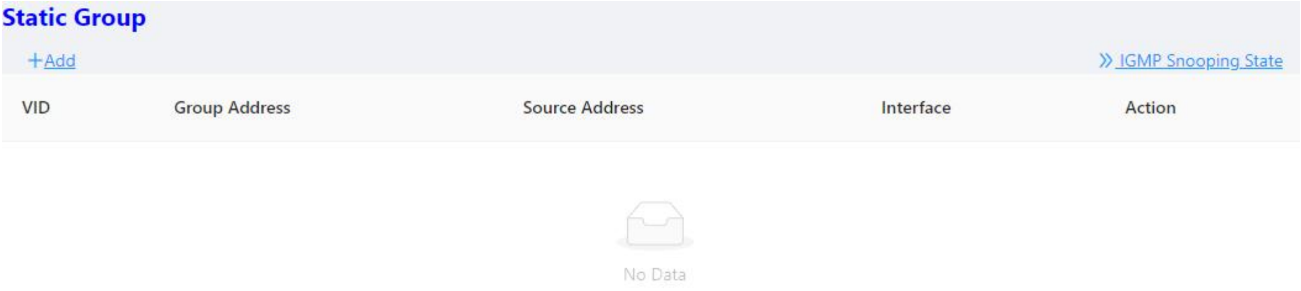
* VID:

* Interface:

4.2.2.3 IGMP Static Group Configuration

1. Select **Advance** > **Layer2** > **IGMP Snooping Configuration** in the navigation area to enter the IGMP Static Group section as shown in Figure 4-10. Table 4-6 describes the IGMP static group configuration items.

Figure 4-10 IGMP static group


Static Group

+Add

» IGMP Snooping State

VID	Group Address	Source Address	Interface	Action

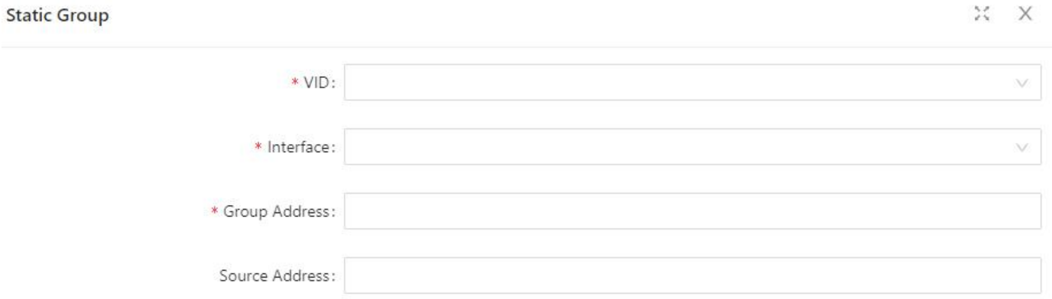
No Data

Table 4-6 IGMP static group items

Item		Description
IGMP Static Group	VID	VLAN ID
	Group Address	Group IP address
	Source Address	Source IP address
	Interface	Interface name.
	Delete	Click to delete this entry.

2. Click the **+Add** button to create an IGMP static group, as shown in Figure 4-11. Configure VID, Group Address, Source Address and Interface, then click **OK**.

Figure 4-11 Creating IGMP static group


Static Group

* VID:

* Interface:

* Group Address:

Source Address:

4.3 MAC Management

4.3.1 Overview

A device maintains a MAC address table for frame forwarding. Each entry in this table indicates the MAC address of a connected device, to which interface this device is connected and to which VLAN the interface belongs. A MAC address table consists of two types of entries: static and dynamic. Static entries are manually configured and never age out. Dynamic entries can be manually configured or dynamically learned and will age out.

Your device learns a MAC address after it receives a frame from a port, port A for example, as it executes the following steps.

1. Checks the frame for the source MAC address (MAC-SOURCE for example).
2. Looks up the MAC address table for an entry corresponding to the MAC address and do the following:
    - If an entry is found for the MAC address, updates the entry.

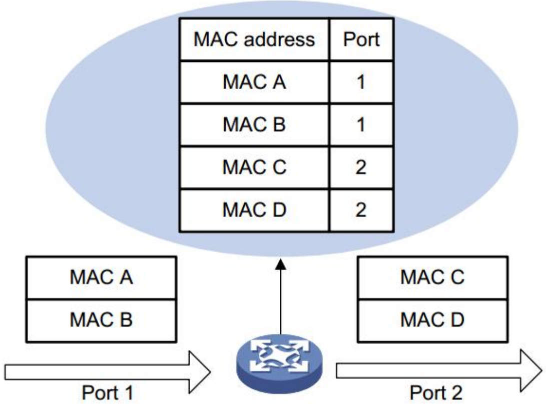
- If no entry containing the MAC address is found, adds an entry that contains the MAC address and the receiving port (port A) to the MAC address table.

3. After the MAC address (MAC-SOURCE) is learned, if the device receives a frame destined for MAC-SOURCE, the device looks up the MAC address table and then forwards the frame from port A.

When forwarding a frame, the device adopts the following forwarding modes based on the MAC address table:

- Unicast mode: If an entry matching the destination MAC address exists, the device forwards the frame directly from the sending port recorded in the entry.
- Broadcast mode: If the device receives a frame with the destination address being all FS, or no entry matches the destination MAC address, the device broadcasts the frame to all the ports except the receiving port.

Figure 4-12 MAC address table of the device



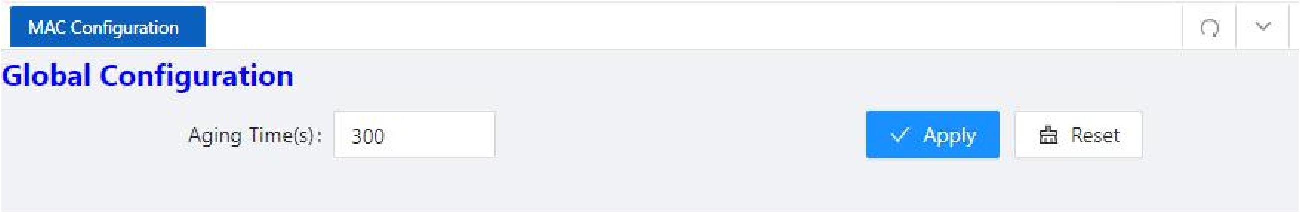
4.3.2 Configuring MAC Addresses

MAC addresses configuration includes the configuring and displaying of static MAC address, Filter MAC Address, and the setting of MAC address entry aging time.

Global Configuration

1. Select **Advance** > **Layer2** > **MAC Configuration** in the navigation area to enter the MAC Global Configuration page shown in Figure 4-13. Table 4-7 describes the MAC configuration items.

Figure 4-13 MAC global configuration



Global Configuration

Aging Time(s): 300

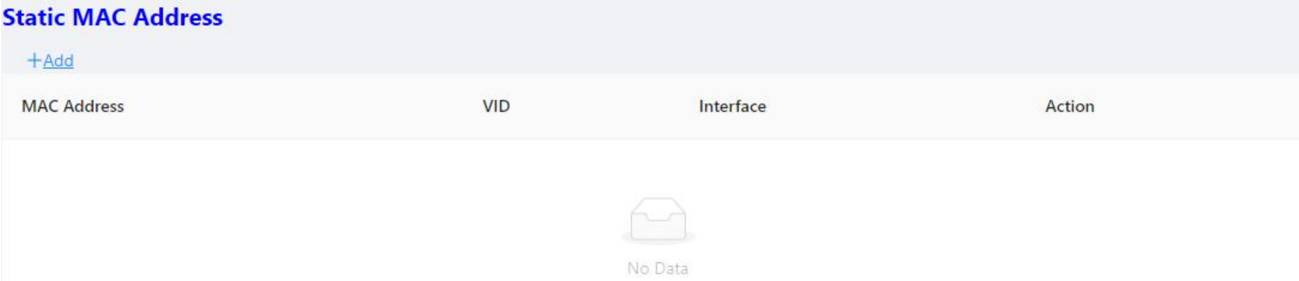
Table 4-7 MAC global configuration items

Item		Description
Global configuration	Aging time	Set the aging time for the MAC address, the default value is 300 seconds.
	Apply	Click to enable

Configuring Static MAC Address

1. Select **Advance** > **Layer2** > **MAC Configuration** in the navigation area to enter the Static MAC Address Configuration page shown in Figure 4-14.

Figure 4-14 MAC static address page



2. Click **+Add** to enter the page for creating static MAC address, as shown in Figure 4-15. Table 4-8 shows the detailed configuration for creating a static MAC address.

3. Type in **MAC address** box, for example ‘00eb.fc00.8877’, select the **VID** in the VLAN drop down list, select the **Interface** in the Interface drop list.

4. Click **OK** to end the operation.

Figure 4-15 Creating static MAC address

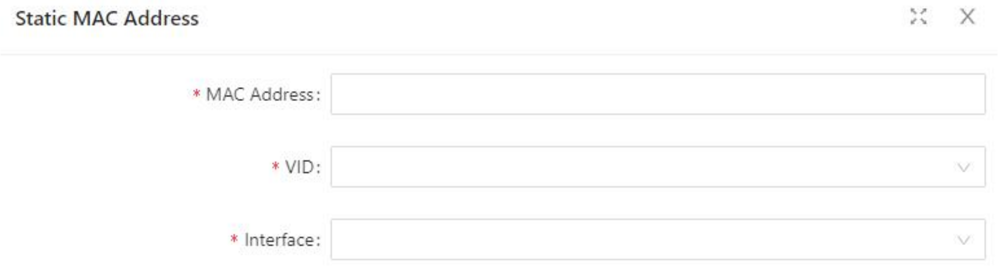


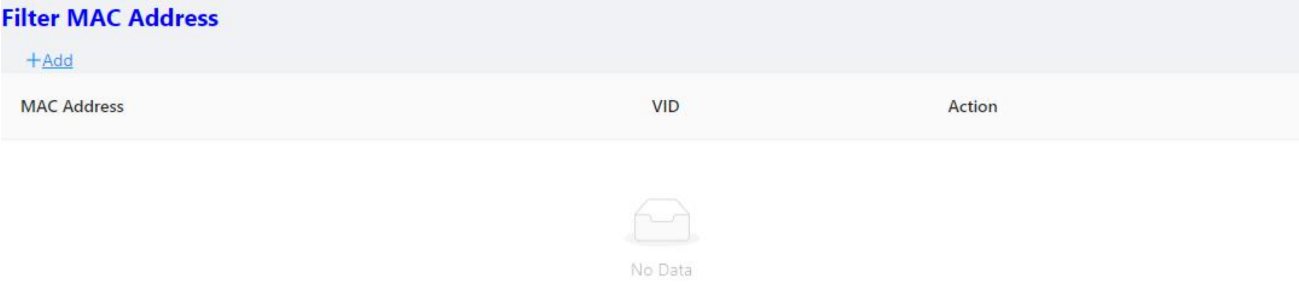
Table 4-8 Static MAC address items

Item		Description
Static Mac Address	MAC Address	Set the MAC address to be added.
	VID	Sets the ID of the VLAN to which the MAC address belongs.
	Interface	Sets the port to which the MAC address belongs.

Configuring Filter MAC Address

1. Select **Advance** > **Layer2** > **MAC Configuration** from the navigation area. The system automatically displays the Filter MAC Address page, as shown in Figure 4-16.

Figure 4-16 MAC static address page



Filter MAC Address

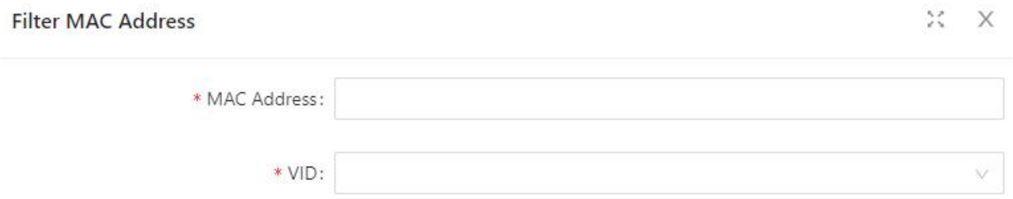
+Add

MAC Address	VID	Action

No Data

2. Click **+Add** to enter the page for creating filter MAC address, as shown in Figure 4-17. Table 4-9 shows the detailed configuration for creating a filter MAC address.
3. Type in **MAC address**, for example '00eb.fc00.8877', select the **VID** in the VLAN drop down list.
4. Click **Apply** to end the operation.

Figure 4-17 Creating filter MAC address



Filter MAC Address

* MAC Address:

* VID:

Table 4-9 Filter MAC address items

Item		Description
Static Mac Address	MAC Address	Set the MAC address to be filtered.
	VID	Sets the ID of the VLAN to which the MAC address belongs.

4.4 DHCP Snooping

4.4.1 Overview

DHCP (Dynamic Host Configuration Protocol) snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. When DHCP snooping is enabled on a VLAN, the system examines DHCP messages sent from untrusted hosts associated with the VLAN and extracts their IP addresses and lease information. This information is used to build and maintain the DHCP snooping database.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

Trusted Sources

The DHCP snooping feature determines whether traffic sources are trusted or untrusted. DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server. The default trust state of all interfaces is untrusted.

DHCP Snooping Limit Rate

Configure the number of DHCP packets per second that an interface can receive, to reduce or eliminate the impact of DHCP packet attack from this interface.

MAC Address Verification

With DHCP snooping MAC address verification enabled, DHCP snooping verifies that the source MAC address and the client hardware address match in DHCP packets that are received on untrusted ports. The source MAC address is a Layer 2 field associated with the packet, and the client hardware address is a Layer 3 field in the DHCP packet.

Option-82 Insertion

DHCP Option82 option is also called DHCP relay agent information option, one of many DHCP options. The Option82 option is a DHCP option proposed to enhance the security of the DHCP server and improve the IP address allocation strategy. The addition and stripping of options are implemented by the relay component.

DHCP Database

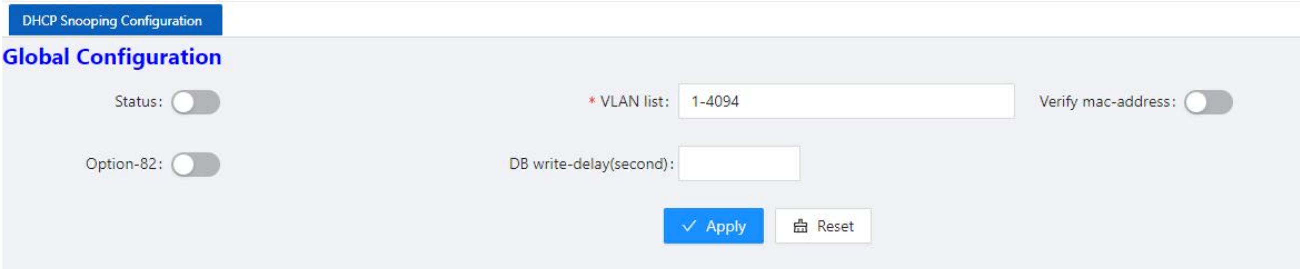
The DHCP snooping feature dynamically builds and maintains the database using information extracted from intercepted DHCP messages. The database contains an entry for each untrusted host with a leased IP address if the host is associated with a VLAN that has DHCP snooping enabled. The database does not contain entries for hosts connected through trusted interfaces. When the IP verify source function is enabled on the interface, database entries act as valid users on the interface.

4.4.2 Configuring DHCP Snooping

Configuring DHCP Snooping Globally

1. Select **Advance** > **Layer2** > **DHCP Snooping** from the navigation tree to enter the DHCP Snooping Configuration page, as shown in Figure 4-18. Table 4-10 describes the configuration items of configuring DHCP globally.

Figure 4-18 DHCP snooping global configuration



DHCP Snooping Configuration

Global Configuration

Status: ○

* VLAN list: 1-4094

Verify mac-address: ○

Option-82: ○

DB write-delay(second):

Table 4-10 The description of DHCP snooping global configuration

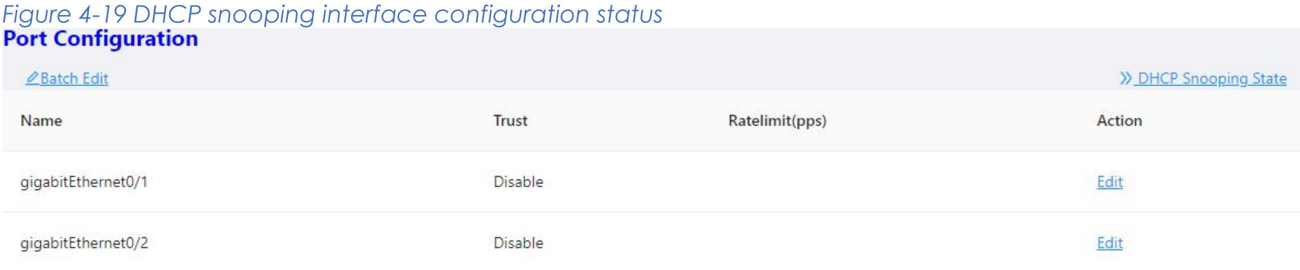
Item	Description
Status	Enable/Disable the DHCP Snooping globally

VLAN	Enable/Disable the DHCP Snooping on the VLANs
Verify mac-address	Verify the source MAC address and the client hardware address is matched in DHCP packets
option-82	Enable/Disable option-82 insertion
DB write-delay(s)	Configure the interval time database writing to flash

Configuring DHCP Snooping Ports

1. Select **Advance** > **Layer2** > **DHCP Snooping** from the navigation tree, as shown in Figure 4-19.

Figure 4-19 DHCP snooping interface configuration status



Port Configuration

Batch Edit

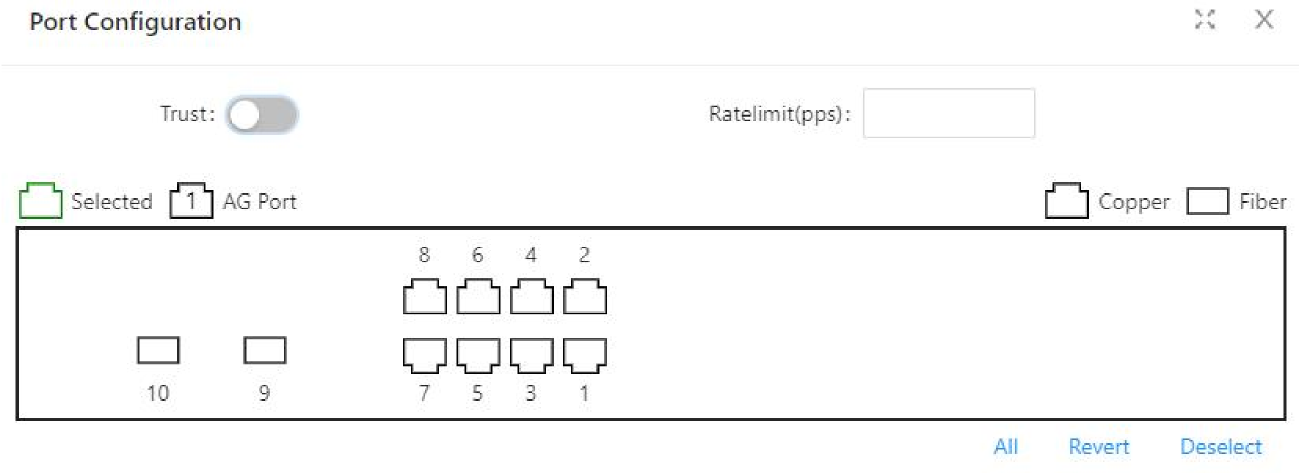
DHCP Snooping State

Name	Trust	Ratelimit(pps)	Action
gigabitEthernet0/1	Disable		Edit
gigabitEthernet0/2	Disable		Edit

2. Click **Batch Edit** button below Port Configuration or **Edit** button correspond of the port to enter the page for configuring ports.

3. Check the ports to be configured, click **Edit** to enter the Interface Configuration page as shown in Figure 4-20. Table 4-11 describes the configuration items of DHCP snooping interface configuration.

Figure 4-20 DHCP snooping global configuration



Port Configuration

Trust: ○

Ratelimit(pps):

Table 4-11 The description of DHCP snooping interface configuration

Item	Description
Trust	determines whether traffic sources are trusted or untrusted
Ratelimit(pps)	Configure the number of DHCP packets per second that an interface can receive

NOTE:

✦ Due to hardware limitations, for DHCP rate limit, when the limit value is not 0, the software rate limit is used, and when the limit value is 0, the hardware rate limit is used. Software rate limit will consume CPU resources.

