8-way Gigabit PoE port+2-way Gigabit SFP slot

Layer 2 Managed Industrial Ethernet Switch

User Manual

Document Version: 02

Issue Date: 10/09/2023

Preface

This Switch User Manual has introduced:

- Product features
- Product network management configuration
- Overview of related principles of network management

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Port Convention

The port number in this manual is only an example, and does not represent the actual port with this number on the device. In actual use, the port number existing on the device shall prevail.

Text Format Convention

Format	Description
" "	Words with “” represent the interface words. Fox example: “Port number”.
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: ‘Light Blue’.
About this chapter	The section ‘about this chapter’ provide links to various sections of this chapter, as well as links to the Principles

Format	Description
	Operations Section of this chapter.

Symbols

Format	Description
 Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
 Note	Conduct a necessary supplements and explanations for the description of operation content.
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Button Operation Convention

Format	Description
	There is a logout button in the upper right corner of the webpage. After clicking it, the webpage returns to the login page.
	There is a port button in the upper right corner of the webpage. Click or press F2 to view the port status, and press F2 or Esc to close the port status page.
	There is a restart button in the upper right corner of the webpage. After clicking, a restart confirmation box pops up. After confirmation, the device will restart.
	There is a Save button in the upper right corner of the webpage. Click it to save the current device configuration. After setting the device, the save icon will flash to remind the user to save the configuration, so as to avoid losing unsaved configuration information due to restart and other operations.
	Click the Add button to add a line of configuration. Note that repeated configuration may result in data overwrite.
	Check the line to be deleted, and then click the Delete button to delete the configuration.

Format	Description
Config	Check the line to be configured, and then click the configure button to enter the configuration page.
	Click the function status button to switch the function status,  means on and  means off.
Apply	Click the Set button to submit the current configuration.
Clear	Click the “Clear” button to clear the information of current page.
Refresh	Click the Refresh button to refresh the information of current page.

Revision Record

Version No.	Date	Revision note
01	3/20/2023	Product release
02	6/09/2023	PoE product release

Content

1 Login the WEB Interface

1.1 System Requirements for WEB Browsing

Using this device, the system should meet the following conditions.

Hardware and Software	System requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	256 colors or above
Browser	Internet Explorer 9.0 or above
Operating system	Windows 7/8/10 or above

1.2 Setting IP Address of PC

The default management IP address of the device as follows:

IP Settings	Default Value
IP Address	192.168.1.254
Subnet mask	255.255.255.0

When configuring a device through the Web:

- Before conducting remote configuration, please confirm the route between computer and device is reachable.
- Before making a local configuration, make sure that the IP address of the computer and the serial server are on the same subnet.

Note:

While configuring the device for the first time, if it's the local configuration mode, first confirm the network segment of current PC is 1.

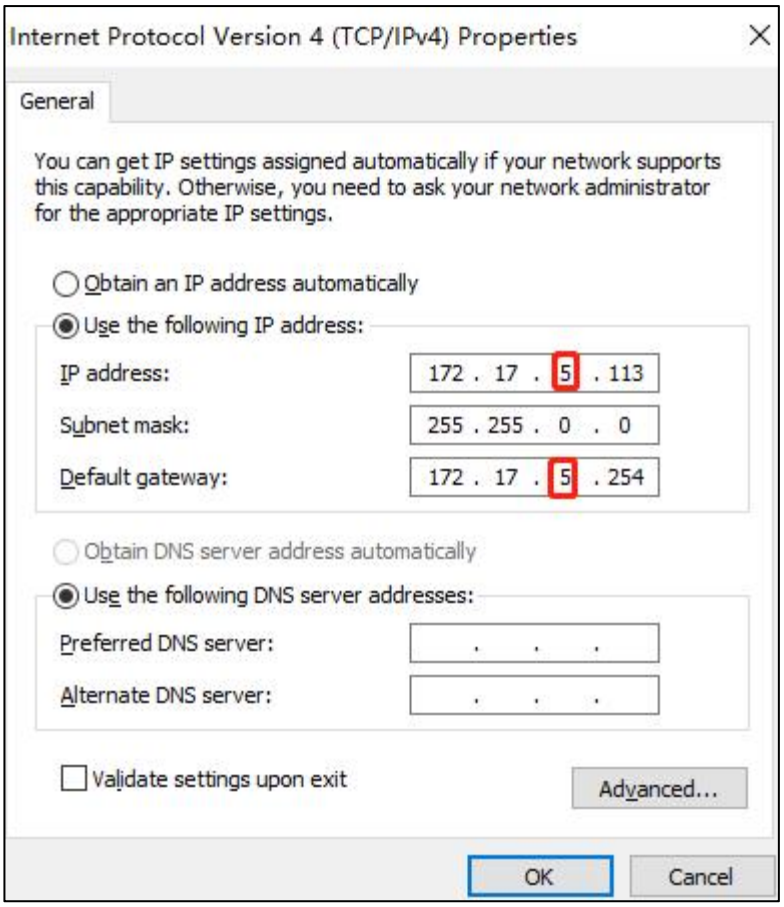
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follow:

Step 1 Open "Control Panel> Network Connection> Local Area Connection> Properties> Internet Protocol Version 4 (TCP / IPv4)> Properties".