View DHCP Snooping State

1. Click the **DHCP Snooping state** button in the current page to enter the DHCP Snooping State page, as shown in Figure 4-21. Table 4-12 describes the configuration items of configuring DHCP snooping database.

Figure 4-21 DHCP snooping database

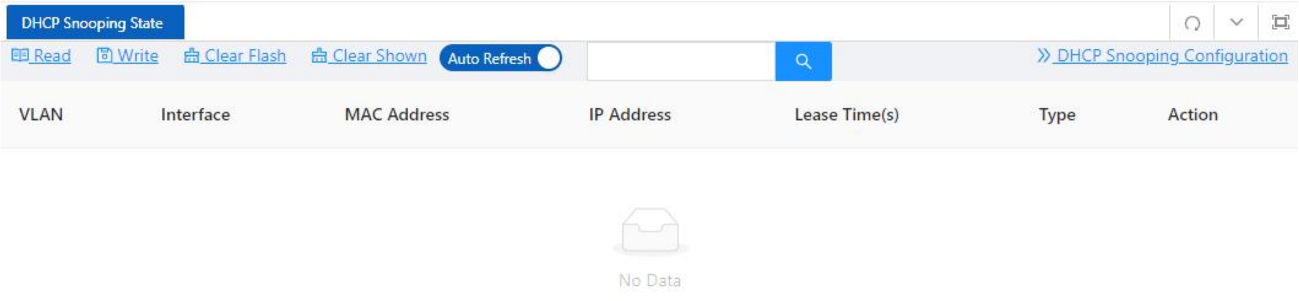


Table 4-12 The description of DHCP snooping database

Item	Description
Search	Search database entries by fuzzy match the input strings
WRITE	Write database entries to flash
READ	Read database entries from flash
CLEAR	Clear database entries, you can narrow the scope by selecting keywords

4.5 QinQ

4.5.1 Overview

Introduction to QinQ

QinQ stands for 802.1Q in 802.1Q. QinQ is a flexible, easy-to-implement Layer 2 VPN technology based on IEEE 802.1Q. QinQ enables the edge device on a service provider network to insert an outer VLAN tag in the Ethernet frames from customer networks, so that the Ethernet frames travel across the service provider network (public network) with double VLAN tags. QinQ enables a service provider to use a single SVLAN to serve customers who have multiple CVLANs.

Background and Benefits

The IEEE 802.1Q VLAN tag uses 12 bits for VLAN IDs. A device supports a maximum of 4094 VLANs. This is far from enough for isolating users in actual networks, especially in metropolitan area networks (MANs).

By tagging tagged frames, QinQ expands the available VLAN space from 4094 to 4094 × 4094.

QinQ delivers the following benefits:

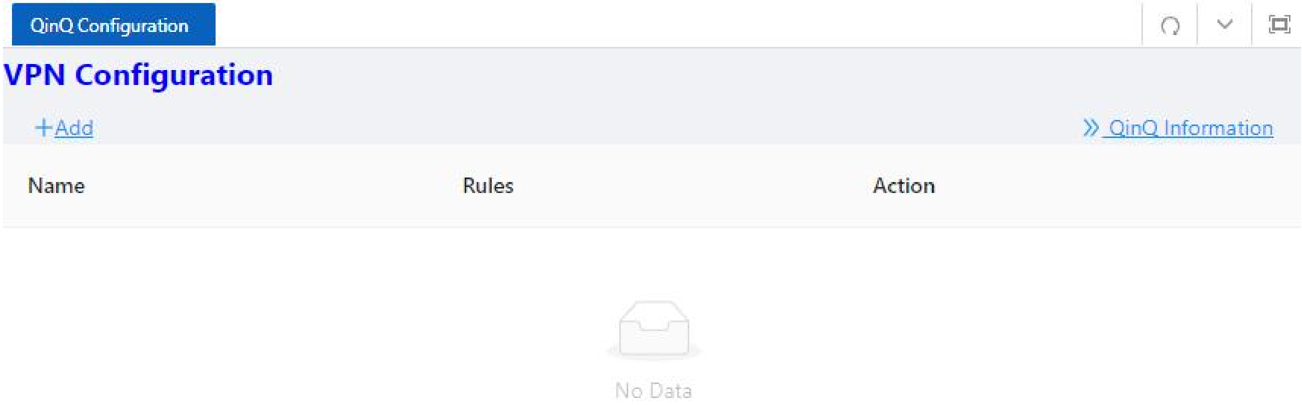
- Releases the stress on the SVLAN resource.
- Enables customers to plan their CVLANs without conflicting with SVLANs.
- Provides an easy-to-implement Layer 2 VPN solution for small-sized MANs or intranets.
- Allows the customers to keep their VLAN assignment schemes unchanged when the service provider upgrades the service provider network.

4.5.2 QinQ Configuration

VPN Configuration

1. Select **Advance** > **Layer2** > **QinQ Configuration** in the navigation area. The system automatically enters the page as shown in Figure 4-22.

Figure 4-22 VPN configuration summary



2. Click **+Add** button below VPN Configuration to enter the VPN Rule Creating page, as shown in Figure 4-23, Table 4-13 describes the items of configuring a QinQ rule.

Figure 4-23 VPN configuration

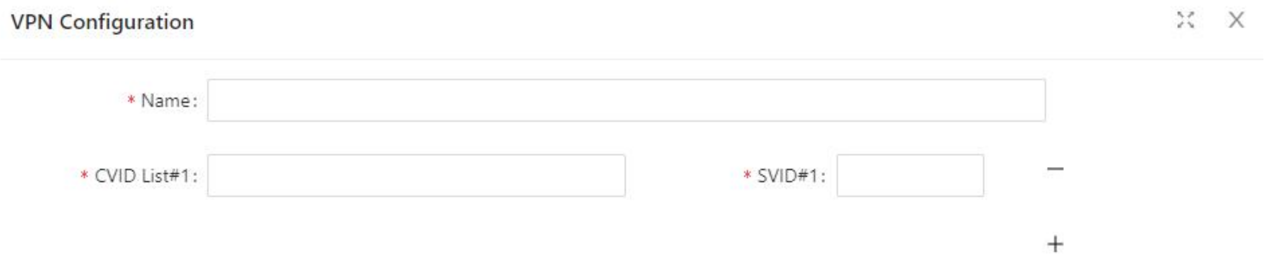


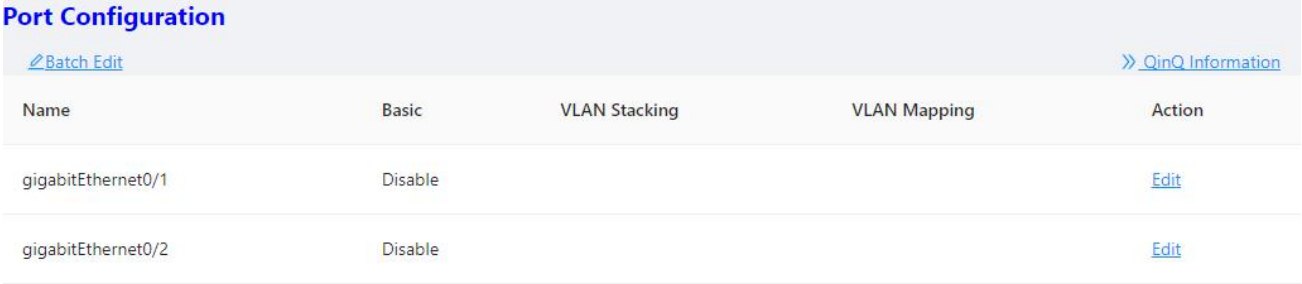
Table 4-13 VPN configuration description

Item	Description
Name	The name of the VLAN VPN Rule
CVID	The ID of the customer VLAN
SVID	The ID of the service provider VLAN

Port Configuration

1. Select **Advance** > **Layer2** > **QinQ Configuration** in the navigation area. The system automatically enters the page as shown in Figure 4-24.

Figure 4-24 Port configuration summary



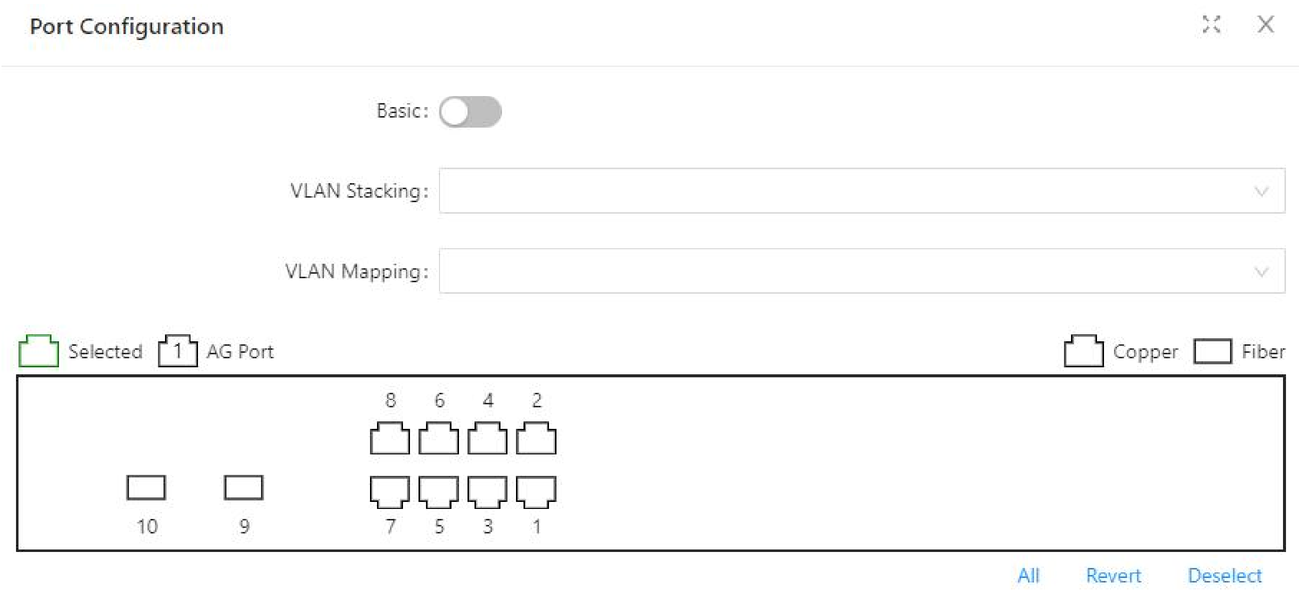
Port Configuration

Batch Edit   » QinQ Information

Name	Basic	VLAN Stacking	VLAN Mapping	Action
gigabitEthernet0/1	Disable			Edit
gigabitEthernet0/2	Disable			Edit

2. Click **Batch Edit** button below Port Configuration or **Edit** button correspond of the port to enter the QinQ Port Configuration page, as shown in Figure 4-25, Table 4-14 describes the items of configuring port.

Figure 4-25 Port configuration



Port Configuration

Basic:

VLAN Stacking:

VLAN Mapping:

Table 4-14 The description of configuring a QinQ rule

Item	Description
Basic	Enable VLAN mapping mode
VLAN Stacking	Multi-layer tag mode
VLAN Mapping	tag replacement mode

4.6 ACL

4.6.1 Overview

An access control list (ACL) is a set of rules (or permit or deny statements) for identifying traffic based on criteria such as source IP address, destination IP address, and port number. ACLs are essentially used for packet filtering. A packet filter drops packets that match a deny rule and permits packets that match a permit rule. ACLs are also widely used by many modules, for example, QoS and IP routing, for traffic identification.

4.6.2 Configuring ACLs

NOTE:

✦ A maximum of 128 rules can be configured under a single ACL-ID; due to hardware resource limitations, please refer to the specific product specification document for the maximum number of application rules supported by a single device.

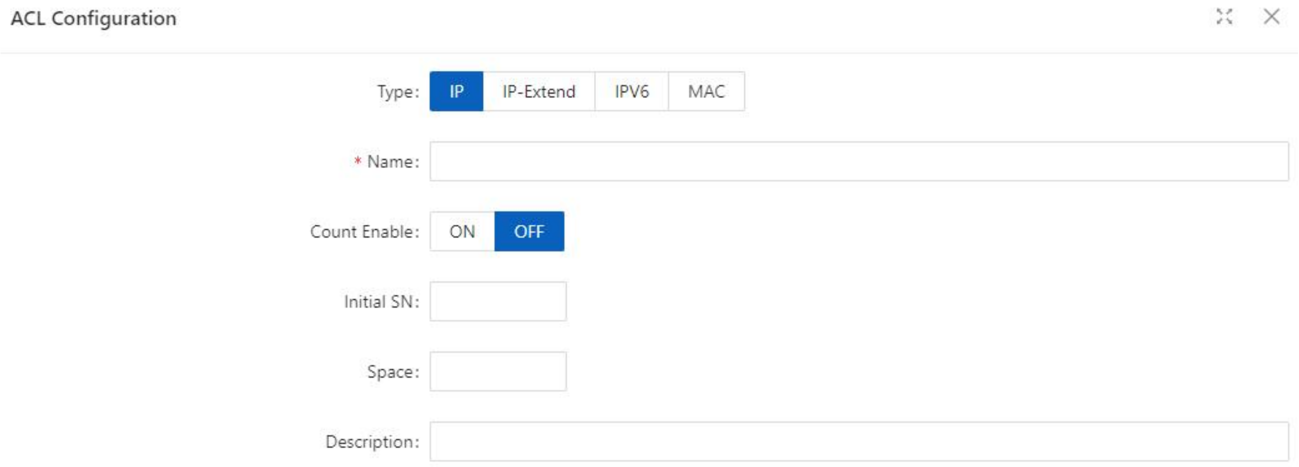
✦When an ACL has been applied to a port, if you need to add and delete rules, you must first unapply them from the port.

Configuring a Rule for an IP ACL

1. Select **Advance** > **Security** > **ACL Configuration** in the navigation area.

2. Click the **+Add ACL** button to enter the Rule Configuration page and choose the ACL type IP for a basic ACL as shown in Figure 4-26. Table 4-15 describes the configuration items of configuring an IP ACL.

Figure 4-26. Configuring a basic IP ACL



ACL Configuration

Type: IP | IP-Extend | IPV6 | MAC (IP selected)

* Name:

Count Enable: ON | OFF (OFF selected)

Initial SN:

Space:

Description:

Table 4-15 The description of the basic IP ACL

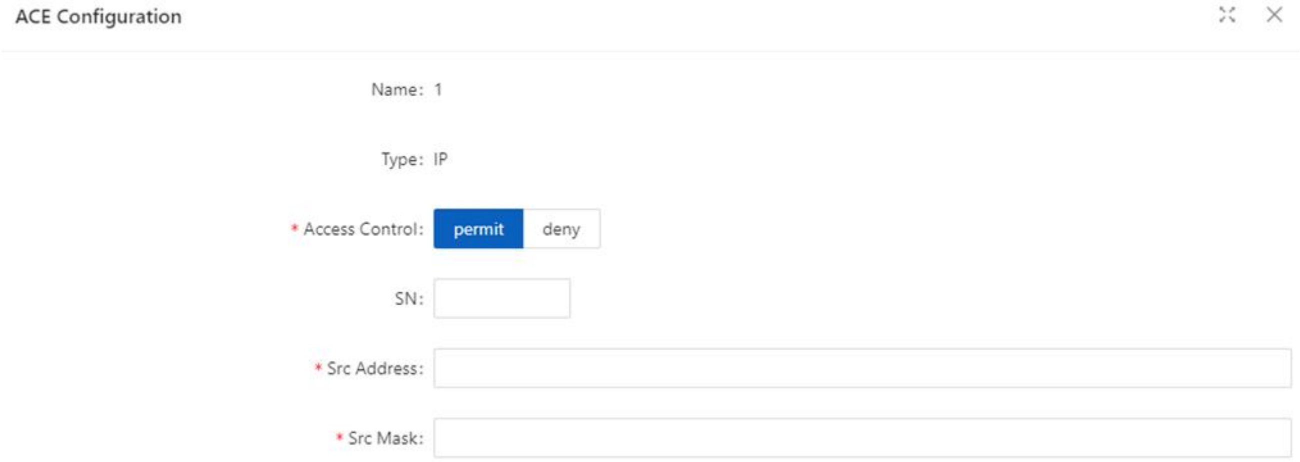
Item		Description
ACL Type	IP	Standard IP ACL can match the source IP field in IPv4 packets
	IP-Extend	the protocol number, source IP address, destination IP address, Layer 4 port number, etc. of IPv4 packets
	IPV6	IPv6 ACL can match IPv6 packet source IP address, destination IP address, protocol number, etc
	MAC	MAC ACL, which can match destination MAC address, source MAC address, Etype and other fields
Name		Standard IP valid number range: <1-99> | <1300-1999> Extended IP valid number range: <100-199> | <2000-2699>

	MAC ACL valid number range: <200-699> IPv6 ACL only supports string naming. All ACLs support string naming. The string length range is <1-64>
Count Enable	Enable the counting function. When a packet hits the ACL, the count value is increased by 1
Initial SN	Starting value of rule entry sequence number, default value: 10, range <1-2147483647>
Space	Increment the serial number, default value: 10, range <1-2147483647>
Description	Define the ACL description information

3. Configure a rule for an IP ACL, and click **OK**.

4. Select IP rule in the box below ACE Configuration and click **+Add ACE** button to enter ACE Configuration page as shown in Figure 4-27. Table 4-16 describes the configuration items of configuring an IP ACE configuration.

Figure 4-27 IP type ACE configuration interface


ACE Configuration

Name: 1

Type: IP

* Access Control: permit deny

SN:

* Src Address:

* Src Mask:

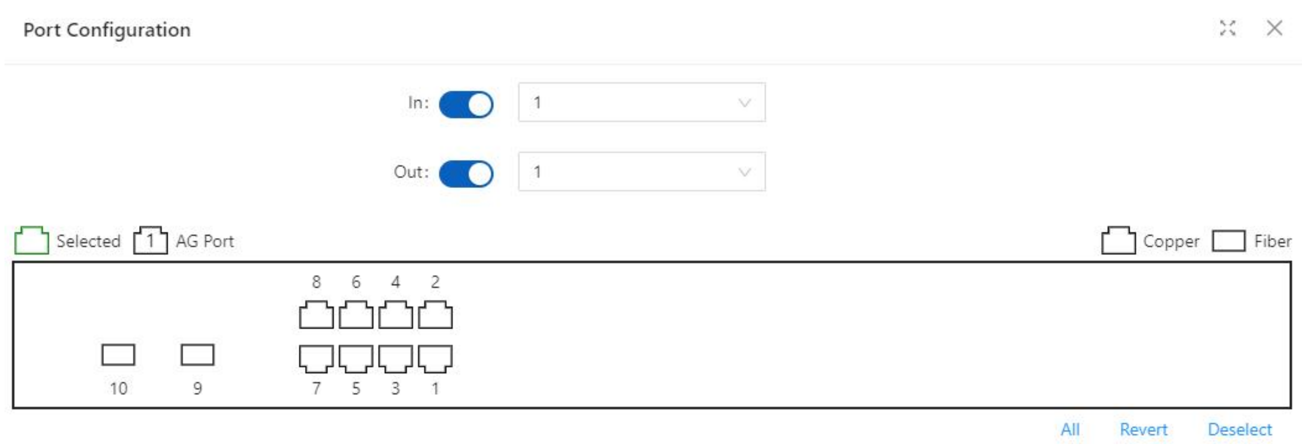
Table 4-16 The description of the IP type ACL

Item		Description
Access Control	permit	Release the packets that match this rule
	deny	Discard packets matching this rule
SN		Rule entry sequence number
Src Address		Source IP address, such as 192.168.64.1
Src Mask		The IP mask is inverted. If it matches the first 24 digits of the IP address, the mask is 255.255.255.0. Here it needs to be configured as 00.00.00.255

5. Configure ACE and click **OK**.

4. Click **Batch Edit** below Port Configuration to enter the ACL Port Configuration page, select the ACL rules of the corresponding port, as shown in Figure 4-28, and click **OK**.

Figure 4-28 Apply the ACL rule to the port



Port Configuration

In: 1

Out: 1

Configuring a Rule for an IP-Extend ACL

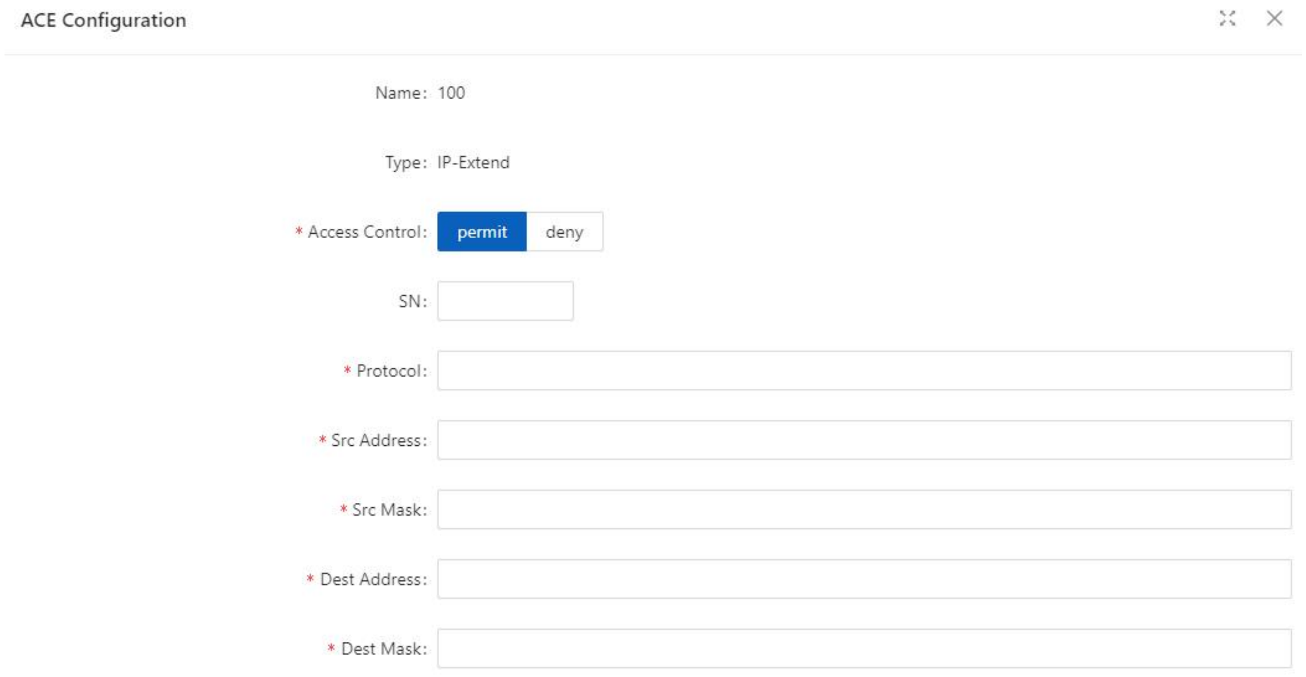
1. Select **Advance** > **Security** > **ACL Configuration** in the navigation area.

2. Click the **+Add ACL** button to enter the Rule Configuration page and choose the ACL type **IP-Extend** for a basic ACL as shown in Figure 4-26.

3. Configure a rule for an IP ACL, and click **OK**.

4. Select ACK rules in the box below ACE Configuration and click **+Add ACE** button to enter ACE Configuration page as shown in Figure 4-29. Table 4-17 describes the configuration items of configuring an IP ACE configuration.

Figure 4-29 IP-Extend type ACE configuration interface



ACE Configuration

Name: 100

Type: IP-Extend

* Access Control: permit deny

SN:

* Protocol:

* Src Address:

* Src Mask:

* Dest Address:

* Dest Mask:

Table 4-17 The description of the IP-Extend ACL

Item		Description
Access Control	permit	Release the packets that match this rule
	deny	Discard packets matching this rule

SN	Rule entry sequence number
Protocol	Supports common protocol message options, including tcp, udp, vrrp, igmp, gre, ipcomp, ospf, pim, rsvp, etc. Supports all IP v4 packets IPv4 messages of customized protocol
Src Address	Source IP address, such as 192.168.64.1
Src Mask	The IP mask is inverted. If it matches the first 24 digits of the IP address, the mask is 255.255.255.0. Here it needs to be configured as 00.00.00.255
Dest Address	Destination IP address, such as 192.168.64.100
Dest Mask	homology mask

5. Configure ACE and click **OK**.

6. Click **Batch Edit** below Port Configuration to enter the ACL Port Configuration page, select the ACL rules of the corresponding port, and click **OK**.

Configuring a Rule for an IPV6 ACL

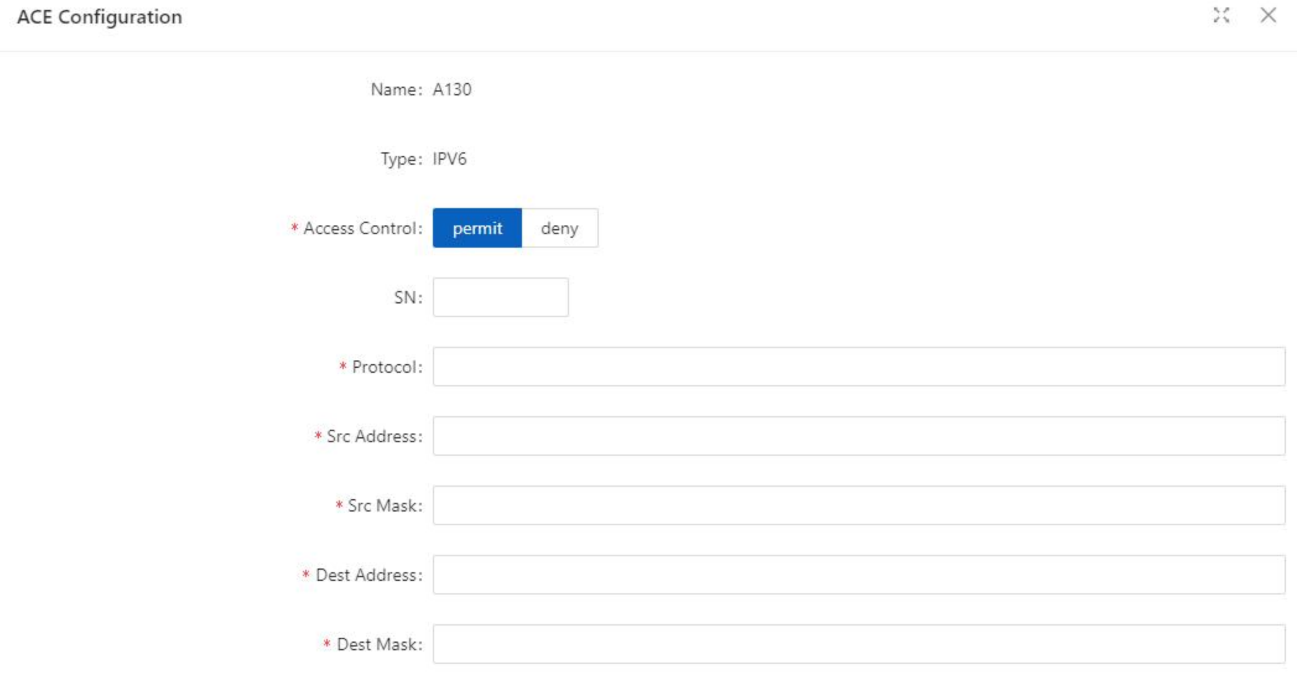
1. Select **Advance** > **Security** > **ACL Configuration** in the navigation area.

2. Click the **+Add ACL** button to enter the rule configuration page and choose the ACL type **IPV6** for a basic ACL as shown in Figure 4-26.

3. Configure a rule for an IP ACL, and click **OK**.

4. Select ACL rules in the box below ACE Configuration and click **+Add ACE** button to enter ACE Configuration page as shown in Figure 4-30. Table 4-18 describes the configuration items of configuring an IP ACE configuration.

Figure 4-30 IPV6 type ACE configuration interface



ACE Configuration

Name: A130

Type: IPV6

* Access Control: permit deny

SN:

* Protocol:

* Src Address:

* Src Mask:

* Dest Address:

* Dest Mask:

Table 4-18 The description of the IPV6 ACL

Item		Description
Access Control	permit	Release the packets that match this rule
	deny	Discard packets matching this rule
SN		Rule entry sequence number
Protocol		Supports common protocol message options , including tcp , udp , icmp , etc. Supports all IP v 6 packets Support IPv6 messages of customized protocol
Src Address		Source MAC address, such as 00.d 0.f 8.22.33.40
Src Mask		The MAC address mask is inverted. If it matches the first 24 digits of the MAC address , the mask is ffff.ff00.0000. Here it needs to be configured as 0000.00 ff.ffff
Dest Address		Destination MAC address, such as 00.d 0.f 8.22.33.41
Dest Mask		homology mask

5. Configure ACE and click **OK**.

6. Click **Batch Edit** below Port Configuration to enter the ACL Port Configuration page, select the ACL rules of the corresponding port, and click **OK**.

Configuring a Rule for an MAC ACL

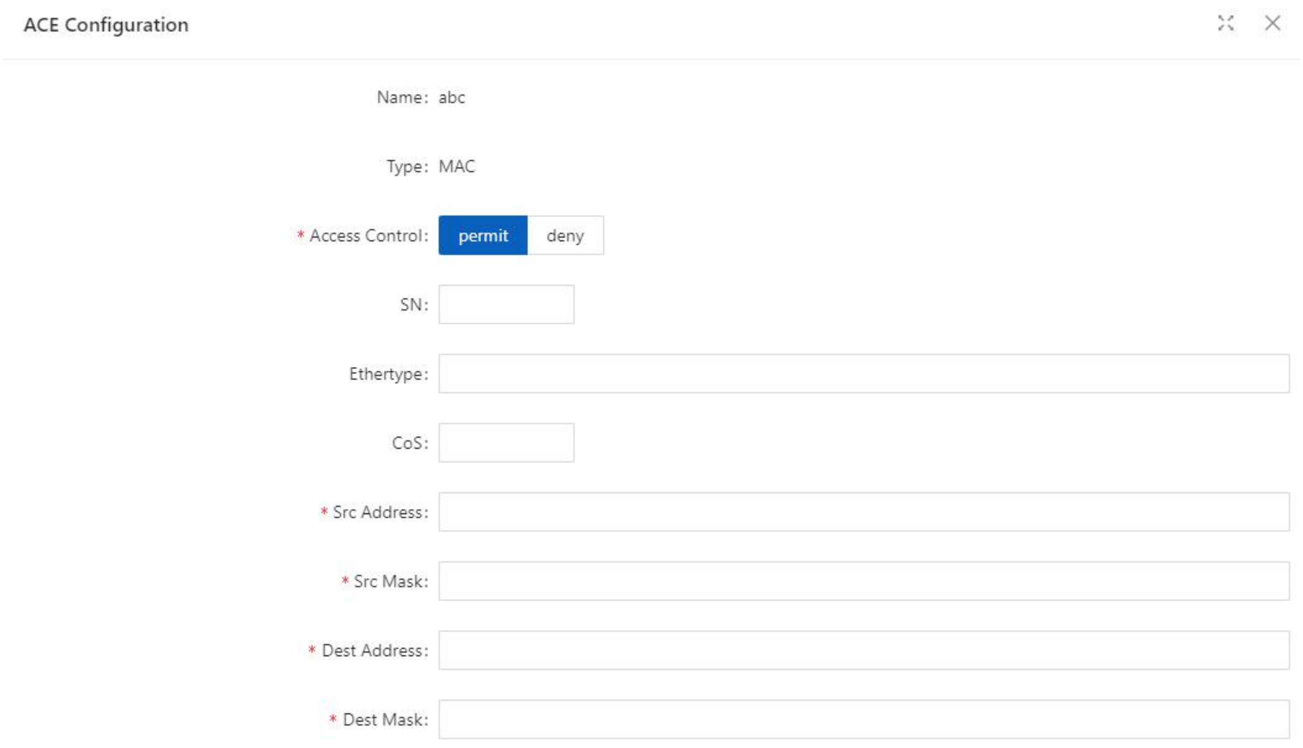
1. Select **Advance** > **Security** > **ACL Configuration** in the navigation area.

2. Click the **+Add ACL** button to enter the Rule Configuration page and choose the ACL type **IPV6** for a basic ACL as shown in Figure 4-26.

3. Configure a rule for an IP ACL, and click **OK**.

4. Select ACK rules in the box below ACE Configuration and click **+Add ACE** button to enter ACE Configuration page as shown in Figure 4-31. Table 4-19 describes the configuration items of configuring an IP ACE configuration.

Figure 4-31 Apply the ACL rule to the port



ACE Configuration

Name: abc

Type: MAC

* Access Control: permit deny

SN:

Ethertype:

CoS:

* Src Address:

* Src Mask:

* Dest Address:

* Dest Mask:

Table 4-19 The description of the MAC ACL

Item		Description
Access Control	permit	Release the packets that match this rule
	deny	Discard packets matching this rule
SN		Rule entry sequence number
Ethertype		Ethernet protocol type, range (0x05DD-0xFFFF)
CoS		CoS value of the message, range (0-7)
Src Address		Source MAC address, such as 00.d0.f 8.22.33.40
Src Mask		The MAC address mask is inverted. If it matches the first 24 digits of the MAC address, the mask is ffff.ff00.0000. Here it needs to be configured as 0000.00ff.ffff
Dest Address		Destination MAC address, such as 00.d0.f 8.22.33.41
Dest Mask		homology mask

5. Configure ACE and click **OK**.

6. Click **Batch Edit** below Port Configuration to enter the ACL Port Configuration page, select the ACL rules of the corresponding port, and click **OK**.

4.7 QoS

4.7.1 Overview

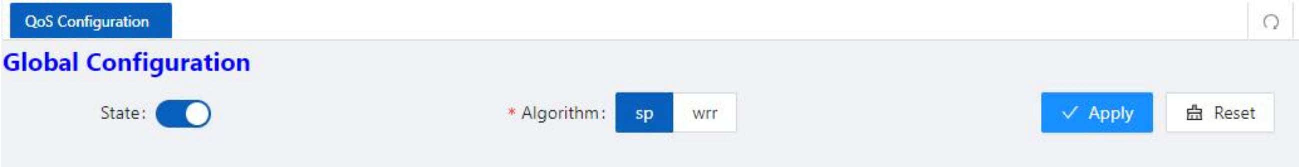
Quality of Service (QoS) reflects the ability of a network to meet customer needs. In an internet, QoS evaluates the ability of the network to forward packets of different services. The evaluation can be based on different criteria because the network may provide various services. Generally, QoS performance is measured with respect to bandwidth, delay, jitter, and packet loss ratio during packet forwarding process.

4.7.2 Configuring QoS

Enable QoS

1. Select **Advance** > **Security** > **QoS Configuration** in the navigation area to enter the QoS Global Configuration page, as shown in Figure 4-32. Table 4-20 describes the QoS summary items.

Figure 4-32 QoS global configuration



2. Click State button, choose Algorithm, **click** Apply to enable QoS.

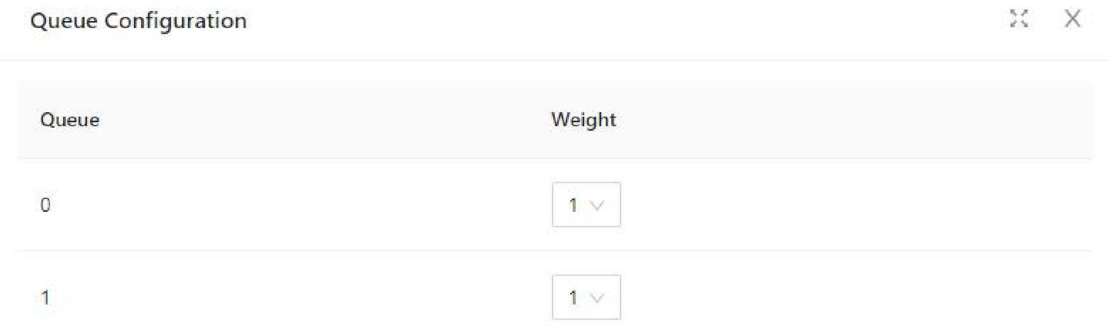
Table 4-20 Descriptions of QoS summary

Item	Description		
QoS Configuration	State		Enable QoS, all QoS functions do not support configuration before enabling
	Algorithm	Sp	Absolute priority scheduling, the queue ID is large, the priority is high, and the low-priority queue is processed after the high -priority queue is processed.
		Wrr	robin scheduling algorithm schedules each queue in turn according to the queue weight, from the largest to the smallest queue ID.

QoS Mapping

1. In current page, click **Queue** button below QoS Mapping to enter Queue Configuration page, as shown in Figure 4-33. Table 4-21 describes the QoS summary items.

Figure 4-33 Queue configuration



Queue Configuration

Queue	Weight
0	1
1	1

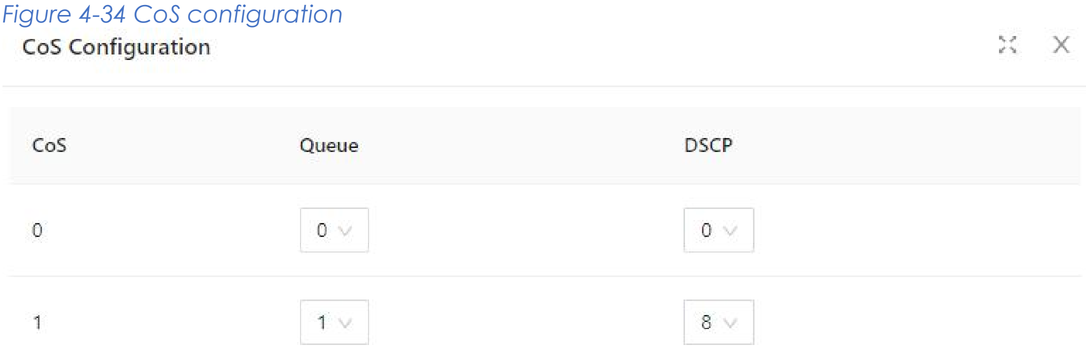
Table 4-21 Descriptions of queue configuration

Item	Description	
	Queue	< 0, 7 >

Queue weight	weight	< 0, 32>, the larger the value, the higher the weight, and the higher the probability of preferential processing of packets in this queue under the condition of channel congestion, 0 means infinity.

2. Click **CoS** button below QoS Mapping to enter CoS Configuration page, as shown in Figure 4-34. Table 4-22 describes the CoS configuration items.

Figure 4-34 CoS configuration



CoS Configuration

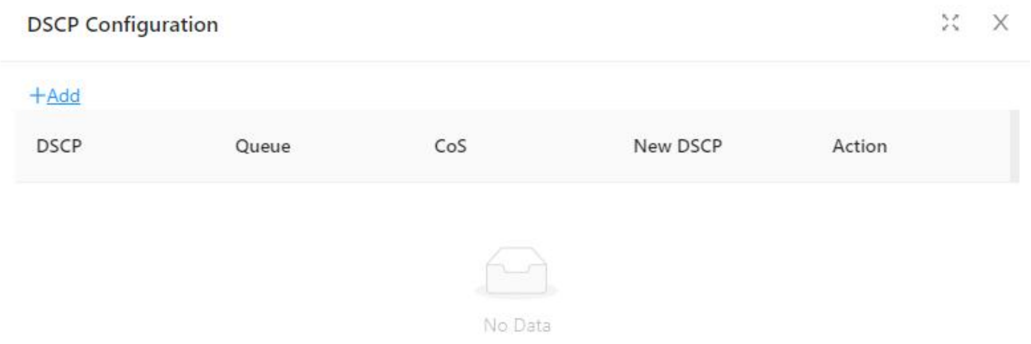
CoS	Queue	DSCP
0	0	0
1	1	8

Table 4-22 Descriptions of CoS configuration

Item		Description
CoS Configuration	CoS	<0, 7>
	Queue	< 0, 7>, CoS-queue mapping relationship, based on the CoS marked on the port, modifying the packet egress queue takes effect when the port is configured as no trust, trust CoS or trust DSCP and non-IP packets.
	DSCP	CoS-dscp mapping relationship takes effect when the port is configured as no trust, trust cos or trust DSCP and is not IP packets. Modify the packet DSCP value.

3. Click **DSCP** button below QoS Mapping to enter DSCP Configuration page, as shown in Figure 4-35. Table 4-23 describes the DSCP configuration items.