Step 2 Change the selected "5" in red frame of the picture below to "1".



Step 3 Click “OK”, IP address is modified successfully.

Step 4 End.

1.3 Log in to the WEB Configuration Interface

Operation Steps

Log in to the WEB configuration interface as follows:

Step 1 Run the computer browser.

Step 2 Enter the address of the device "http://192.168.1.254" in the address bar of the browser.

Step 3 Click the “Enter” key.

Step 4 Pop-up dialog box as shown below, enter the user name and password in the login window.

Note:

- The default username and password are “admin123”; please strictly distinguish capital and small letter while entering.
- Default user account has the administrator privileges.
- When the user has not operated the Web network management configuration page for a long time, the system will log out and return to the Web login page after timeout; By default, the timeout of Web page login is 15 minutes.
- When the number of consecutive password login errors of a user reaches the limit (default is 5 times), the user will be restricted from logging in for the following time (default is 10 minutes).

Step 5 Click "Login".

Step 6 End.

After successful login, you can configure the relevant parameters and information of the WEB interface as needed.

2 System Information

Function Description

View port status such as port type and connection status.

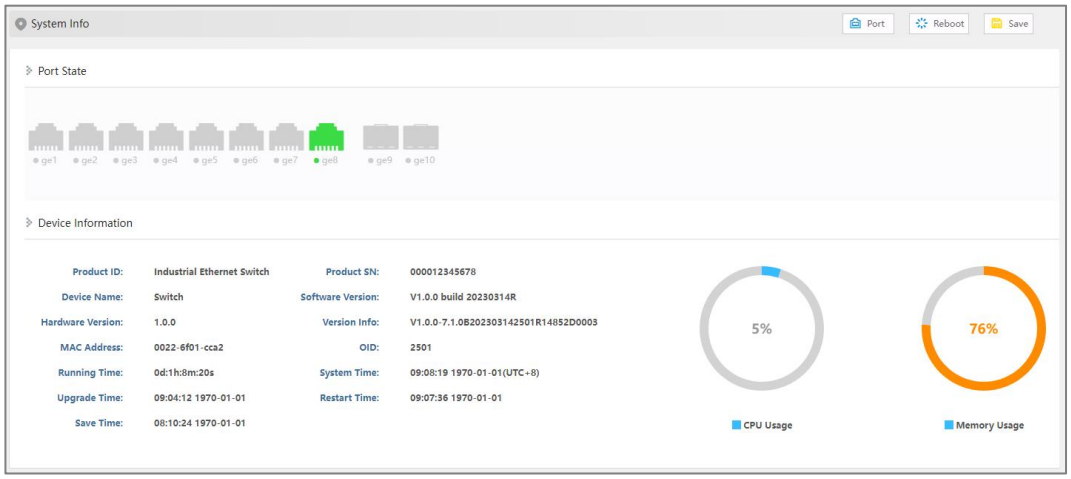
Check device information such as product model, software and hardware version, etc.

Operation Path

Open in the navigation bar: “System Information”.

Interface Description

System information interface as follows:



The main element configuration description of state information interface:

Interface Element	Description
Port State	Display port icon and port connection status of the device: •  Copper port icon, highlighting indicates that the port is connected. • Copper port icon, grayed out indicates that the

Interface Element	Description
	port is not connected or disabled. •  Fiber port icon, highlighting indicates that the port is connected. • Fiber port icon, grayed out indicates that the port is not connected or disabled.
Device information	Basic information of software, hardware and operation of the device. • Product ID • Device Name • Hardware Version • MAC Address • System Time • Restart Time • Product SN • Software Version • Version Information • OID • Uptime • Upgrade Time • Save Time • CPU Usage • Memory Usage

3 Login Configuration

3.1 IP Address

3.1.1 IPv4

Function Description

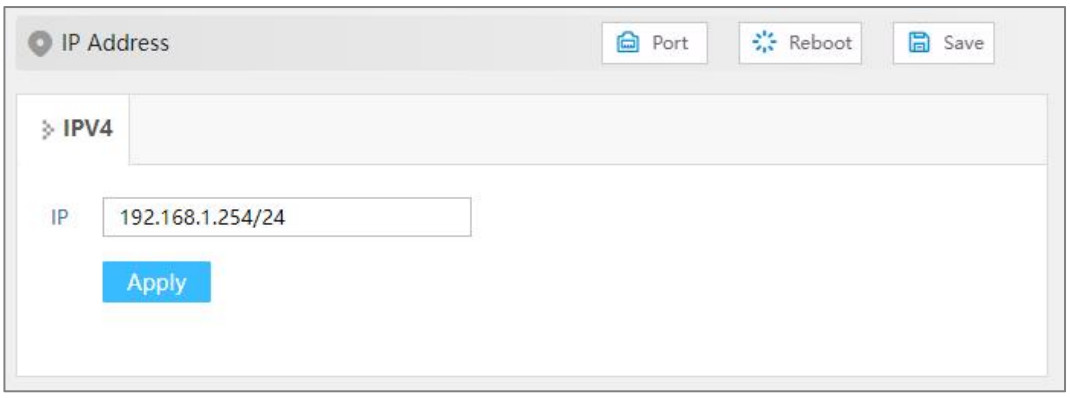
Configure the IPv4 address of the vlanif1 interface.