Figure 4-35 CoS configuration



DSCP Configuration

+Add

DSCP	Queue	CoS	New DSCP	Action

No Data

Table 4-23 Descriptions of CoS configuration

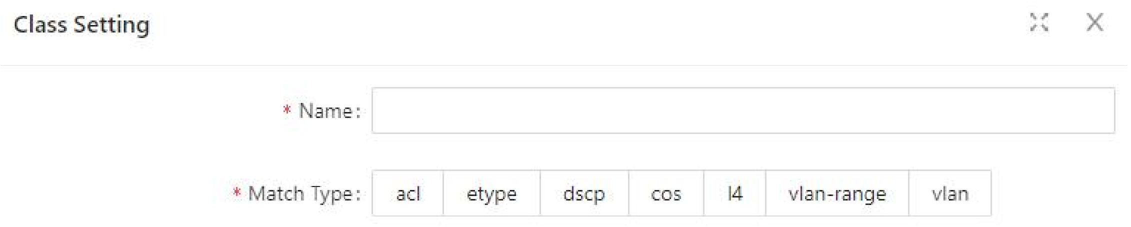
Item		Description
DSCP Map	DSCP	<0, 63>
	Queue	< 0, 7>, dsp-queue mapping relationship, which takes effect when the port is configured as trust DSCP and IP packets, modify the packet export queue
	CoS	< 0, 7>, dscp-cos mapping relationship, which takes effect when the port is

		configured as trust DSCP and IP packets, modify the cos field of the packet
	New DSCP	< 0, 63 >, dscp-dscp mapping relationship, which takes effect when the port is configured as trust DSCP and IP packets, first perform dscp-dscp mapping, and then perform dscp-cos mapping

Class Setting

1. In current page, click **+Add** button below Class Setting to enter Class Setting page, as shown in Figure 4-36. Table 4-24 describes the QoS summary items.

Figure 4-36 Class setting page


Class Setting

* Name:

* Match Type: acl | etype | dscp | cos | l4 | vlan-range | vlan

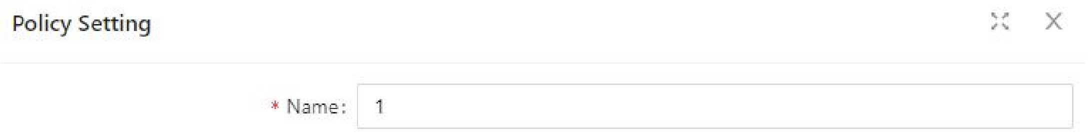
Table 4-24 Descriptions of class setting

Item		Description
Class Setting	Name	Create a category, define the category name
	Match	Define match type, support associated ACL; Support packet ETYPE, DSCP, CoS, l4port, VLAN field matching

Policy Setting

1. In current page, click **+Add Policy** button below Policy Setting to enter Policy Setting page, as shown in Figure 4-37. Text the box behind **Name**, click **OK** button.

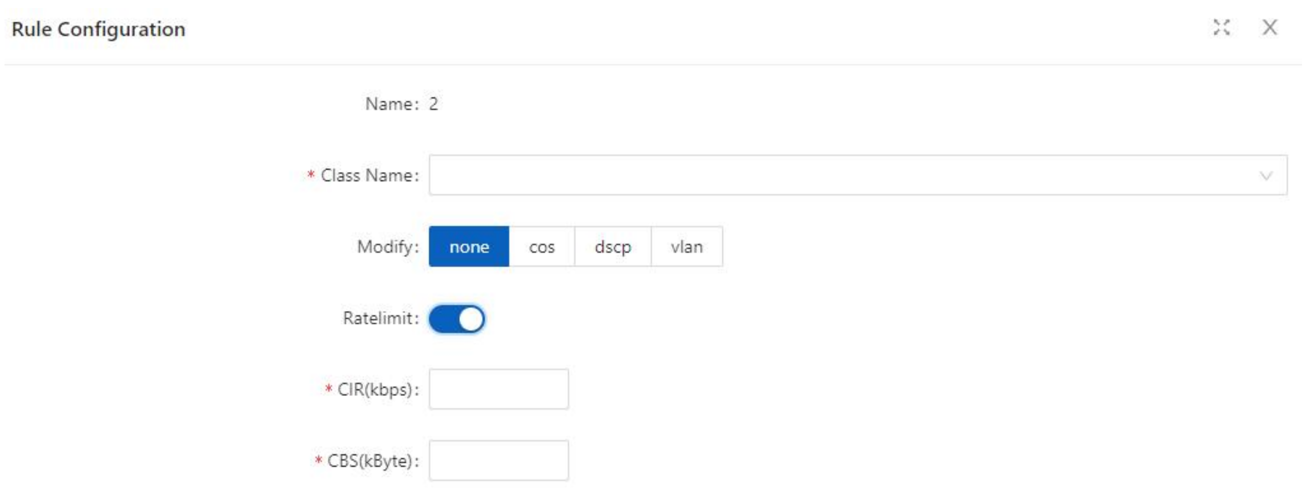
Figure 4-37 Class setting page


Policy Setting

* Name: 1

2. Click **+Add Policy Rule** button below Policy Setting to enter Policy Rule Setting page, as shown in Figure 4-38. Table 4-25 describes the QoS rule configuration items.

Figure 4-38 Rule configuration page



Rule Configuration

Name: 2

* Class Name:

Modify: none cos dscp vlan

Ratelimit:

* CIR(kbps):

* CBS(kByte):

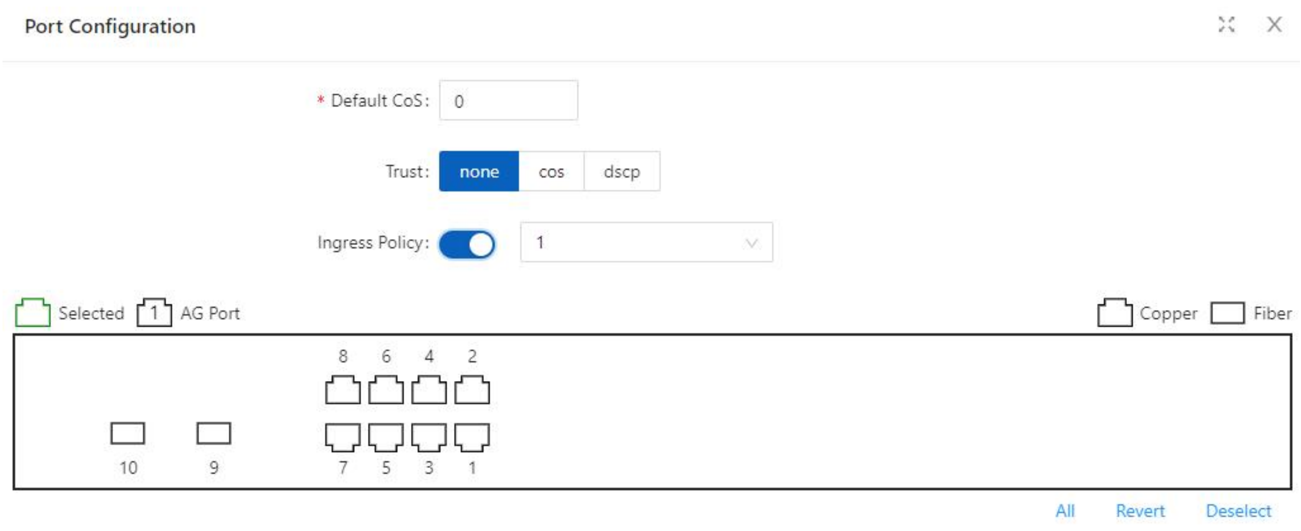
Table 4-25 Descriptions of class setting

Item		Description
Rule Configuration	Name	Rule name
	Class Name	Create a policy, define a policy name
	Modify	policy, supports modifying CoS, DSCP, VLAN and other actions
	Ratelimit	Action 2 corresponding to the strategy, speed limit
	CIR	Speed limit waterline, unit kbps
	CBS	burst capability, unit Kbyte

Port Configuration

1. In current page, click **+Batch Edit** button below Port Configuration to enter Port Configuration page, as shown in Figure 4-39. Table 4-26 describes the port configuration items.

Figure 4-39 Port configuration page



Port Configuration

* Default CoS: 0

Trust: none cos dscp

Ingress Policy: 1

Table 4-26 Descriptions of port configuration

Item		Description
Port Configuration	Default CoS	< 0, 7>, when the configuration port is not trusted, or the configuration is trusted but the message does not meet the trust condition, the port default cos is used to mark the ingress message

	Trust	Support untrust, trust cos, trust DSCP configuration. When in no trust mode, the entry stage modifies the cos field and DSCP field of the message according to the default cos of the port; when trust cos is configured, the same as the no trust mode for untagged messages, and for tagged messages, choose the message with its own 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.
	Ingress Policy	Select Ingress Policy

4.8 DoS

4.8.1 Overview

Denial of Service (DoS) attack aims to prevent the computer or network from providing normal service. There are many kinds of DoS attacks, and also many different implementation methods. Its common trait is that the victim host or network can not receive and process external requests in time. Here are some typical DoS attack types.

SYN Flood Message Attack:

SYN Flood attack is the most common DDOS attack on the current network, but also the most classic DoS attack. By sending a large number of attack messages with fake source addresses to the port of the network service, the target server connection queue is full, thus blocking access to other legitimate users.

ICMP Flood Message Attack:

ICMP Flood attack is a DDOS attack that sends a large number of ping packets to the target host in a short period of time and consumes the host resources. The host can't provide any other service after its resources are exhausted.

ARP Flood Message Attack:

ARP Flood attack is a DDOS attack that sends a large number of ARP request packets to the target host in a short period of time and consumes the host resources. Unable to answer other ARP requests after the host resources are exhausted.

NULL SCAN Message Attack:

NULL SCAN attack is mainly that the attacker sends TCP packets without any flag to the target host's IP, and parts of operating systems actively feedback RST messages, so that the attacker obtains the port that does not close the session. Anti-NULL SCAN attack is to discard TCP messages without any TCP flag bits, which can effectively prevent attackers from launching subsequent attacks after obtaining the closure of each port through NULL SCAN.

TCP Message with SYN and FIN：

Normally, the SYN sign (connection request sign) and the FIN sign (connection removal sign) can’t appear in one TCP message, and the RFC does not specify how the IP stack will handle such a deformed message. The attacker can take advantage of this feature to determine the type of operating system by sending TCP messages with SYN and FIN settings.

TCP Message with FIN without ACK:

Under normal circumstances, except for the first message(SYN message), all messages possess ACK signs, including the TCP connection removal message (message with FIN sign setting). However, some attackers may send TCP messages which are with FIN and without ACK to the target host so that it may cause the target host to crash.

TCP Message with SYN and Source Port Number Between 0-1023:

0-1023 is the known port number assigned by IANA and in most systems can be used only by the system (or root) process or the procedure executed by privileged users. These ports (0-1023) can’t be used as the source port number for the first TCP message (already has been set the SYN sign). Start the anti-illegal TCP message attack function, the device will check according to the characteristics of non-TCP message, if illegal, then discarded.

Our company provides the above several anti-DoS attack functions.

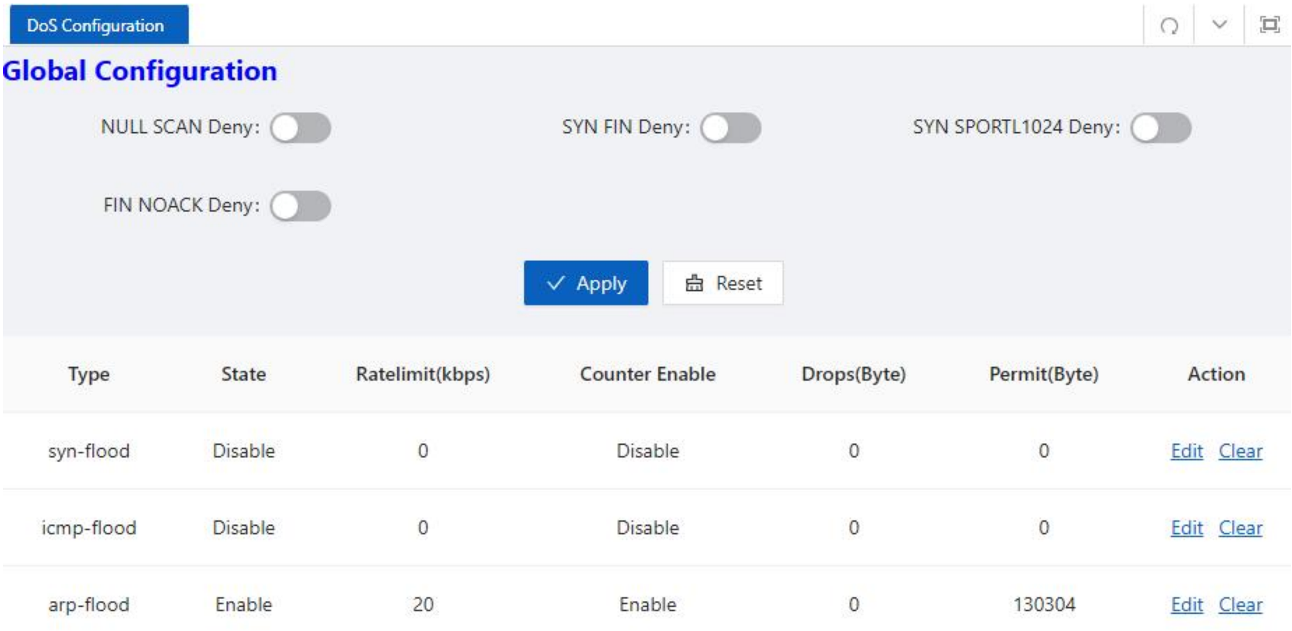
4.8.2 Configuring DoS

In the navigation area, select **Advance** > **Security** > **DoS Configuration** and enter the DoS Configuration page. This page contains four parts: Global Configuration, SYN Configuration, ICMP Configuration, and ARP Configuration.

Global Configuration

The DoS Global Configuration page is shown in Figure 4-40, including several global anti-DoS attack configurations, and the specific parameters are shown in Table 4-27. Global SYN Flood, ICMP Flood and ARP Flood configure in the same way. Take the ARP Flood Configuration for example, the setting page is as Figure 4-41.

Figure 4-40 Global configuration page



DoS Configuration

Global Configuration

NULL SCAN Deny: ○ SYN FIN Deny: ○ SYN SPORTL1024 Deny: ○

FIN NOACK Deny: ○

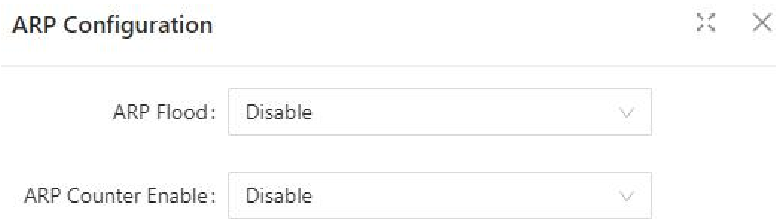
✓ Apply Reset

Type	State	Ratelimit(kbps)	Counter Enable	Drops(Byte)	Permit(Byte)	Action
syn-flood	Disable	0	Disable	0	0	Edit Clear
icmp-flood	Disable	0	Disable	0	0	Edit Clear
arp-flood	Enable	20	Enable	0	130304	Edit Clear

Table 4-27 Descriptions of global configuration

Item	Description
NULL SCAN Deny	Configure the global anti-NULL SCAN attack, and discard the TCP message without any flag
SYN FIN Deny	Configure global anti-SYN FIN attack, and discard TCP messages set by both SYN and FIN flag
SYN SPORT1024 Deny	Configure the global anti-SYN SPORTL1024 attack, and discard the synchronous message of the source port (0-1023) TCP after opening
FIN NOACK Deny	Configure global anti-FIN NOACK attack, and discard TCP messages with FIN set without ACK set
SYN/ICMP/ARP Flood	Configure global anti-SYN/ICMP/ARP Flood attack
SYN/ICMP/ARP Flood rate-limit	Configure the rate limit range of anti-SYN/ICMP/ARP Flood attack and if its value is 0, deny all attack messages
Counter enable	Configure the counter enable function of anti-SYN/ICMP/ARP Flood attack and if it's enabled, count the hit attack message

Figure 4-41 ARP configuration page



ARP Configuration

ARP Flood: Disable

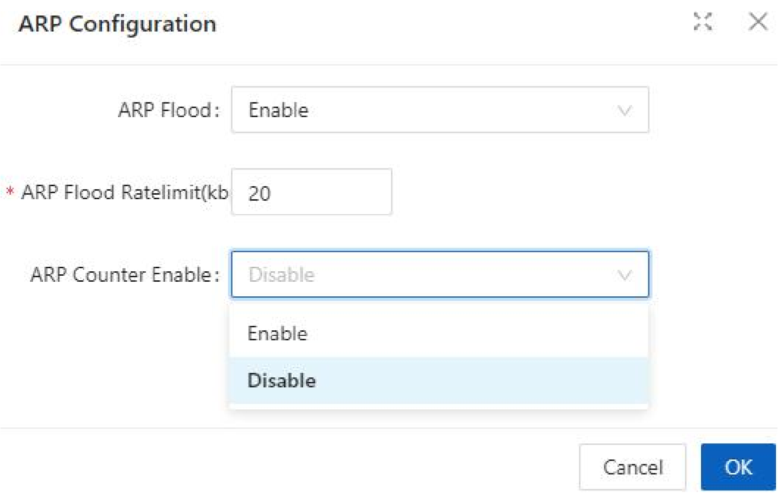
ARP Counter Enable: Disable

Operating Steps

1. Select **Advance** > **Security** > **DoS Configuration** in the navigation bar to enter the DoS Configuration page.

2. Click the **Edit** button in the Global Configuration table to enter the anti-DoS attack creation modal, and fill in the parameters according to requirements. Take the Global ARP Flood Configuration for instance, as shown in Figure 4-42, and click the **OK** button to complete the configuration.

Figure 4-42 ARP Flood configuration page



ARP Configuration

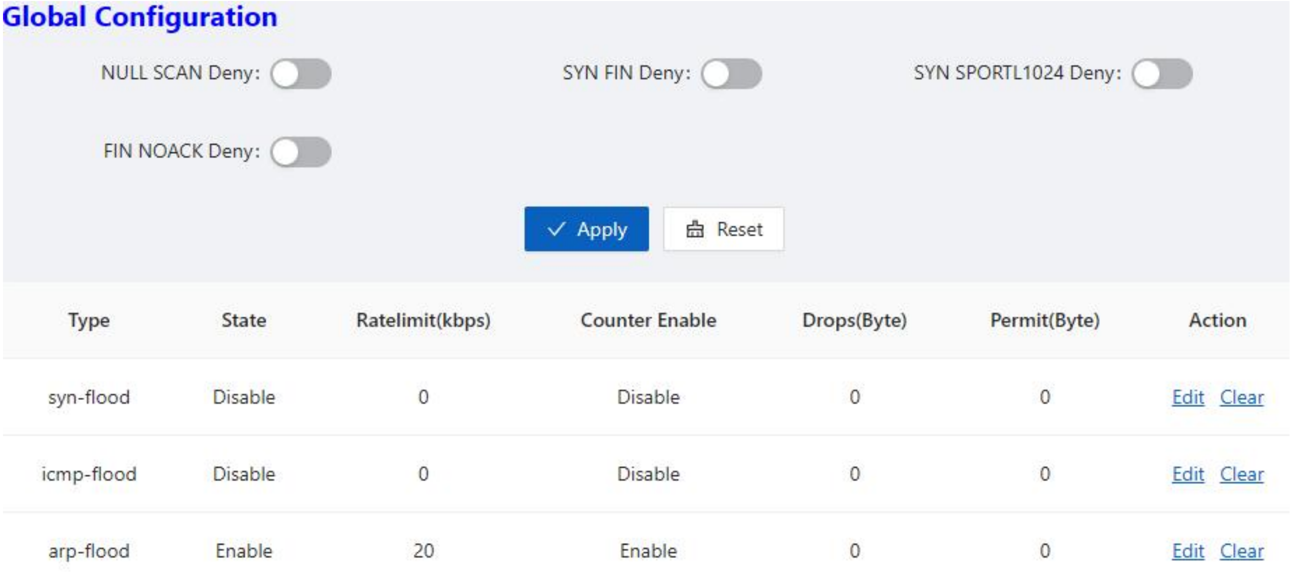
ARP Flood: Enable

* ARP Flood Ratelimit(kb: 20

ARP Counter Enable: Disable

After above steps, the successful DoS Global Configuration page is shown in Figure 4-43.

Figure 4-43 Global ARP Flood configuration page



Global Configuration

NULL SCAN Deny: ○ SYN FIN Deny: ○ SYN SPORTL1024 Deny: ○

FIN NOACK Deny: ○

Type	State	Ratelimit(kbps)	Counter Enable	Drops(Byte)	Permit(Byte)	Action
syn-flood	Disable	0	Disable	0	0	Edit Clear
icmp-flood	Disable	0	Disable	0	0	Edit Clear
arp-flood	Enable	20	Enable	0	0	Edit Clear

SYN/ICMP/ARP Configuration

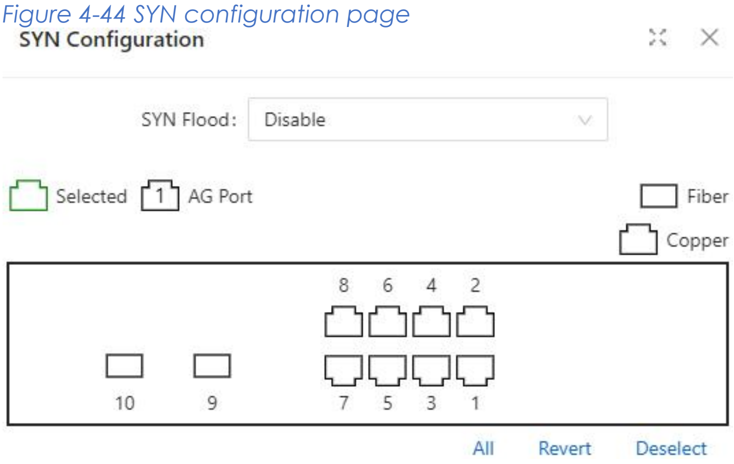
Port Configuration against DoS attack includes SYN Flood, ICMP Flood and ARP Flood. The configuration page is shown in Figure 4-44~46, and the parameters' descriptions is shown in Table 4-28.

Table 4-28 Descriptions of SYN/ ICMP/ARP configuration

Item	Description
SYN Flood	Enable SYN Flood attack

SYN Flood rate-limit	Limit the SYN message attack flow rate
ICMP Flood	Enable ICMP Flood attack
ICMP Flood rate-limit	Limit the ICMP message attack flow rate
ARP Flood	Enable ARP Flood attack
ARP Flood rate-limit	Limit the ARP message attack flow rate

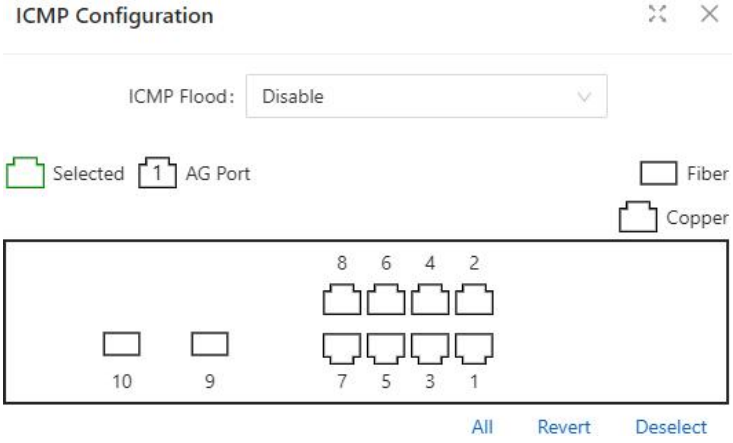
Figure 4-44 SYN configuration page



SYN Configuration

SYN Flood: Disable

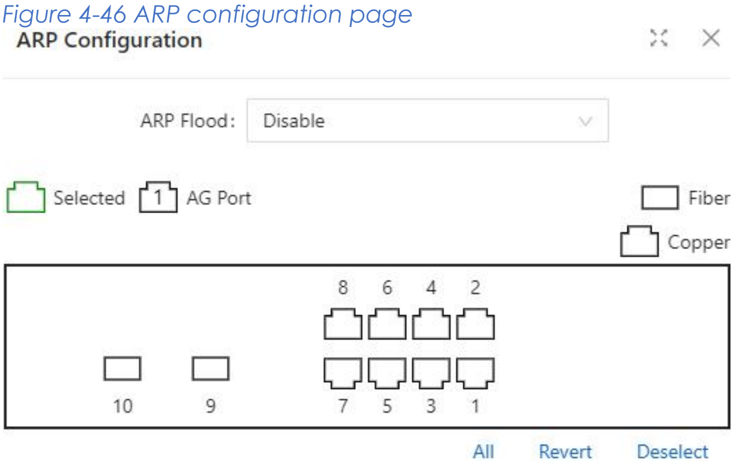
Figure 4-45 ICMP configuration page



ICMP Configuration

ICMP Flood: Disable

Figure 4-46 ARP configuration page



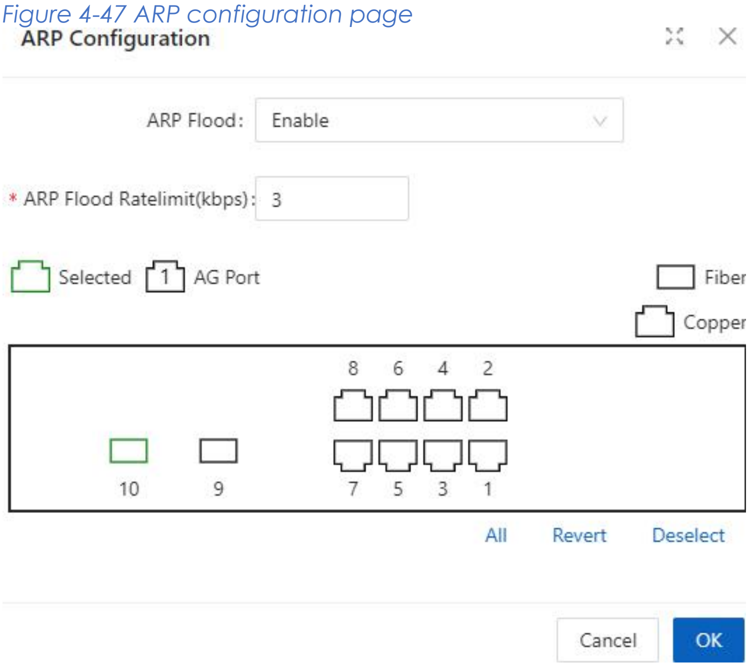
ARP Configuration

ARP Flood: Disable

Operating Steps

1. Select **Advance** > **Security** > **DoS Configuration** in the navigation bar to enter the DoS Configuration page.
2. Click the **Batch Edit** button under SYN/ICMP/ARP Configuration to enter the creation page. Take the ARP Configuration as an example, as shown in Figure 4-47.

Figure 4-47 ARP configuration page



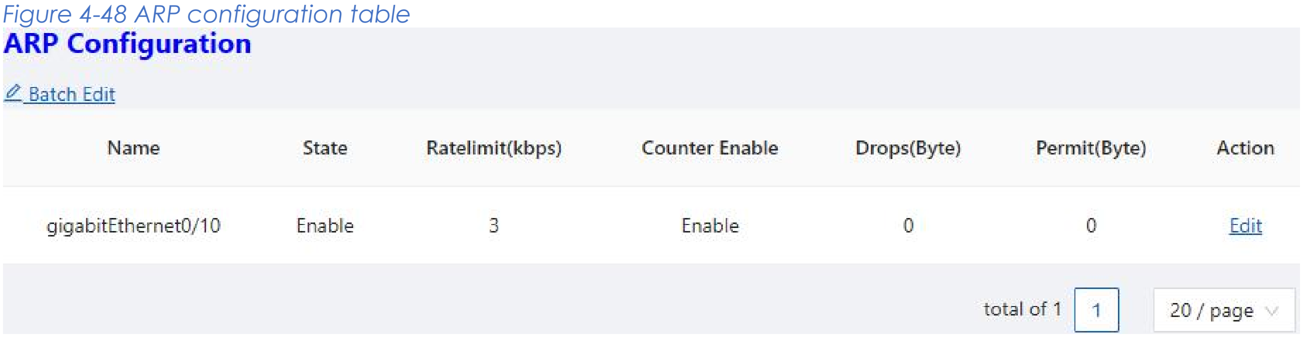
ARP Configuration

ARP Flood: Enable

* ARP Flood Ratelimit(kbps): 3

After above steps, the successful ARP Configuration page is shown in Figure 4-48.

Figure 4-48 ARP configuration table



ARP Configuration

Batch Edit

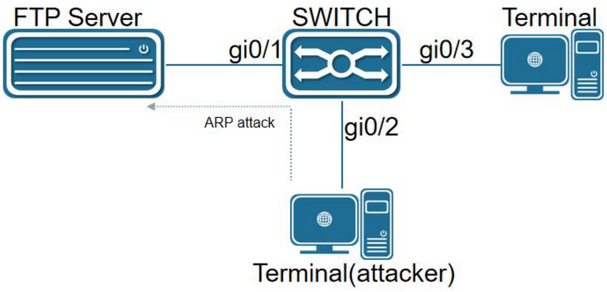
Name	State	Ratelimit(kbps)	Counter Enable	Drops(Byte)	Permit(Byte)	Action
gigabitEthernet0/10	Enable	3	Enable	0	0	Edit

A Configuration Example

Take ARP Flood Configuration for example, the following networking requirements are shown in Figure 4-49:

- Port gi0/1 connects to FTP server while port gi0/2 and gi0/3 connect to terminal devices respectively.
- The connecting terminal of port gi0/2 forges a large number of IP and MAC addresses to launch ARP attacks, leaving the FTP server unable to handle normal requesting ARP messages.

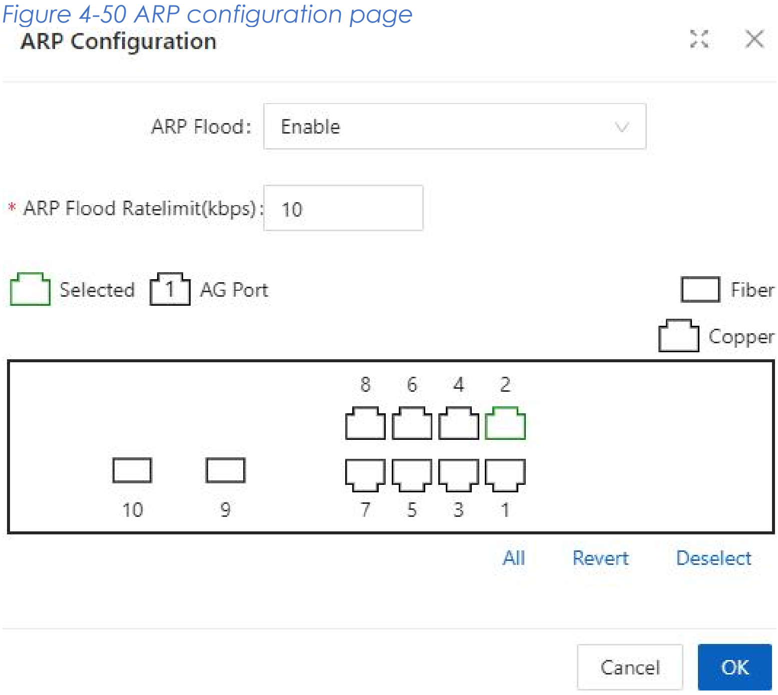
Figure 4-49 Network topology



1. Select **Advance** > **Security** > **DoS Configuration** in the navigation bar to enter the DoS Configuration page.

2. Click the **Batch Edit** button under ARP Configuration to enter the ARP Configuration modal, select GigabitEthernet0/2 in the port panel, and click **OK** to complete the configuration, as shown in Figure 4-50.

Figure 4-50 ARP configuration page


ARP Configuration

ARP Flood: Enable

* ARP Flood Ratelimit(kbps): 10

3. Click the **Save** button in the navigation bar to save such configuration.

4.9 Route

4.9.1 ARP/Neighbor Configuration

4.9.1.1 Overview

ARP resolves an IP address into a physical address, such as an Ethernet MAC address.

On an Ethernet LAN, a device uses ARP to get the MAC address of the target device for a packet

ARP Table

After obtaining the MAC address for the destination host, the device puts the IP-to-MAC mapping into its own ARP table. This mapping is used for forwarding packets with the same destination in the future.

An ARP table stores dynamic and static ARP entries.

Dynamic ARP Entry

ARP automatically creates and updates dynamic entries. A dynamic ARP entry is removed when its aging timer expires or the output interface goes down, and it can be overwritten by a static ARP entry.

Static ARP Entry

A static ARP entry is manually configured and maintained. It cannot get aged or be overwritten by a dynamic ARP entry.

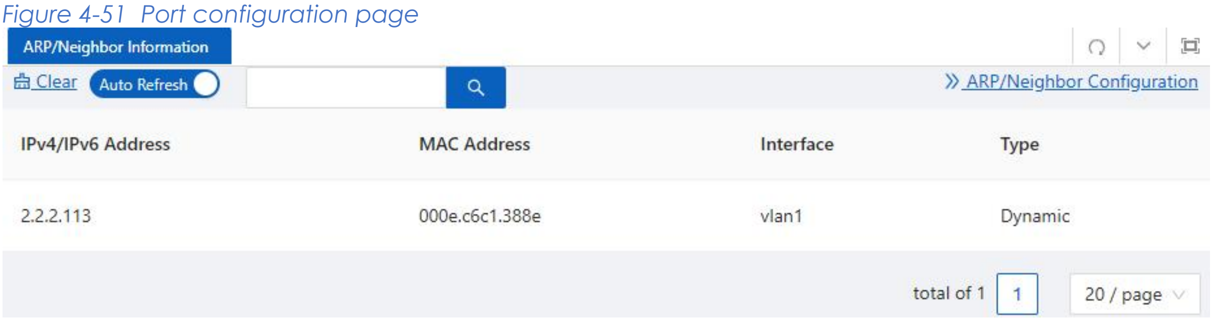
Static ARP entries protect communication between devices, because attack packets cannot modify the IP-to-MAC mapping in a static ARP entry.

4.9.1.2 Configuring ARP/Neighbor

Displaying ARP/Neighbor

1. Select **Monitor** > **ARP/Neighbor Information** in the navigation area to enter ARP/Neighbor displaying page as shown in Figure 4-51. Table 4-29 describes the configuration items of ARP/Neighbor.

Figure 4-51 Port configuration page



IPv4/IPv6 Address	MAC Address	Interface	Type
2.2.2.113	000e.c6c1.388e	vlan1	Dynamic

Table 4-29 Descriptions of ARP/Neighbor

Item	Description
IPv4/IPv6 Address	Terminal IP address
MAC Address	Terminal MAC address
Interface	The name of the Layer 3 interface where the terminal is located
Type	ARP/neighbor address type

Configuring ARP/Neighbor

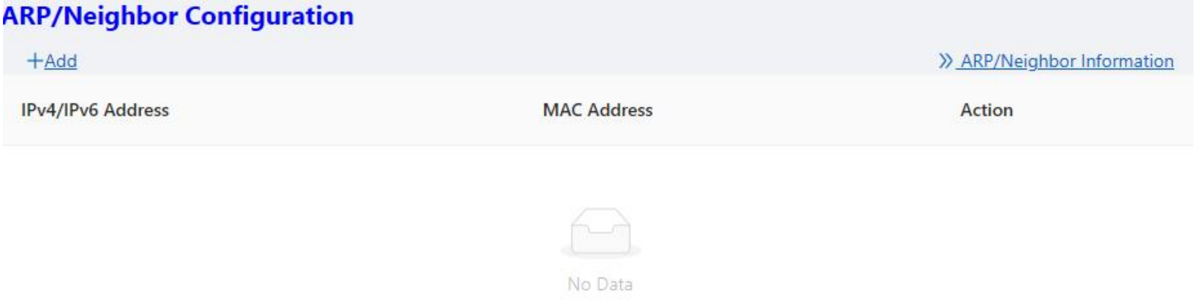
1. Select **Advance** > **Layer3** > **ARP/Neighbor Configuration** in the navigation area to enter ARP/Neighbor Configuration page as shown in Figure 4-52.

2. Click **+Add** button to enter the crating page as shown in Figure 4-53.

3. Configure the IP address and MAC address.

4. Click **OK** button to complete the configuration.

Figure 4-52 ARP/Neighbor configuration page



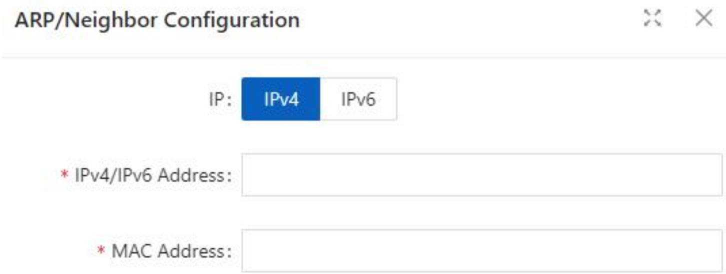
ARP/Neighbor Configuration

+Add » ARP/Neighbor Information

IPv4/IPv6 Address	MAC Address	Action

No Data

Figure 4-53 Creating a new ARP/Neighbor



ARP/Neighbor Configuration

IP: IPv4 IPv6

* IPv4/IPv6 Address:

* MAC Address:

4.9.2 Route

Routers are responsible for routing packets on the Internet. A router selects an appropriate route according to the destination address of a received packet and forwards the packet to the next router. The last router on the path is responsible for sending the packet to the destination host.

4.9.2.1 Routing Table

Routers forward packets through a routing table. Each entry in the table specifies which physical interface a packet should go out to reach the next hop (the next router) or the directly connected destination.

Routes in a routing table fall into three categories by origin:

- Direct routes: Routes discovered by data link protocols, also known as interface routes.
- Static routes: Routes that are manually configured.
- Dynamic routes: Routes that are discovered dynamically by routing protocols.

A route entry has the following items:

- Destination IP address: Destination IP address or destination network.
- Mask (IPv4)/prefix length (IPv6): Specifies, together with the destination address, the address of the destination network.

- Outbound interface: Specifies the interface through which a matching IP packet is to be forwarded.
- Next hop: Specifies the address of the next hop router on the path.
- Preference for the route: Routes to the same destination may be found by various routing protocols or manually configured, and routing protocols and static routes have different priorities configured. The route with the highest priority (the smallest value) will be selected as the optimal route.

4.9.2.2 Static Route

A static route is manually configured. If a network 's topology is simple, you only need to configure static routes for the network to work normally. The proper configuration and usage of static routes can improve network performance and ensure bandwidth for important network applications.

The disadvantage of using static routes is that they cannot adapt to network topology changes. If a fault or a topological change occurs in the network, some routes will be unreachable. In this case, the network administrator has to modify the static routes manually.

While configuring a static route, you can specify either the output interface or the next hop address as needed. The next hop address cannot be a local interface 's IP address; otherwise, the route configuration will not take effect.

Actually, it is necessary to identify next hop addresses for all route entries because the router needs to use the next hop address of a matching entry to resolve the corresponding link layer address.

4.9.2.3 Configuring Static Route

Displaying Static Route

1. Select **Advance** > **Layer3** > **Static Route** in the navigation area to enter Static Route displaying page as shown in Figure 4-54. Table 4-30 describes the configuration items of static route.