Operation Path

Open in order: "Login Configuration > IP Address > IPV4".

Interface Description

The IPV4 interface is as follows:



Main elements configuration descriptions of IPV4 interface:

Interface Element	Description
IP	The IPv4 address and subnet mask of the vlanif1 interface of the device. The default IP is 192.168.1.254/24. Note:

Interface Element	Description
	After modifying the IP of the device, re-enter the corresponding IP address to access the WEB interface.

3.2 Users

Function Description

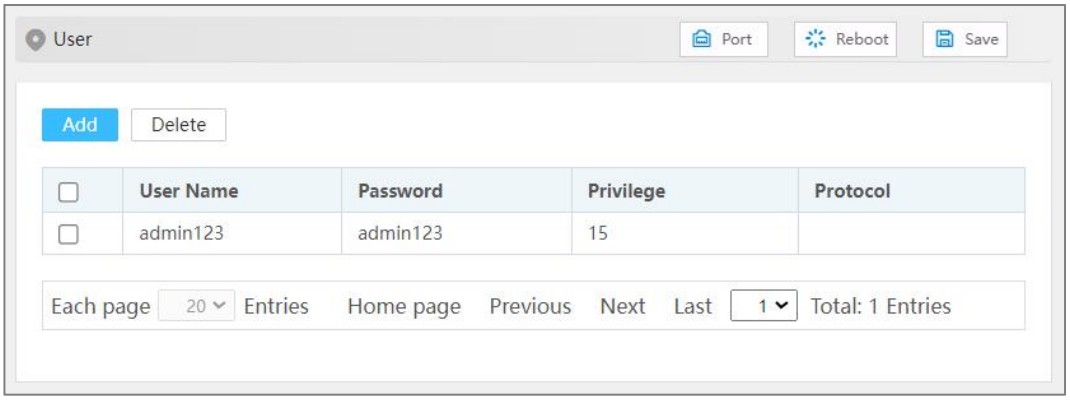
To add and delete user, user needs to enter username and password to access the device, the initial username and password are: admin123.

Operation Path

Open in order: "Login Configuration > User".

Interface Description

User interface as follows:



The main element configuration description of user interface:

Interface Element	Description
Username	Identification of the visitor. Note: • User name supports 1-16 valid characters, consisting of uppercase letters, lowercase letters, numbers or special characters (! @ _-). • User name does not support sensitive characters such as root, daemon, bin, sys, sync, mail, proxy, www-data, backup, operator, haldaemon, dbus, ftp, nobody, sshd, default, etc.
Password	Password used by the visitor. Note: • Password supports 8-16 valid characters, consisting of combination of two or more of uppercase letters, lowercase letters, numbers, special characters (~! @ # $% _-.).

Interface Element	Description
	• The password is valid for 90 days by default, and the password needs to be revised after it expires.
Privilege	The visitor's privilege is 0-15, and it supports 16 priorities in 4 categories. • 0: visit level; You can only view the system information, IP address and log information of the device, and conduct network diagnosis (Ping, Traceroute). • 1: view level; The configuration information of the device can be viewed, but the configuration of the device cannot be modified. • 2: configuration level; User can view the configuration information of the device and configure some functional parameters of the device, but cannot manage the device. • 3-15: manage level, user has all privileges of the device, including downloading, uploading, rebooting, modifying device information and other other operations. Notice: • Users can view, delete, or add other users whose priority does not exceed their own. • If the added user name already exists, the original user information will be overwritten.
Protocol	User protocol type, the options are as follows: • SSH: support SSH login. • Telnet: support Telnet login. • None: SSH and Telnet login are not supported.

3.3 Protocol Authorization

Function Description

Configure device TELNET service and SSH service.

The CLI interface of the device can be accessed through TELNET protocol and SSH2.0 protocol. TELNET transmission process uses TCP protocol for plaintext transmission, and SSH (Secure Shell) protocol provides secure remote login, ensuring the safe transmission of data.

Operation Path

Open in order: "Login Configuration > Protocol Authorization".

Interface Description

Protocol authorization interface is as below:

Configuration description of main elements of the protocol authorization interface:

Interface Element	Description
Telnet enable	TELNET service enable switch button, which is enabled by default.
SSH enable	SSH service enable switch button, which is disabled by default.

4 Port Configuration

4.1 Port Settings

Function Description

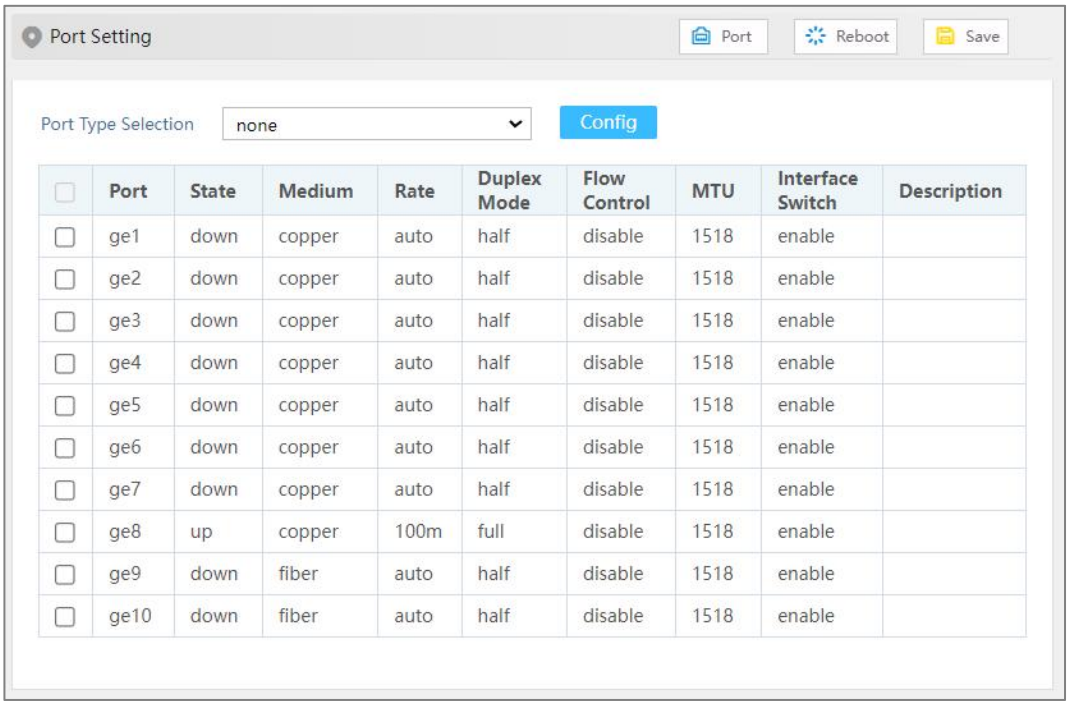
Set port parameters individually or in batches.

Operation Path

Open in order: "Port Configuration > Port Setting".

Interface Description

Port setting interface as follows:



Port	State	Medium	Rate	Duplex Mode	Flow Control	MTU	Interface Switch	Description
ge1	down	copper	auto	half	disable	1518	enable	
ge2	down	copper	auto	half	disable	1518	enable	
ge3	down	copper	auto	half	disable	1518	enable	
ge4	down	copper	auto	half	disable	1518	enable	
ge5	down	copper	auto	half	disable	1518	enable	
ge6	down	copper	auto	half	disable	1518	enable	
ge7	down	copper	auto	half	disable	1518	enable	
ge8	up	copper	100m	full	disable	1518	enable	
ge9	down	fiber	auto	half	disable	1518	enable	
ge10	down	fiber	auto	half	disable	1518	enable	

Main elements configuration description of port settings interface:

Interface Element	Description
Port type selection	Select ports of the same type in batches for configuration, and the options are as follows: • none • fe:100M port • ge: Gigabit port • xe: 10Gigabit port • sa: static aggregation group • po: dynamic aggregation group Note: The port type is based on the actual port of the device.
Port	The corresponding port name of the device Ethernet port.
State	Ethernet port connection status, display status as follows: • down: represent the port is disconnected; • up: represent the port is connected.
Medium	The connection types of Ethernet ports, the status are shown as follows: • fiber: fiber port medium. • copper: copper port medium.
Rate	The default is self-adaption mode, and the display status is as follows: • auto: self-adaption; • 10m: 10M; • 100m: 100M; • 1g: Gigabit.
Duplex Mode	The default is self-adaption mode, and the display status is as follows: • auto: self-adaption; • half: half-duplex • full: full duplex
Flow Control	Port flow control status, the display status is as follows: • disable • Both: Enable port data sending or receiving flow control.
Max-Frame	Ethernet port transmitted maximum data frame length, the value range is 64-10240.
Interface switch	Enable or disable Ethernet port. Options are as follows: • enable • disable
Description	Port description information, which supports 0-32 characters

Interface Element	Description
	and consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).

4.2 Link Aggregation

4.2.1 Link Aggregation

Function Description

Link aggregation is the shorter form of Ethernet link aggregation; it binds multiple Ethernet physical links into a logical link, achieving the purpose of increasing the link bandwidth. At the same time, these bundled links can effectively improve the link reliability by mutual dynamic backup.

The Link Aggregation Control Protocol (LACP) protocol based on the IEEE802.3ad standard is a protocol for implementing dynamic link aggregation. Devices running this protocol exchange LACPDU (Link Aggregation Control Protocol Data Unit, Link Aggregation Control Protocol Data Unit) to exchange link aggregation related information.