Figure 4-54 Creating a new static ARP

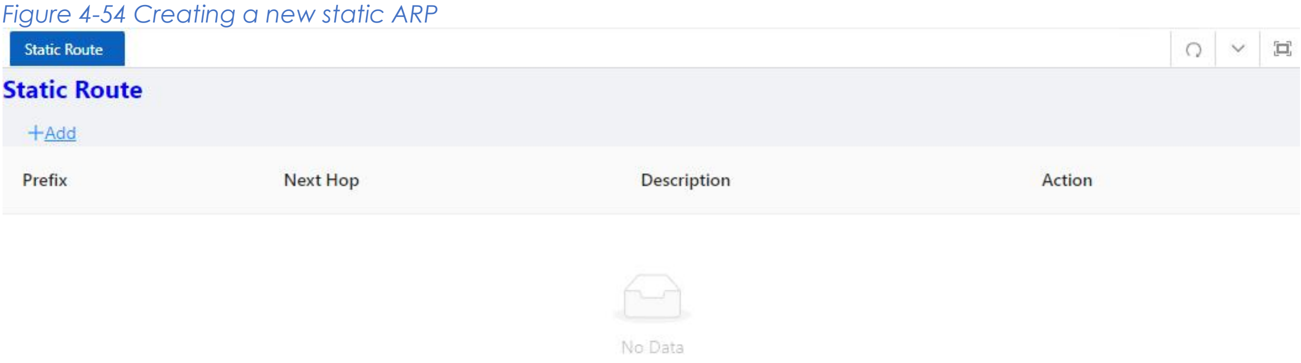


Table 4-30 Descriptions of static route

Item	Description

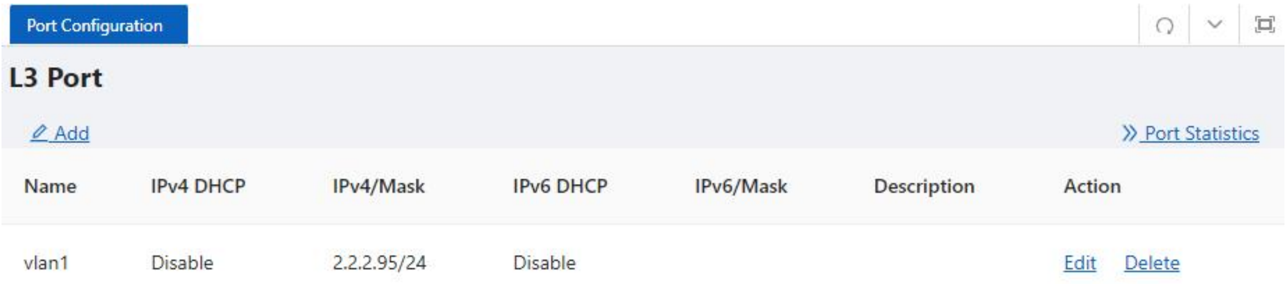
Route Type	IPv4 or IPv6 route
Prefix	Routing prefix address, or routing network segment; for example, common route 0.0.0.0/0 192.168.1.1, the prefix IP is 0.0.0.0
Next Hop	Next hop IP address of the route
Description	Route description information, optional configuration
Action	Delete or modify

Creating New the Static Route

1. Select **Configuration** > **VLAN** in the navigation area to create VLAN ID.

2. Select **Configuration** > **Port** > **Port Configuration** > **L3 port** in the navigation area to create L3 SVI port as shown in Figure 4-55.

Figure 4-55 Creating a L3 SVI port



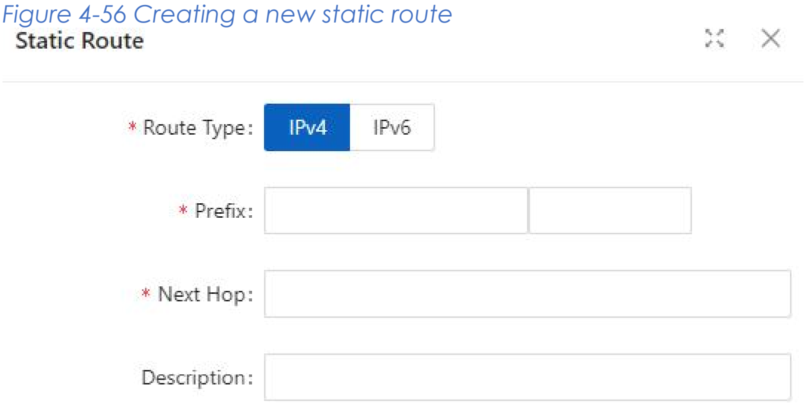
Name	IPv4 DHCP	IPv4/Mask	IPv6 DHCP	IPv6/Mask	Description	Action
vlan1	Disable	2.2.2.95/24	Disable			Edit Delete

3. Select **Advance** > **Layer3** > **Static Route** in the navigation area to enter Static Route page, click **+Add** button to enter the crating page as shown in Figure 4-56.

4. Configure the Prefix and Next Hop.

5. Click **OK** button to complete the configuration.

Figure 4-56 Creating a new static route



* Route Type: IPv4 IPv6

* Prefix:

* Next Hop:

Description:

NOTE:

✦ When adding a new SVI port, the default management IP address will be automatically deleted. Please ensure that the new SVI port can continue to be accessed.

5 Maintenance

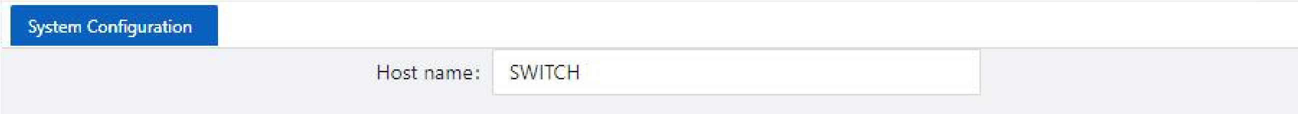
5.1 System Configuration

The system configuration module provides host name settings, services of Telnet, SSH, HTTP, HTTPS, and management IP setting.

5.1.1 Host Name Settings

Select **Maintenance** > **system configuration** from the navigation area to enter the System Configuration page, as shown in Figure 5-1. User can set the host name of the switch here.

Figure 5-1 Management information page



Host name: SWITCH

5.1.2 Services Enable

The service management module provides the following types of services: FTP, Telnet, SSH, SFTP, HTTP and HTTPS. You can enable or disable the services as needed. In this way, the performance and security of the system can be enhanced, thus secure management of the device can be achieved.

Telnet Server

The Telnet protocol is an application layer protocol that provides remote login and virtual terminal functions on the network.

SSH Server

Secure Shell (SSH) offers an approach to securely logging in to a remote device. By encryption and strong authentication, it protects devices against attacks such as IP spoofing and plain text password interception

HTTP Server

The Hypertext Transfer Protocol (HTTP) is used for transferring web page information across the Internet. It is an application-layer protocol in the TCP/IP protocol suite. You can log in to the device using the HTTP protocol with HTTP service enabled, accessing and controlling the device with Web-based network management.

HTTPS Server

The Secure HTTP (HTTPS) refers to the HTTP protocol that supports the Security Socket Layer (SSL) protocol. The SSL protocol of HTTPS enhances the security of the device in the following ways:

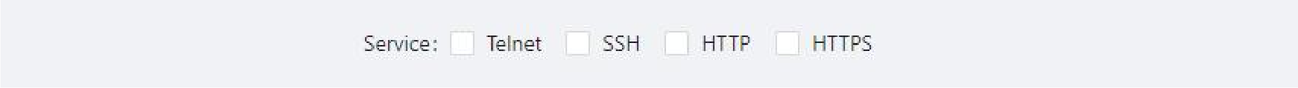
- Uses the SSL protocol to ensure the legal clients to access the device securely and prohibit the illegal clients;

- Encrypts the data exchanged between the HTTPS client and the device to ensure the data security and integrity, thus realizing the security management of the device;
- Defines certificate attribute-based access control policy for the device to control the access right of the client, in order to further avoid attacks from illegal clients.

Configuring Service

1. Select **Maintenance** > **System Configuration** from the navigation area to enter the System Configuration page, as shown in Figure 5-2.
2. Check the box in front of the services, click **Apply** button to enable service.
3. When HTTPS Server is enabled, the certificate and private key should be uploaded. If no certificate is specified, the device will use the default certificate.

Figure 5-2 Service page

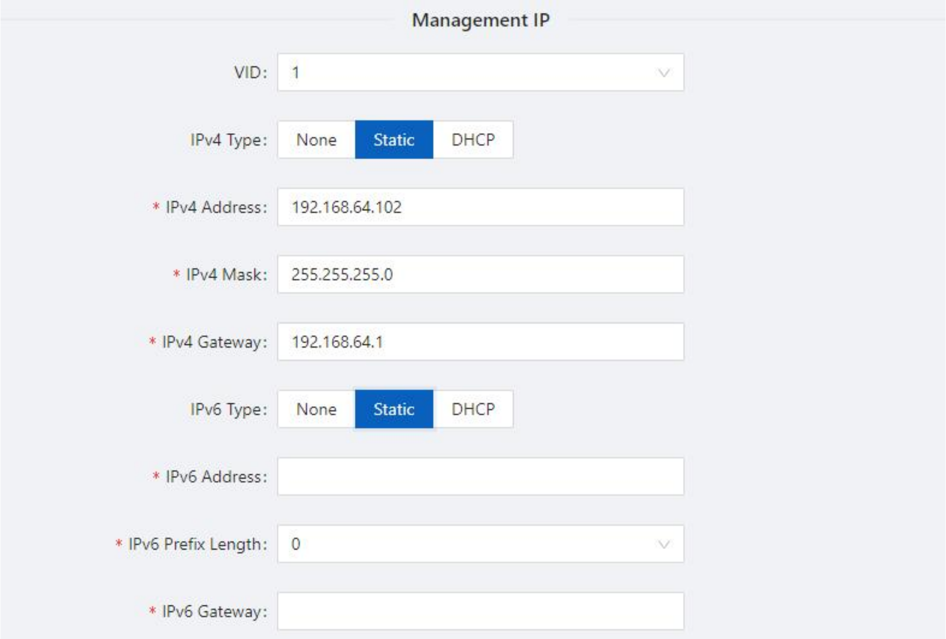


Service: □ Telnet □ SSH □ HTTP □ HTTPS

5.1.3 Management IP

1. Select **Maintenance** > **System Configuration** from the navigation area to enter the System Configuration page, as shown in Figure 5-3. Table 5-1 lists the configuration items of the management IP address.

Figure 5-3 Management information page



Management IP

VID: 1

IPv4 Type: None Static DHCP

* IPv4 Address: 192.168.64.102

* IPv4 Mask: 255.255.255.0

* IPv4 Gateway: 192.168.64.1

IPv6 Type: None Static DHCP

* IPv6 Address:

* IPv6 Prefix Length: 0

* IPv6 Gateway:

Table 5-1 Management information configuration items

Item	Description
VID	Specify the management VLAN ID. The default management VLAN is 1.

IPv4 Type	None：IPv4 management address is not used. Static：Select this option to manually specify an IPv4 address and the mask length DHCP：Select the option to get an IPv4 address through DHCP.
IPv4 Address	Specify the IPv4 management address. The default IP is 172.16.10.166.
IPv4 Mask	Specify the IPv4 management mask. The default mask is 255.255.255.0.
IPv4 Gateway	Specify the IPv4 management gateway. The default gateway is 172.16.10.1.
IPv6 Type	None：IPv6 management address is not used. Static：Select this option to manually specify an IPv6 address and the mask length. DHCP：Select the option to get an IPv6 address through DHCP.
IPv6 Address	Specify the IPv6 management address.
IPv6 Prefix Length	Specify the IPv6 management address prefix length.
IPv6 Gateway	Specify the IPv6 management gateway.

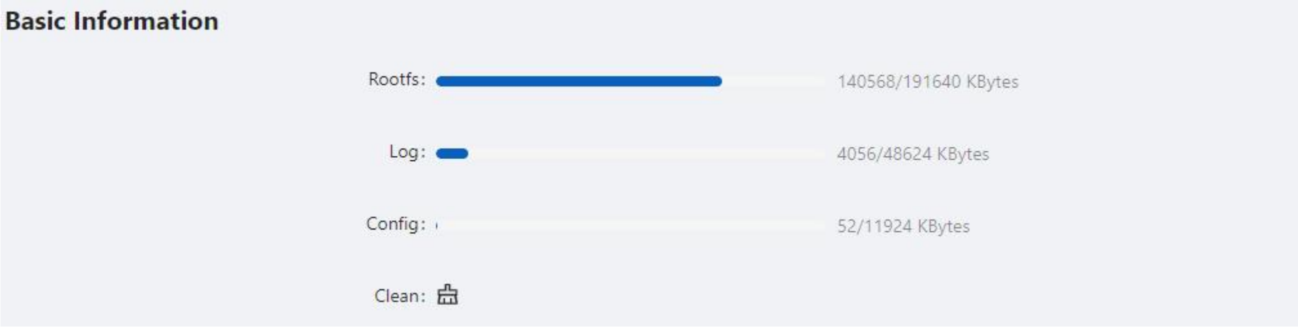
5.2 File Management

The file management module includes basic information, image management, configuration management, certificate management, and page package management functions.

5.2.1 Basic Information

Select **Maintenance** > **File Management** > **Basic Information** from the navigation area to enter the page as shown in Figure 5-4. In the basic information page, you can view the usage of each partition of the device, and click the **Clean** button to clear the system log.

Figure 5-4 Basic information page



Basic Information

Rootfs: 140568/191640 KBytes

Log: 4056/48624 KBytes

Config: 52/11924 KBytes

Clean:

5.2.2 Image Management

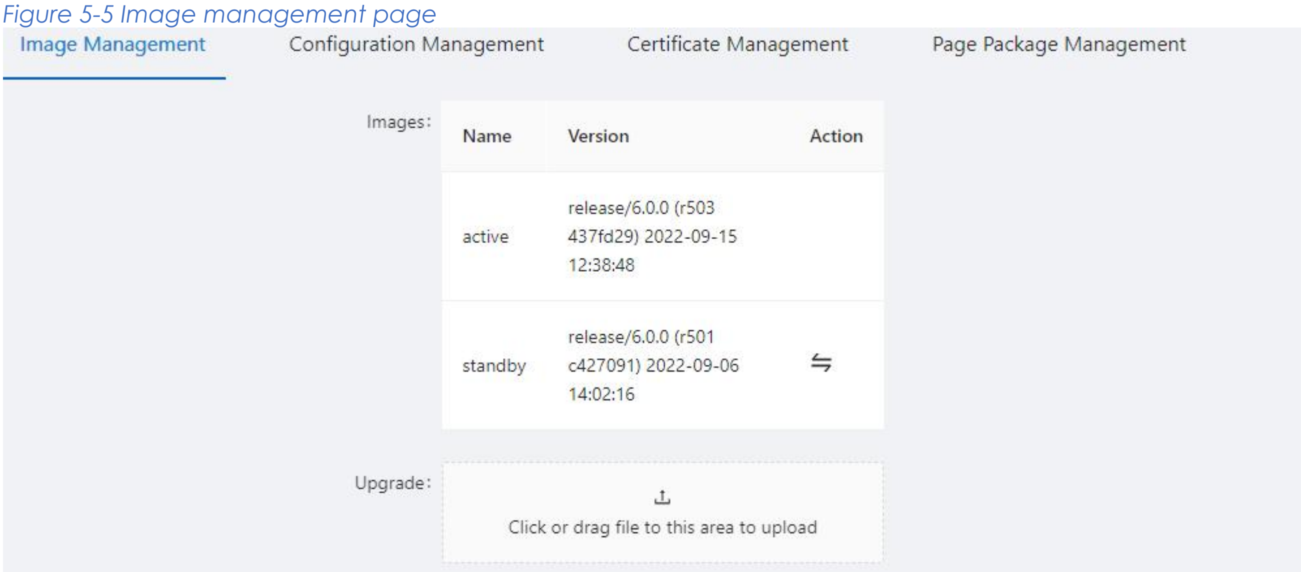
Software upgrade allows you to obtain a target application file from the current host and set the file as the main boot file or backup boot file to be used at the next reboot.

NOTE:

- A software upgrade takes some time. Do not perform any operation on the web interface during the upgrading procedure; otherwise, the upgrade operation may be interrupted.

1. Select **Maintenance** > **File Management** > **Image Management** from the navigation area to enter the page as shown in Figure 5-5.

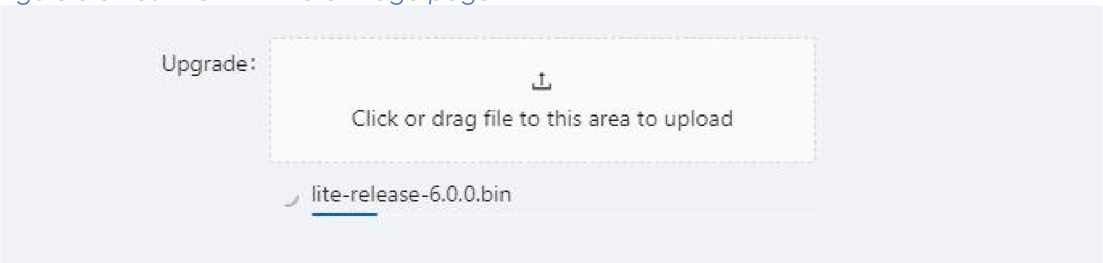
Figure 5-5 Image management page



Name	Version	Action
active	release/6.0.0 (r503 437fd29) 2022-09-15 12:38:48	
standby	release/6.0.0 (r501 c427091) 2022-09-06 14:02:16	⇋

2. Click **Upgrade** button, In the pop-up dialog box, select the upgrade file corresponding to the device, the upgrade file is *.bin format, and the upgrade process is shown in Figure 5-6. After upgrade finished, the device will be rebooted.

Figure 5-6 Flash new firmware image page

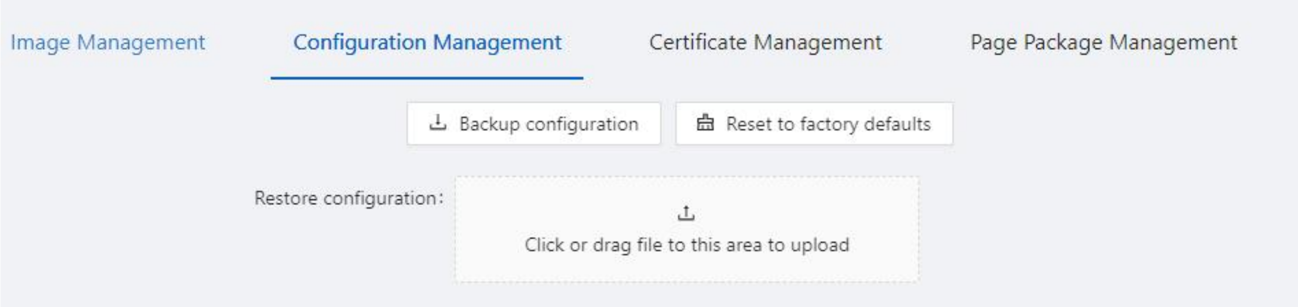


lite-release-6.0.0.bin

5.2.3 Configuration Management

Select **Maintenance** > **File Management** > **Image Management** from the navigation area to enter the page as shown in Figure 5-7.

Figure 5-7 Configuration file management page



Backup Configuration

Click the **Backup configuration** button, a file download dialog box appears. You can save the file locally.

Restore Configuration

After you click the **Choose File** button in this figure, the file upload dialog box appears. You can select the *.conf file to be uploaded, then the device will be reboot.

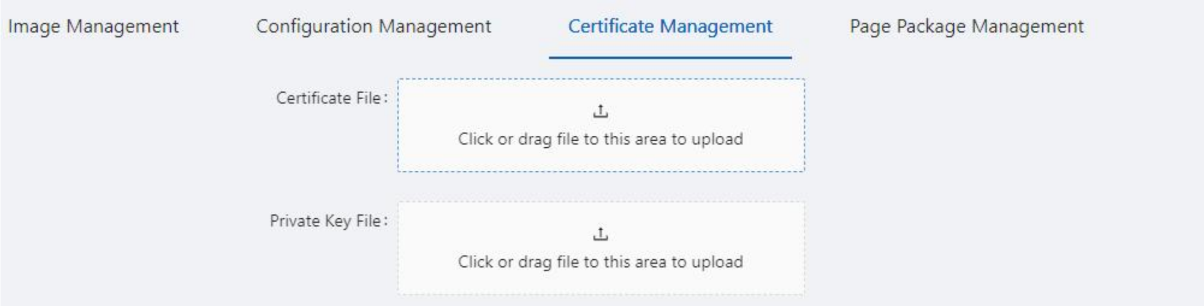
Reset to Factory Defaults

This operation restores the system to factory defaults, delete the current configuration file, and reboot the device. Click the **Reset to Factory Defaults** button to apply this operation.

5.2.4 Configuration Management

When you enable HTTPS, you need to upload the certificate and private key, as shown in Figure 5-8. If you do not specify a certificate, the device uses the default certificate.