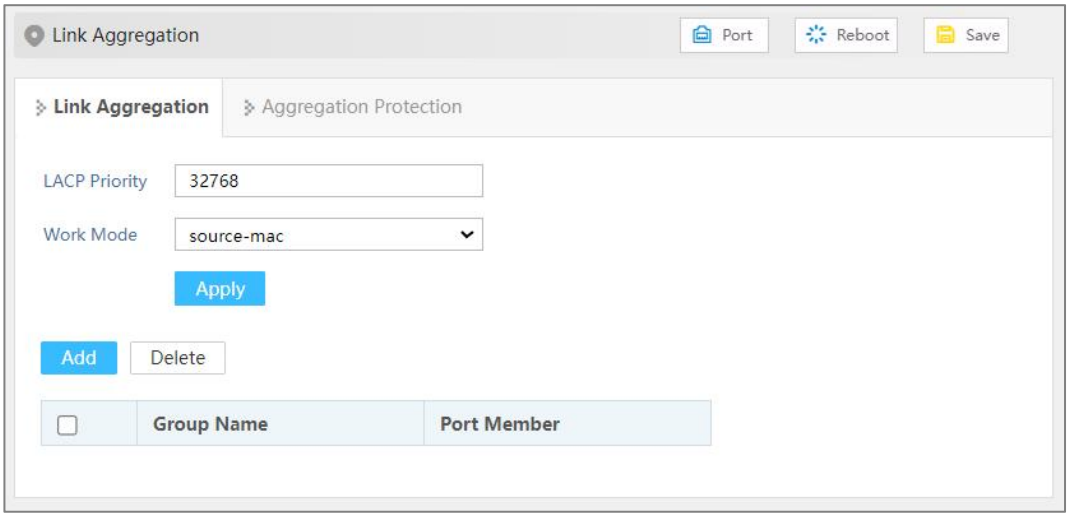
Based on the enabling or disabling of LACP protocol, the link aggregation can be divided into two modes, static aggregation and dynamic aggregation.

Operation Path

Open in order: "Port Configuration > Link Aggregation > Link Aggregation".

Interface Description

Link Aggregation interface as below:



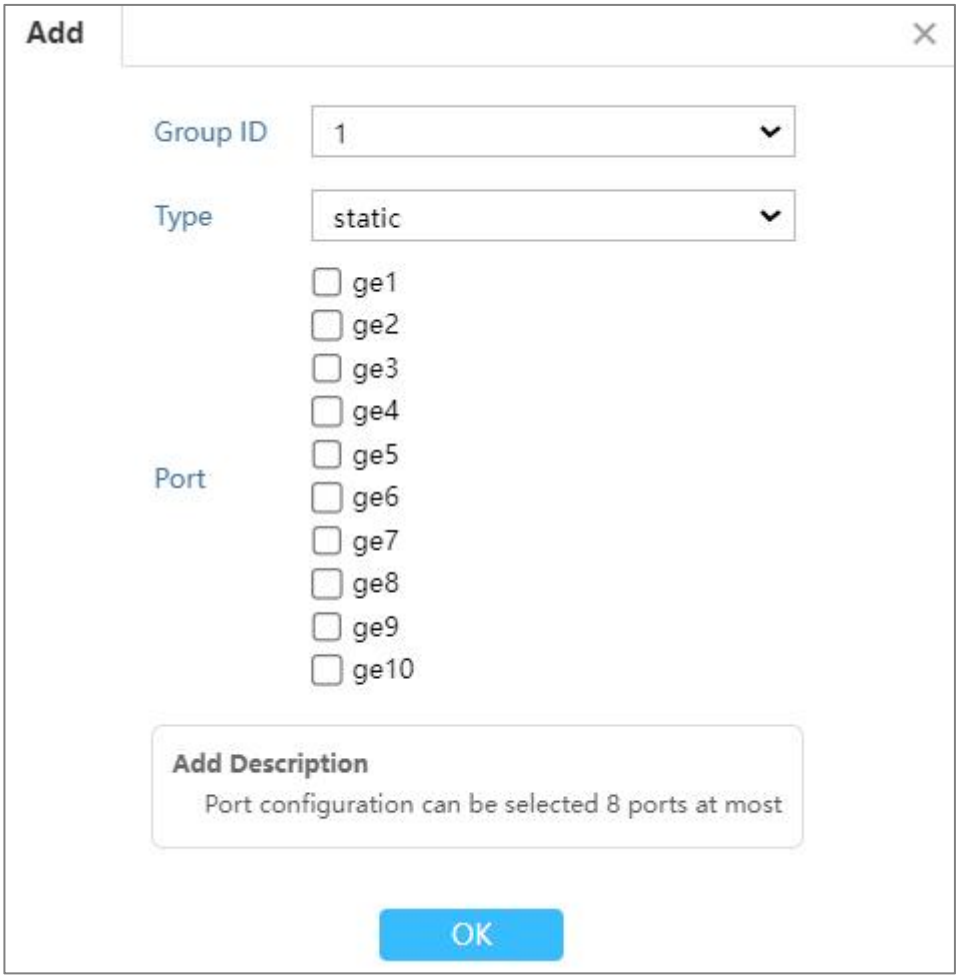
The main element configuration description of Link Aggregation interface:

Interface Element	Description
LACP Priority	Priority level setting of dynamic aggregation system, the setting range is 1-65535, defaults to 32768. Note: The lower the priority value of the system LACP is, the higher the priority is, and the activity interface of the device with high system priority is selected at both ends of the aggregation link.
Work Mode	Configure the load balancing mode of the aggregation group. The options are as follows: • destination-mac: Load balance mode based on destination MAC • destination-ip: the load balancing mode based on destination IP • destination-port: the load balancing mode based on destination TCP/UDP ports • source-mac: Load balance mode based on source MAC • source-ip: the load balancing mode based on source IP • source-port: the load balancing mode based on source TCP/UDP ports • source-dest-ip: Load balance mode based on source and destination IP • source-dest-mac: Load balance mode based on source and destination MAC • source-dest-port: The load balancing mode is based on the source and destination TCP/UDP ports.
Group Name	Group type and ID, sa is a static aggregation group, po is a dynamic aggregation group, and the aggregation group ID supports up to 12 groups. Each group can configure up to 8

Interface Element	Description
	ports to join aggregation.
Port Member	Port member in the link aggregation group.

Interface Description: Add

The Link Aggregation-Add interface as follows:



The main elements configuration description of Link Aggregation-Add interface:

Interface Element	Description
Group ID	The ID number of the aggregation group, which can support up to 12 groups.
Type	Type of aggregation group: • static: static aggregation • dynamic: dynamic aggregation
Aggregation Mode	Dynamic Aggregation Group Mode: • active: active mode, in which the port actively initiates the aggregation negotiation process.

Interface Element	Description
	• passive: the mode in which the port passively receives the aggregate negotiation process. Note: Under dynamic type, display this configuration.
Port	Port members in this aggregation group. Each group can configure up to 8 ports to join the aggregation.

4.2.2 Aggregation Protection

Function Description

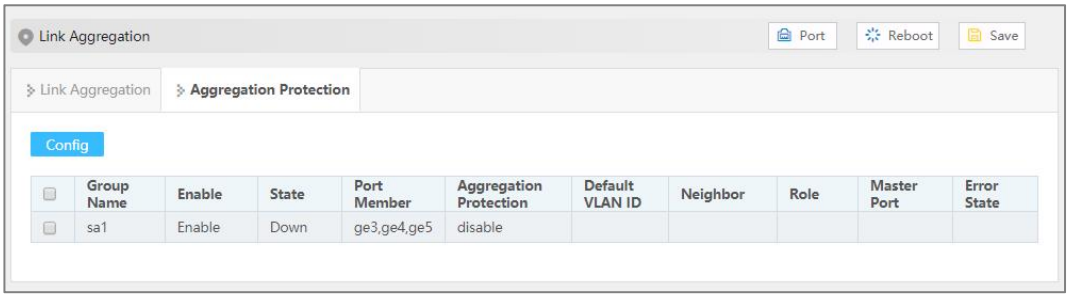
Configure static aggregation protection.

Operation Path

Open in order: "Port Configuration > Link Aggregation > Aggregation Protection".

Interface Description

The aggregation protection interface is shown as follows:



Description of configuration of main elements of aggregation protection interface:

Interface Element	Description
Group Name	The name of the static aggregation group set in Link Aggregation.
Enable	The enabled state of the aggregation group. • Enable • Disable
State	Status of the aggregation group port. • Up: as long as any port member is Up, the status of the aggregation group is up; • Down: if all port members are Down, the status of the aggregation group is Down.
Port Member	Port member in the aggregation group.

Interface Element	Description
Aggregation Protection	The enabled state of the aggregation protection. • Enable • Disable
Default VLAN ID	The VLAN where that aggregate group port reside.
Neighbor	MAC address of the opposite device of aggregation group. Note: If no device is connected to the opposite end, the MAC address is displayed as 0000.0000.0000.
Role	Elected roles in this device and the opposite device • Master: the one with a smaller MAC address is elected as Master • Slave: the one with a larger MAC address is elected as Slave
Master Port	The second link port of the master device is the master port.
Error State	Error message prompt of aggregation protection: • Neighbor timed out • Loop: forming a loop • Link error (such as generating a large number of error frames).

4.3 Port Rate Limit

Function Description

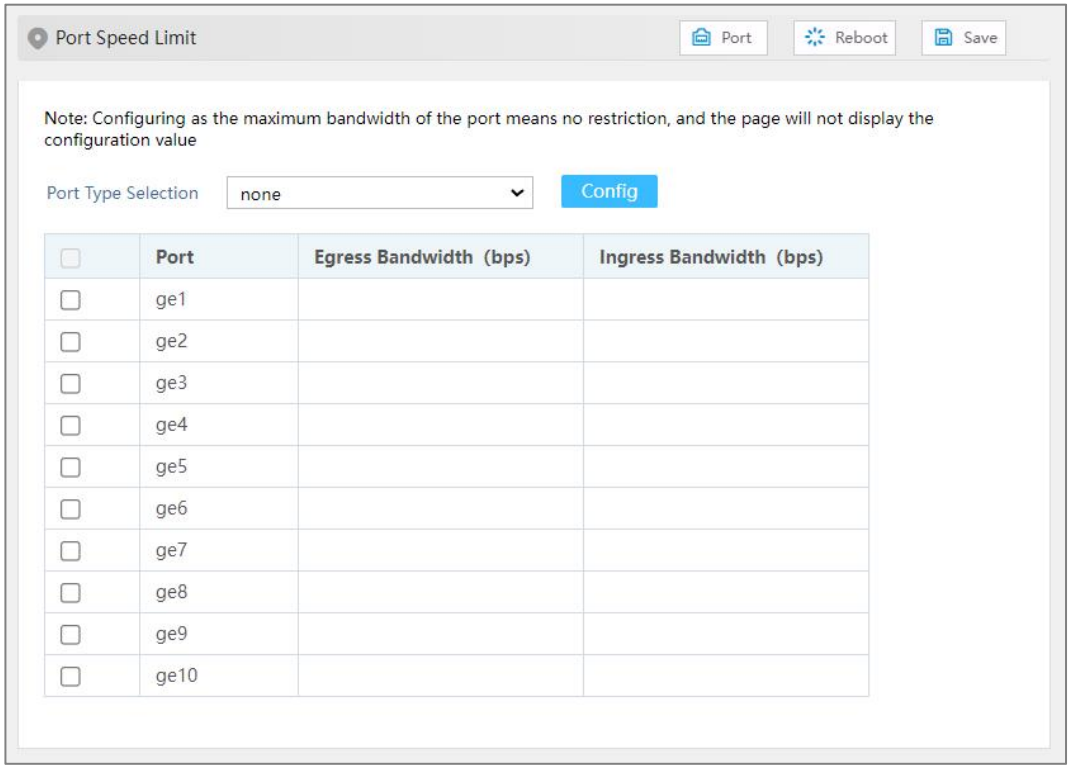
Limit the egress bandwidth and ingress bandwidth of the port.