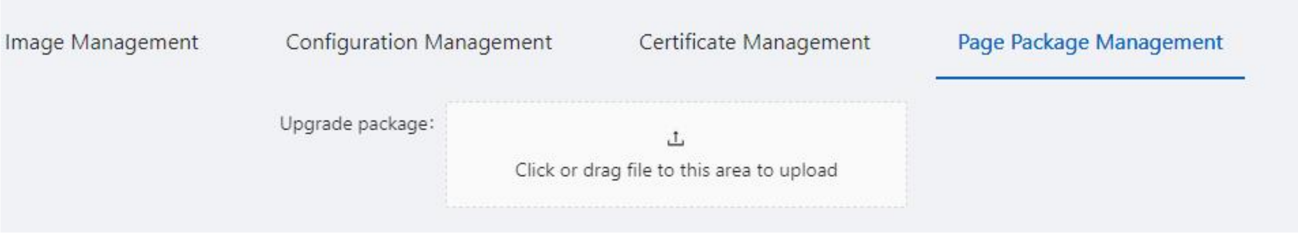
Figure 5-8 Configuration file management page



5.2.5 Page Package Management

The page package management module provides the ability to obtain the target page package file from the local host and apply the file as a device page package file, as shown in Figure 5-9.

Figure 5-9 Configuration file management page



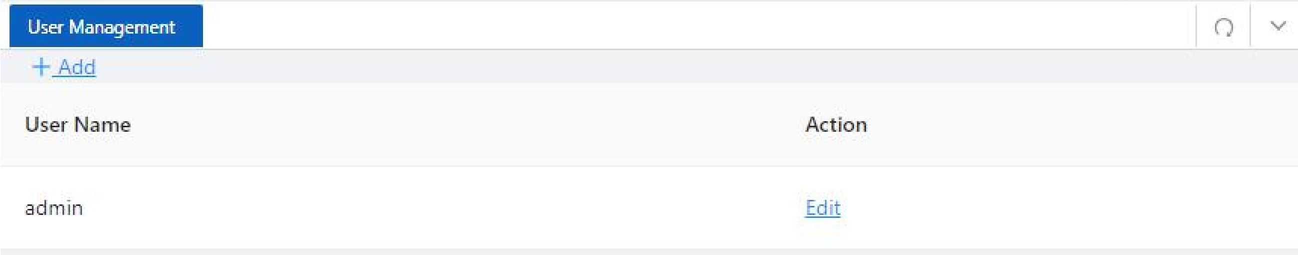
5.3 User Management

In the user management part, you can:

- Set the username, password.
- Create a new user.

Select **Maintenance** > **User Management** from the navigation area to enter the User Management page, as shown in Figure 5-10. Table 5-2 lists the configuration items of the user management.

Figure 5-10 User management page



User Name	Action
admin	Edit

Table 5-2 Account configuration items

Item		Description
Account	Name	User name
	Edit	Click to change the password
	Delete	Click to delete the user account
	+Add…	Click to create a new user

5.4 Time Management

The system time module allows you to display and set the device system time on the Web interface. The device supports setting system time through manual configuration and automatic synchronization of NTP server time.

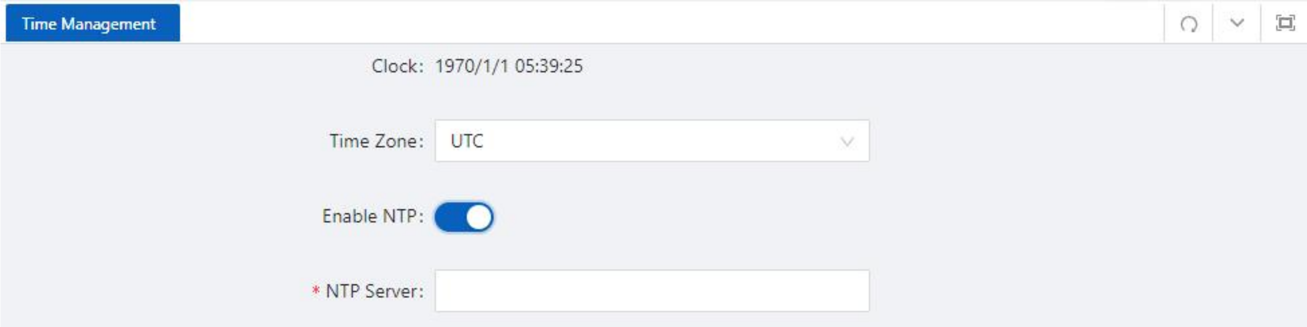
An administrator cannot keep time synchronized among all the devices within a network by changing the system clock on each device, because this is a time consuming task and cannot guarantee clock precision.

Defined in RFC 1305, the Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients. NTP allows quick clock synchronization within the entire network and ensures a high clock precision so that the devices can provide diverse applications based on consistent time.

5.4.1 View the System Time

Select **Maintenance** > **Time Management** from the navigation area to enter the Time Management page, as shown in Figure 5-11. The current system time and clock status are displayed. Table 5-3 shows the network time configuration items.

Figure 5-11 System time configuration page



Clock: 1970/1/1 05:39:25

Time Zone: UTC

Enable NTP: ●

* NTP Server:

Table 5-3 System time configuration items

Item	Description
Clock	System date and time
Time Zone	Choose time zone
Enable NTP	Enable/Disable NTP
NTP Server	Set the NTP server IP address

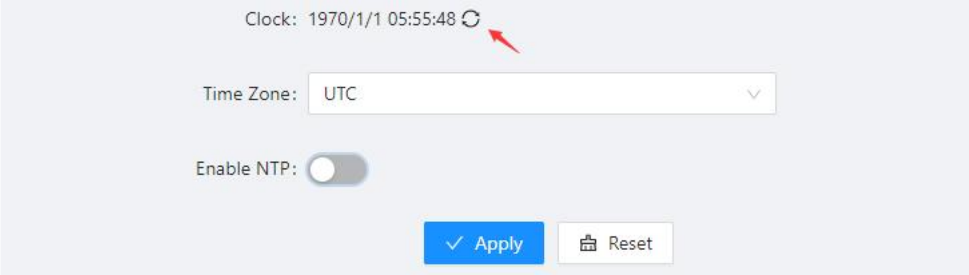
5.4.2 Configuring System Time

1. Select **Maintenance** > **Time Management** from the navigation area to enter Time Management page.

2. Click synchronous button ⟳ behind clock, then click **Apply** button, as shown in Figure 5-12. The time of the PC will be synchronized to the switch.

3. Click **Save** of the auxiliary area.

Figure 5-12 System time configuration page



Clock: 1970/1/1 05:55:48

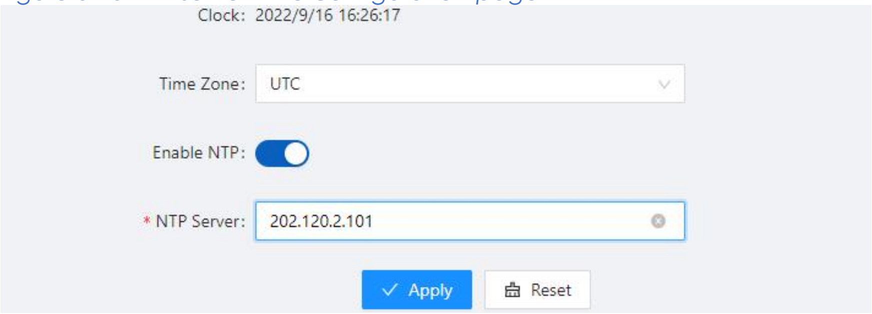
Time Zone: UTC

Enable NTP: ○

5.4.3 Configuring NTP Server

1. Select **Maintenance** > **Time Management** from the navigation area to enter Time Management page.
2. Enable NTP
3. Type **202.120.2.101** in the NTP Server IP box, as shown in Figure 5-13, click **Apply**.
4. Click **Save** of the auxiliary area.

Figure 5-13 NTP server time configuration page



Clock: 2022/9/16 16:26:17

Time Zone: UTC

Enable NTP: ●

* NTP Server: 202.120.2.101

5.5 SNMP

Simple Network Management Protocol (SNMP) offers the communication rules between a management device and the managed devices on the network; it defines a series of messages, methods, and syn taxes to implement the access and management from the management device to the managed devices. SNMP has the following characteristics:

- Automatic network management. SNMP enables network administrators to search and modify information, find and diagnose network problems, plan for network growth, and generate reports on network nodes.
- SNMP shields the physical differences between various devices and thus realizes automatic management of products from different manufacturers. Offering only the basic set of functions, SNMP makes the management tasks independent of both the physical features of the managed devices and the underlying networking technology. Thus, SNMP achieves effective management of devices from different manufacturers, especially in small, high-speed, and low-cost network environments.

SNMP Mechanism

An SNMP enabled network comprises Network Management Station (NMS) and agent.

- An NMS is a station that runs the SNMP client software. It offers a user-friendly interface, making it easier for network administrators to perform most network management tasks.
- An agent is a program on the device. It receives and handles requests sent from the NMS. Only under certain circumstances, such as interface state change, will the agent inform the NMS. NMS manages an SNMP enabled network, whereas agents are the managed network device. NMS and agents exchange management information through the SNMP protocol.

SNMP provides the following four basic operations:

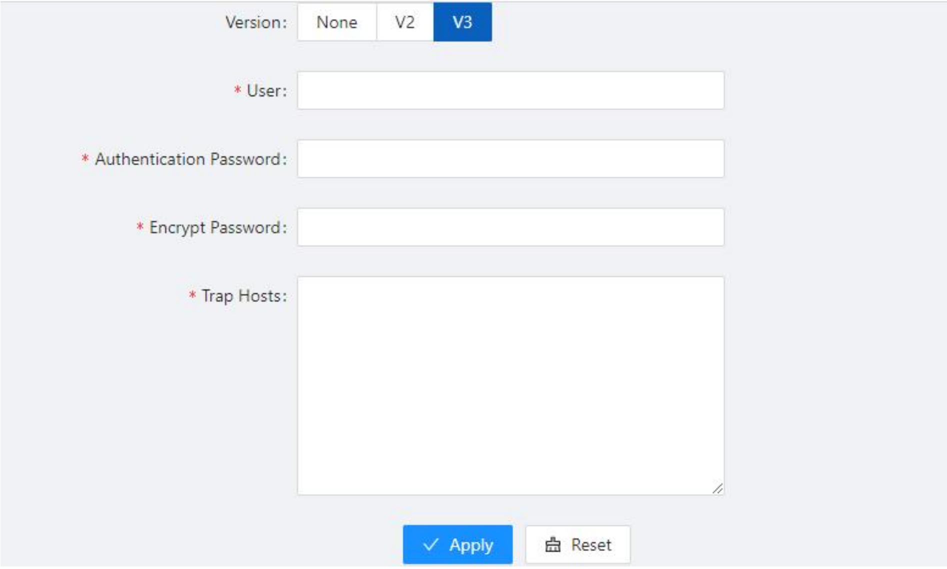
- Get operation: NMS gets the value of a certain variable of the agent through this operation.
- Set operation: NMS can reconfigure the value of one or more objects in the agent MIB (Management Information Base) by means of this operation.
- Trap operation: The agent sends traps to the NMS through this operation.
- Inform operation: The NMS sends traps to other NMSs through this operation.

SNMP Configuration

1. Select **Maintenance** > **SNMP** from the navigation area to enter the SNMP page, as shown in Figure 5-15.

2. Select the SNMP version, configure the user, authentication encryption password, Trap host, and click the **Apply** button to complete the configuration.

Figure 5-15 SNMP configuration page


Version: None V2 V3
* User:
* Authentication Password:
* Encrypt Password:
* Trap Hosts:

5.6 Syslog Server

5.6.1 Overview

During the operation of the device, various state changes such as link state UP, DOWN, etc. and also there will occur some events like abnormal handling and so on. The system log provides a serial of service that automatically generates messages in a fixed format during a status changes or an event happens, which are recorded on the device's log file. It can be displayed on the trunk port and remote login terminal, and can also be sent to 1~3 groups of log servers on the network for administrators to analyze the network conditions and locate the problems.

To facilitate administrator reading and management of log messages, these log messages can be time-stamped, and graded by the priority of log information.

5.6.2 Configuring Syslog Server

Select **Maintenance** > **Syslog Server** in the navigation area to enter the Syslog Server page, as shown in Figure 5-16, parameter instructions as shown in Table 5-4.

Figure 5-16 Syslog server configuration page

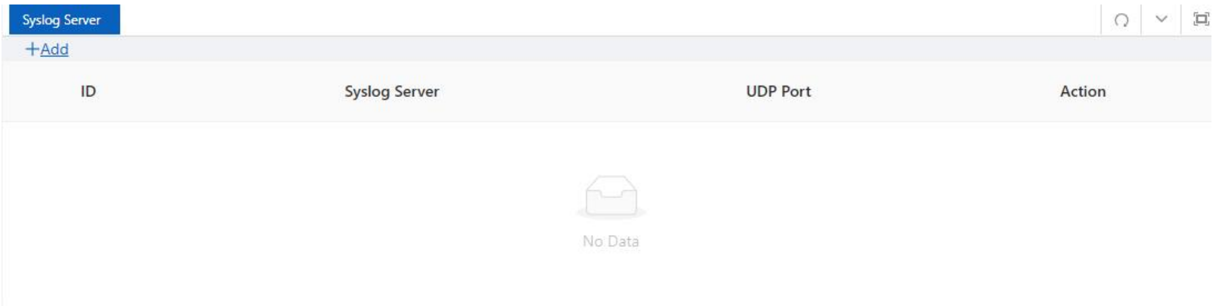


Table 5-4 Syslog server parameters

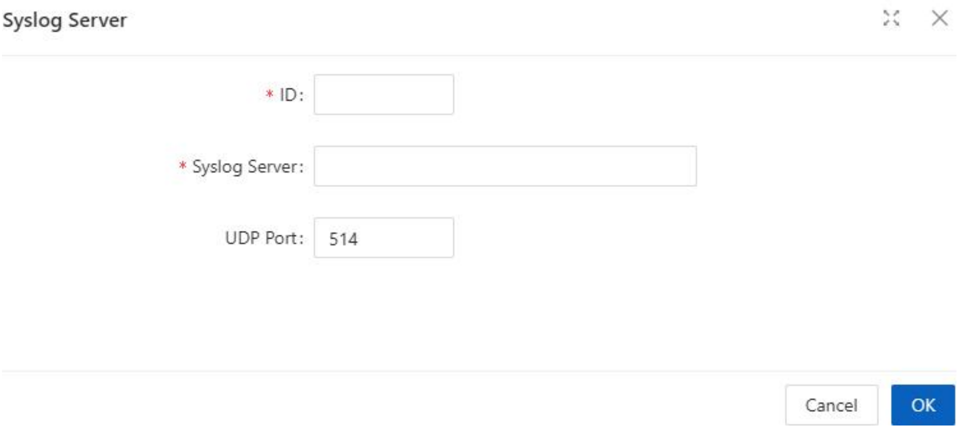
Item	Description
ID	The ID of the Syslog Server
Syslog Server	Configure the IP address of the remote server, and supports up to 3 remote server configurations
UDP port	Support remote server UDP protocol port configuration, range <1-65535>; default port number is 514 when UDP port isn't configured

Operating Steps

1. Select **Maintenance** > **Syslog Server** in the navigation area to enter the Syslog Server page.

2. Click the **+Add** button under Syslog Server to enter the creation page, fill in the parameters according to the requirements, as shown in Figure 5-17, and click the **OK** button to complete the configuration.

Table 5-17 Syslog server configuration page



Syslog Server

* ID:

* Syslog Server:

UDP Port: 514

A Configuration Example

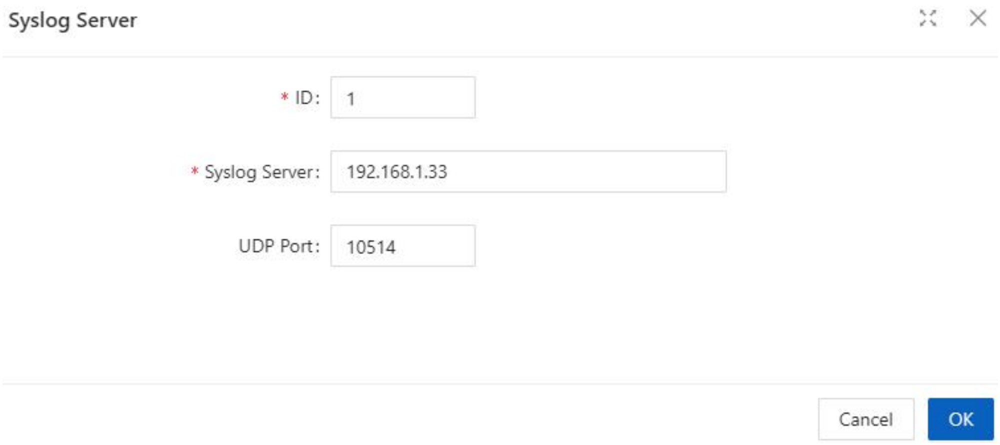
Device's syslog sends to the remote server and the device's IP is 192.168.1.240 while the remote server IP is 192.168.1.33, and the UDP port number is 10514.

1. Select **Maintenance** > **Syslog Server** in the navigation area to enter the Syslog Server page.

2. Click the +**Add** button under Syslog Server to enter the creation page, fill in the parameters according to the requirements, and click **OK** to complete the configuration, as shown in Figure 5-18.

3. Click the **Save** in the auxiliary area to save the configuration.

Figure 5-18 Syslog server configuration page



Syslog Server

* ID: 1

* Syslog Server: 192.168.1.33

UDP Port: 10514

6 Diagnosis

6.1 Network Utility

6.1.1 Overview

Ping

You can use the ping function to check whether a device with a specified address is reachable, and to examine network connectivity. A successful execution of the ping command involves the following steps:

1. The source device sends an ICMP echo request (ECHO-REQUEST) to the destination device.
2. The destination device responds by sending an ICMP echo reply (ECHO-REPLY) to the source device after receiving the ICMP echo request.
3. The source device displays related statistics after receiving the reply. Output of the ping command falls into the following:
   - The ping command can be applied to the destination's host name or IP address. If the destination's host name is unknown, the prompt information is displayed.
   - If the source device does not receive an ICMP echo reply within the timeout time, it displays the prompt information and the statistics during the ping operation. If the source device receives an ICMP echo reply within the timeout time, it displays the number of bytes of the echo reply, the message sequence number, Time to Live (TTL), the response time, and the statistics during the ping operation. Statistics during the ping operation include number of packets sent, number of echo reply messages received, percentage of messages not received, and the minimum, average, and maximum response time.

Traceroute

By using the traceroute command, you can display the Layer 3 devices involved in delivering a packet from source to destination. This function is useful for identification of failed node(s) in the event of network failure.

The traceroute command involves the following steps in its execution:

1. The source device sends a packet with a TTL value of 1 to the destination device.
2. The first hop (the Layer 3 device that first receives the packet) responds by sending a TTL-expired ICMP message to the source, with its IP address encapsulated. In this way, the source device can get the address of the first Layer 3 device.
3. The source device sends a packet with a TTL value of 2 to the destination device.
4. The second hop responds with a TTL-expired ICMP message, which gives the source device the address of the second Layer 3 device.

This process continues until the ultimate destination device is reached. In this way, the source device can trace the addresses of all the Layer 3 devices involved to get to the destination device.