Operation Path

Open in order: "Port Configuration > Port RateLimit".

Interface Description

Port rate limit interface as follows:



The main element configuration description of port rate limit interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Egress Bandwidth (bps)	The limitation of port on the bandwidth of egress data transmission.
Ingress Bandwidth (bps)	The limitation of port on the bandwidth of ingress data transmission. Note: Support unit selection of K/M/G when configuring the bandwidth. In WEB display, unit conversion will be conducted and similar values will be taken according to the input value and the unit.

Note

- When using the port rate limit, flow control should be enabled, otherwise the rate between devices will no longer be a smooth curve;
- When using the port rate limit, packet loss should not occur unless the flow control is disabled. The representation of packet loss is the fluctuating transmission speed.
- Port speed limit has high requirements on network cable quality, otherwise lots of conflict packets and broken packet would appear.

4.4 Storm Suppression

Function Description

Configure the maximum broadcast, multicast or unknown unicast packet flow the port allows.

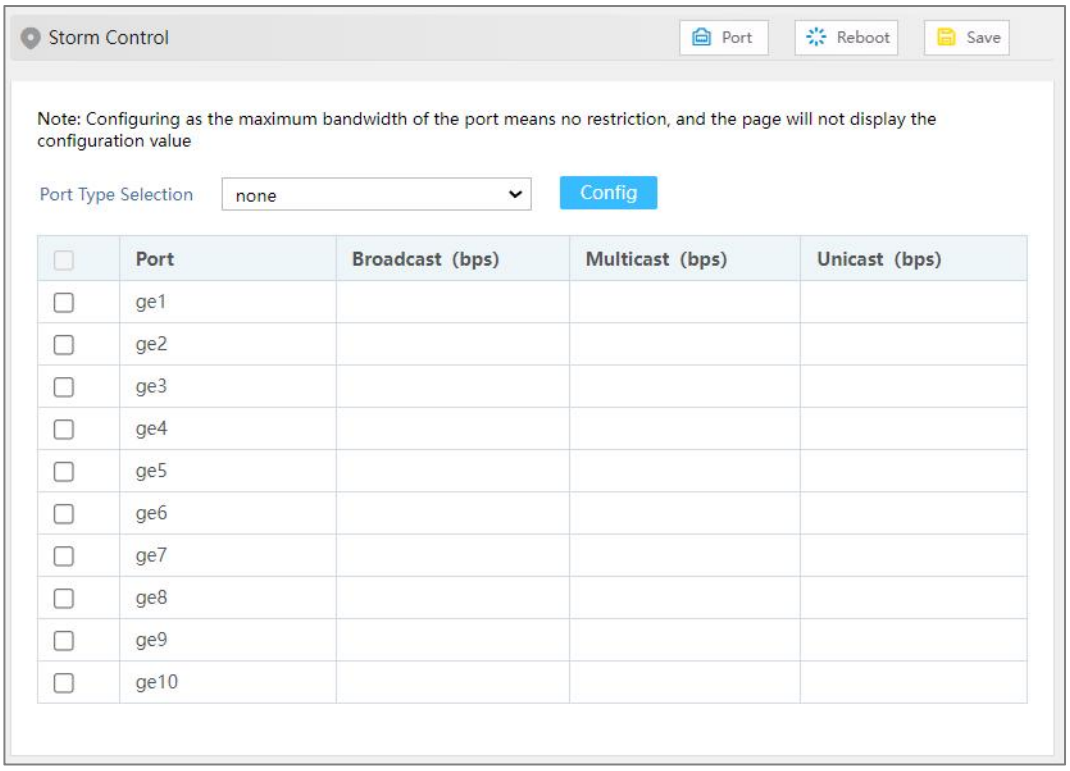
When the sum of each port broadcast, unknown multicast or unknown unicast flow achieves the value user sets, the system will discard the packets beyond the broadcast, unknown multicast or unknown unicast flow limit, so that the proportion of overall broadcast, unknown multicast or unknown unicast flow can be reduced to limited range, ensuring the normal operation of network business.