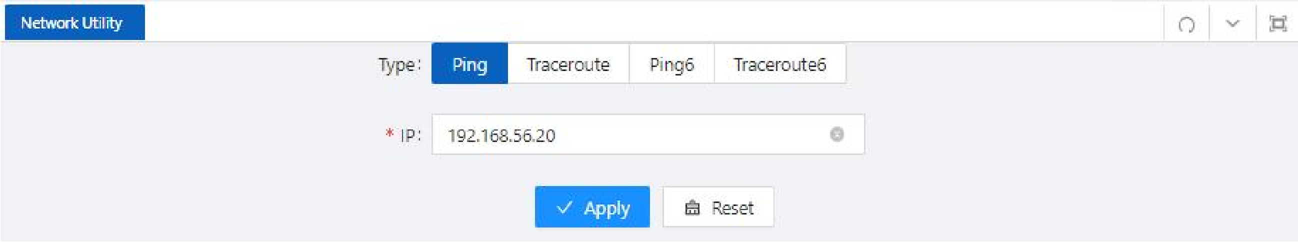
The traceroute command can be applied to the destination's host name or IP address. If the destination's host name is unknown, the prompt information is displayed

6.1.2 Diagnostic Tool Operations

Ping Operation

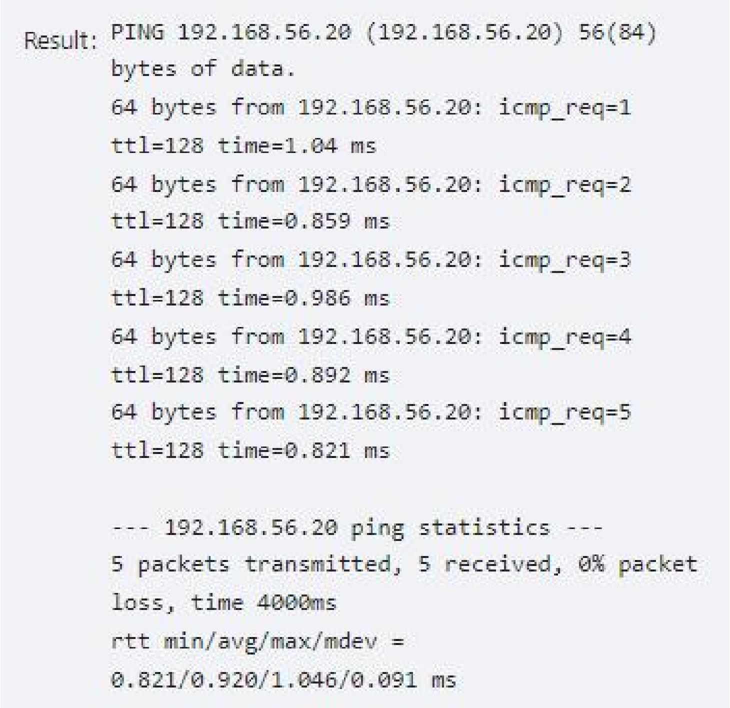
1. Select **Diagnosis** > **Network Utility** from the navigation tree to enter the IPv4&IPv6 Ping Configuration page.
2. Type the IPv4/IPv6 address of the destination device in the text box, as shown in Figure 6-1.
3. Click **PING** to execute the ping command, and you can see the result in the box below, as shown in Figure 6-2.

Figure 6-1 Network utility page



* IP: 192.168.56.20

Figure 6-2 The ping result



Result:

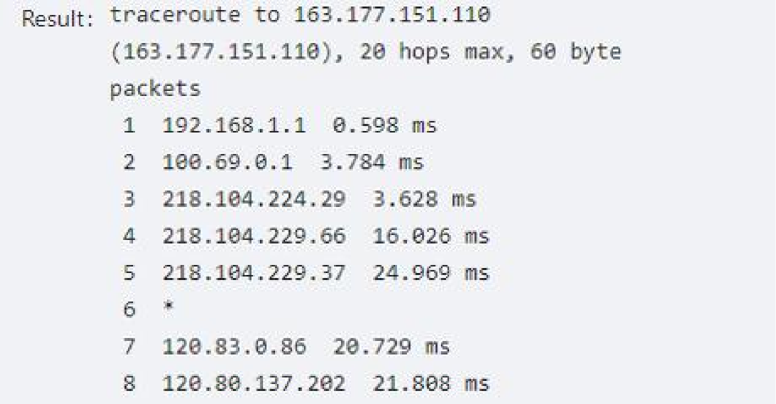
```
PING 192.168.56.20 (192.168.56.20) 56(84)
bytes of data.
64 bytes from 192.168.56.20: icmp_req=1
ttl=128 time=1.04 ms
64 bytes from 192.168.56.20: icmp_req=2
ttl=128 time=0.859 ms
64 bytes from 192.168.56.20: icmp_req=3
ttl=128 time=0.986 ms
64 bytes from 192.168.56.20: icmp_req=4
ttl=128 time=0.892 ms
64 bytes from 192.168.56.20: icmp_req=5
ttl=128 time=0.821 ms

--- 192.168.56.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet
loss, time 4000ms
rtt min/avg/max/mdev =
0.821/0.920/1.046/0.091 ms
```

The Traceroute Operation

1. Select **Diagnostic** > **Network Utility** from the navigation tree.
2. Type the destination IP address in the text box.

3. Click **Traceroute** to execute the trace route command, and you see the result in the box below, as shown in Figure 6-3.

Figure 6-3 The trace route result



```
Result: traceroute to 163.177.151.110
        (163.177.151.110), 20 hops max, 60 byte
        packets
         1  192.168.1.1  0.598 ms
         2  100.69.0.1  3.784 ms
         3  218.104.224.29  3.628 ms
         4  218.104.229.66  16.026 ms
         5  218.104.229.37  24.969 ms
         6  *
         7  120.83.0.86  20.729 ms
         8  120.80.137.202  21.808 ms
```

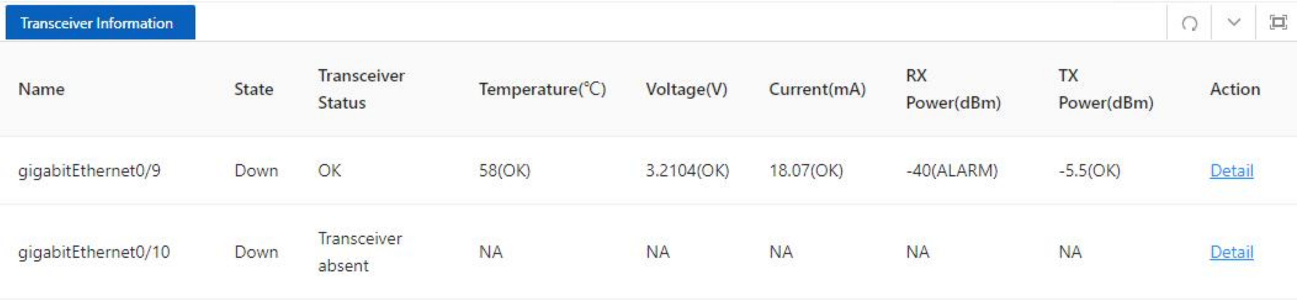
6.2 Optical Transceiver Information

Optical fiber is commonly used for long distance data transmission. However, when link issues occur, it is very costly to troubleshoot fiber cables and fiber transceivers at remote sites. To solve this problem, Moxa industrial Ethernet switches provide digital diagnostics and monitoring (DDM) functions on SFP optical fiber links and allow users to measure optical parameters and its performance from a central site. This function can greatly facilitate the troubleshooting process for optical fiber links and reduce costs for onsite debugging.

6.2.1 Displaying Optical Transceiver Information

Select **Diagnosis** > **Transceiver Information** from the navigation area. The system automatically displays the optical transceiver information, as shown in Figure 6-4. Table 6-1 describes the optical transceiver information items.

Figure 6-4 Optical transceiver information



Name	State	Transceiver Status	Temperature(℃)	Voltage(V)	Current(mA)	RX Power(dBm)	TX Power(dBm)	Action
gigabitEthernet0/9	Down	OK	58(OK)	3.2104(OK)	18.07(OK)	-40(ALARM)	-5.5(OK)	Detail
gigabitEthernet0/10	Down	Transceiver absent	NA	NA	NA	NA	NA	Detail

Table 6-1 Optical transceiver information items

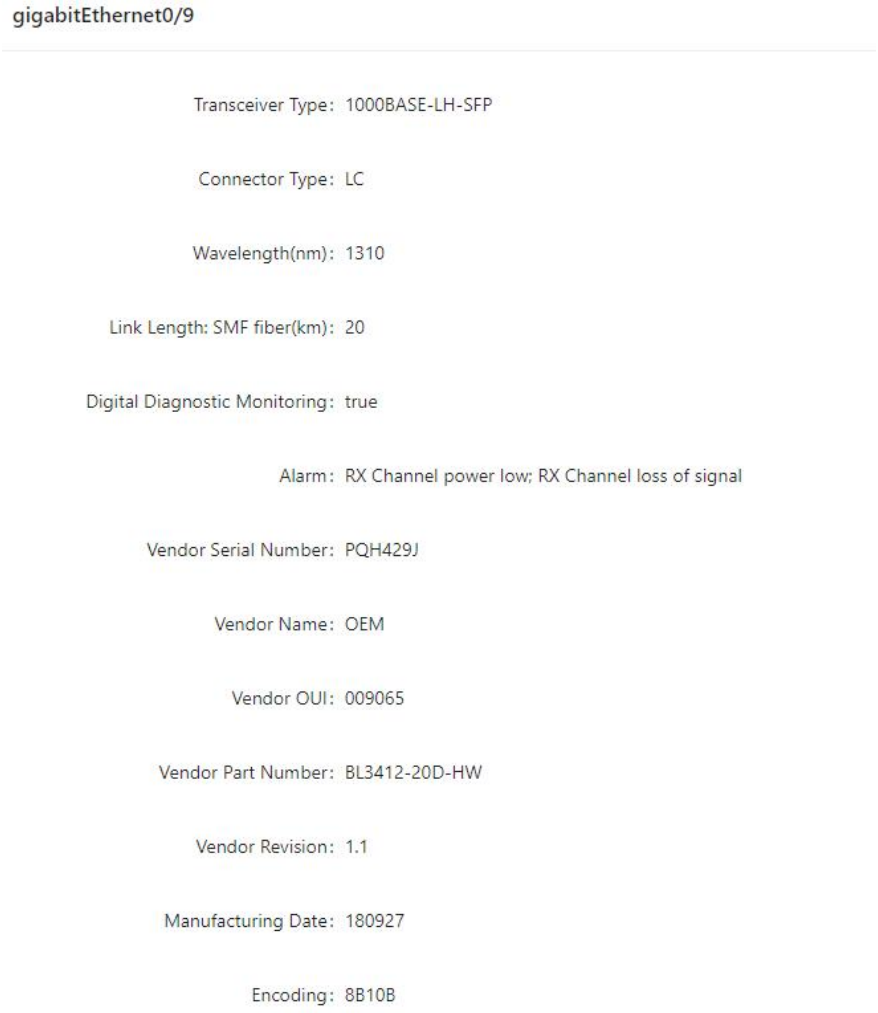
Item	Description
Name	Switch port number that the SFP is plugged into.
State	The state of the fiber interface, up/down.
Transceiver State	The absent of the transceiver.

Temperature(degree)	SFP casing temperature
Voltage(V)	Voltage supply to the transceiver.
Current(mA)	Current consumed by transceiver.
Rx Power(dBm)	The amount of light being received from the fiber optic cable
TX Power(dBm)	The amount of light being transmitted into the fiber optic cable
Detail	Click to show the detail information of the transceiver.

6.2.2 Displaying Detail Information

Click **Detail** interface to enter the Transceiver Detail Information page. as shown in Figure 6-5.

Figure 6-5 Transceiver detail information



gigabitEthernet0/9

Transceiver Type: 1000BASE-LH-SFP

Connector Type: LC

Wavelength(nm): 1310

Link Length: SMF fiber(km): 20

Digital Diagnostic Monitoring: true

Alarm: RX Channel power low; RX Channel loss of signal

Vendor Serial Number: PQH429J

Vendor Name: OEM

Vendor OUI: 009065

Vendor Part Number: BL3412-20D-HW

Vendor Revision: 1.1

Manufacturing Date: 180927

Encoding: 8B10B

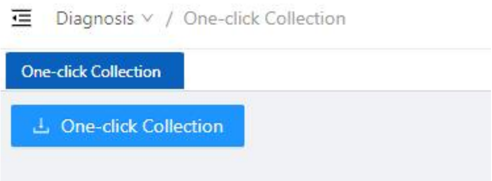
6.3 One-click Collection

Each functional module has its own running information, and generally, you need to view the output information for each module one by one. To receive as much information as possible in one operation during daily maintenance or when system failure occurs, the diagnostic information module allows you to save the running statistics of multiple functional modules to a file, and then you can locate problems faster by checking this file.

1. Select **Diagnosis** > **One-click Collection** from the navigation area to enter the page as shown in Figure 6-6.

2. When you click **One-click Collection** button, the system begins to generate the diagnostic information file, and after the file is generated, the File Download dialog box appears. You can save this file to the local host.

Figure 6-6 Backup log page



6.4 Dying Gasp

6.4.1 Overview

The networking devices rely on a temporary back-up power supply on a capacitor, that allows for a graceful shutdown and the generation of the dying-gasp message. This temporary power supply is designed to last from 10 to 20 milliseconds to perform these tasks.

According to the definition in 802.3ah, when a device power failure event occurs, the device sends an OAM event message to its connected device. Since OAM is a point-to-point protocol, the power failure event message will not be sent to the next device that supports OAM. Continue to forward again. The device that receives a power failure event will output a power failure LOG prompt message.

In addition to the OAM alarm information, the power-off device will also send a trap message to the SNMP server.

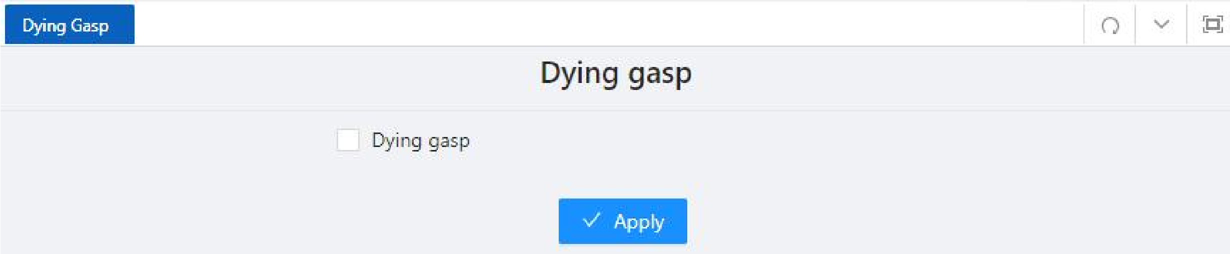
Node information	Data
Mib files	DOT3-OAM-MIB.mib
Oid	1, 3, 6, 1, 2, 1, 158, 1, 6, 1, 4
Value	DyingGaspEvent(257)

6.4.2 Configuring Dying Gasp

1. Select **Diagnosis** > **Dying Gasp** from the navigation area to enter the Dying Gasp Configuration page, as shown in Figure 6-7.

2. Select the box of dying gasp, click **Apply** button to enable dying gasp.

Figure 6-7 Dying gasp configuration page



Dying gasp

□ Dying gasp

✓ Apply

6.5 Cable Detect

Note

Only electrical ports support this command

Performing this operation will cause the already Up port to automatically go Down and Up again.

When the line length is less than 6 meters, there is a deviation between the test results and the actual value.

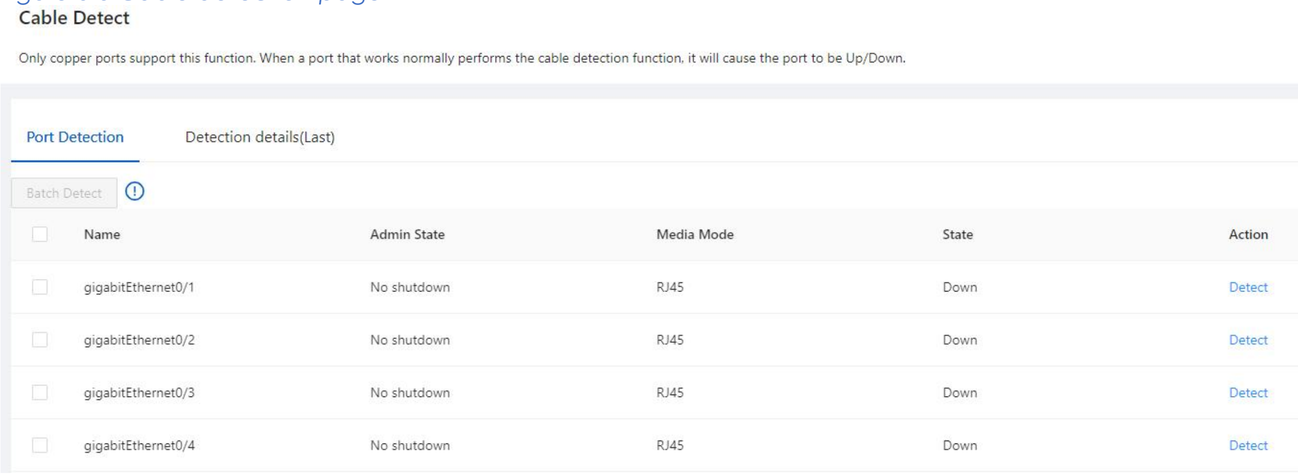
Cable detection means that users can detect the current status of the cable connected to the Ethernet interface on the device, and the system will return the detection results within 5 seconds. The detection content includes whether there is a short circuit or open circuit in the cable and the length of the faulty cable.

Step 1: Select **Diagnosis** > **Cable Detect** in the navigation bar to enter the Cable Detection page, as shown in Figure 6-8.

Step 2: Select the interface to be tested, click the **Detect** button to start the incoming line test, and the system will return the test results within 5 seconds.

Step 3: As shown in Figure 6-9, view the detection results on the pop-up page.

Figure 6-8 Cable detection page

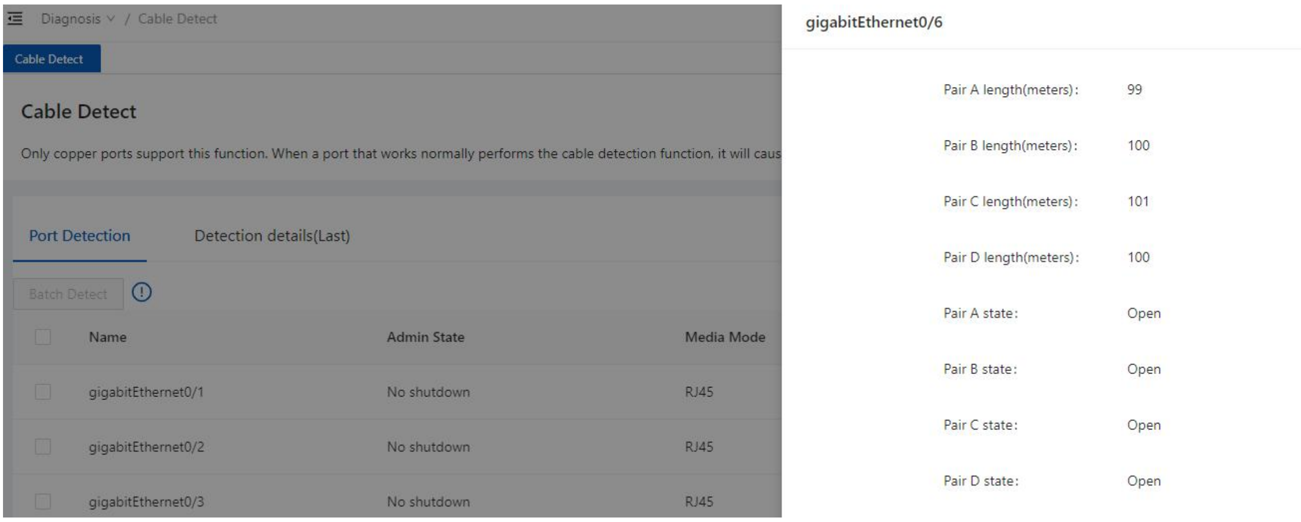


Cable Detect

Only copper ports support this function. When a port that works normally performs the cable detection function, it will cause the port to be Up/Down.

□	Name	Admin State	Media Mode	State	Action
□	gigabitEthernet0/1	No shutdown	RJ45	Down	Detect
□	gigabitEthernet0/2	No shutdown	RJ45	Down	Detect
□	gigabitEthernet0/3	No shutdown	RJ45	Down	Detect
□	gigabitEthernet0/4	No shutdown	RJ45	Down	Detect

Figure 6-9 Detection results



Cable Detect

Only copper ports support this function. When a port that works normally performs the cable detection function, it will caus

	Name	Admin State	Media Mode
□	gigabitEthernet0/1	No shutdown	RJ45
□	gigabitEthernet0/2	No shutdown	RJ45
□	gigabitEthernet0/3	No shutdown	RJ45

gigabitEthernet0/6

Pair A length(meters):	99
Pair B length(meters):	100
Pair C length(meters):	101
Pair D length(meters):	100
Pair A state:	Open
Pair B state:	Open
Pair C state:	Open
Pair D state:	Open

Note

Pair X length: unit meter, cable length, in case of fault, the length from the interface to the fault location

Pair X status:

OK (normal): Indicates that the line pair (PAIR) is terminated normally

Open: Indicates that the line pair is open

Short: Indicates a short circuit on the pair

Unknown: Other unknown causes of failure