Operation Path

Open in order: "Port Configuration > Storm Suppression".

Interface Description

Storm control interface as follows:



Main elements configuration description of storm suppression interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Broadcast (bps)	The device procedure can suppress the transmission speed of broadcast packet

Interface Element	Description
	Note: Broadcast packet, namely, the data frame with the destination address of FF-FF-FF-FF-FF-FF.
Multicast (bps)	Port suppression to the transmission speed of unknown multicast data packet. Note: Multicast packet, namely, the destination address is XX-XX-XX-XX-XX-XX data frame, the second X is odd number, such as: 1, 3, 5, 7, 9, B, D, F, other X represents arbitrary number.
Unicast (bps)	Port suppression to the transmission speed of unknown unicast data packet. Note: Unknown unicast packet, namely, the MAC address of the data frame doesn't exist in the MAC address table of the device, which needs to be forwarded to all ports.

Note

Support unit of K/M/G when click the "Config" button to configure the rate. In WEB display, unit conversion will be conducted and similar values will be taken according to the input value and the unit.

4.5 Port Mirroring

Function Description

Copy the data from the origin port to appointed port for data analysis and monitoring.

Operation Path

Open in order: "Port Configuration > Port Mirroring".

Interface Description

Port mirror interface as follows:

The main element configuration description of port mirror interface:

Interface Element	Description

Source port	Data source port, which can be one or more, from which the device will collect data in the specified direction.
Direction	Data direction of the source port, options are as follows: • transmit: the message sent by the source port will be mirrored to the destination port. • receive: the packet received by the source port will be mirrored to the destination port. • both: the packet received or sent by the source port will be mirrored to the destination port.
Destination port	The destination port of device mirroring. The device only supports one destination port.

Note

- The function must be shut down in normal usage, otherwise all senior management functions based on port are not available, such as RSTP, IGMP snooping etc.
- Mirror function only deals with FCS normal packet; it cannot handle the wrong data frame

4.6 Port Isolation

Function Description

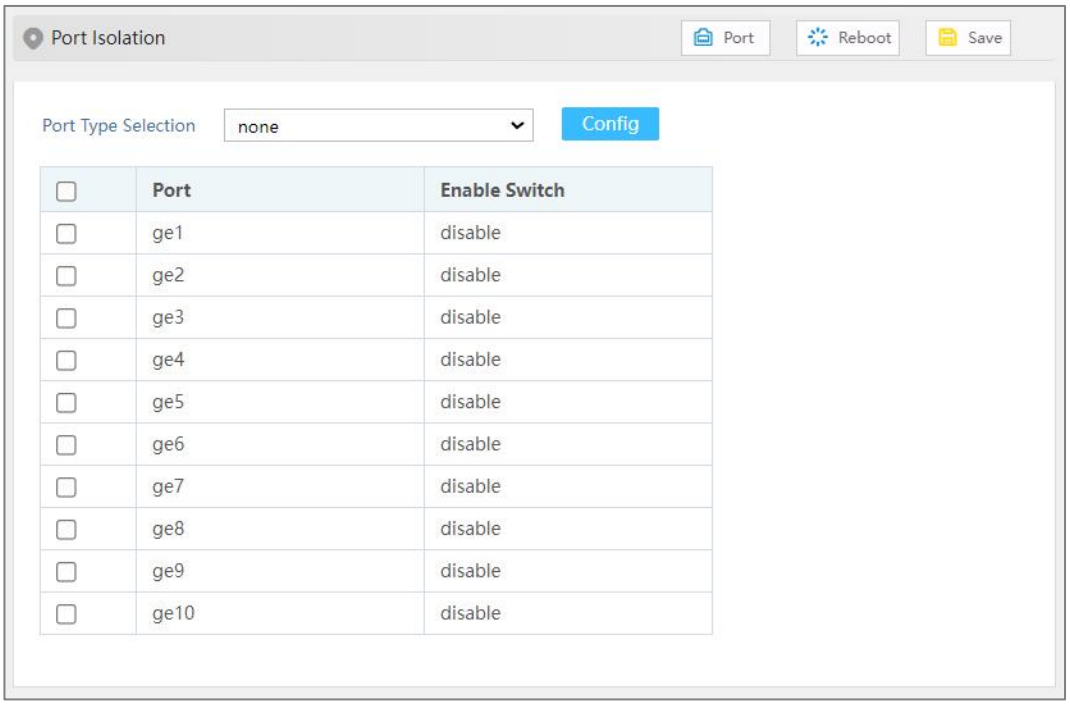
Port isolation is used for the layer 2 isolation between messages. It could add different ports to different VLANs, but waste limited VLAN resources. Adopting isolate-port characteristics can achieve isolation of ports within the same VLAN. After adding the ports to isolation group, user can achieve the layer 2 data isolation of ports within isolation group. Port isolation function has provided safer and more flexible networking scheme for users.

Operation Path

Open in order: "Port Configuration > Port Isolation".

Interface Description

Isolate-port configuration interface as follows:



The main element configuration description of isolate-port config interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Enable	Port isolation enable status can be displayed as follows: • disable • enable

4.7 Port Statistics

4.7.1 Port Statistics-Overview

Function Description

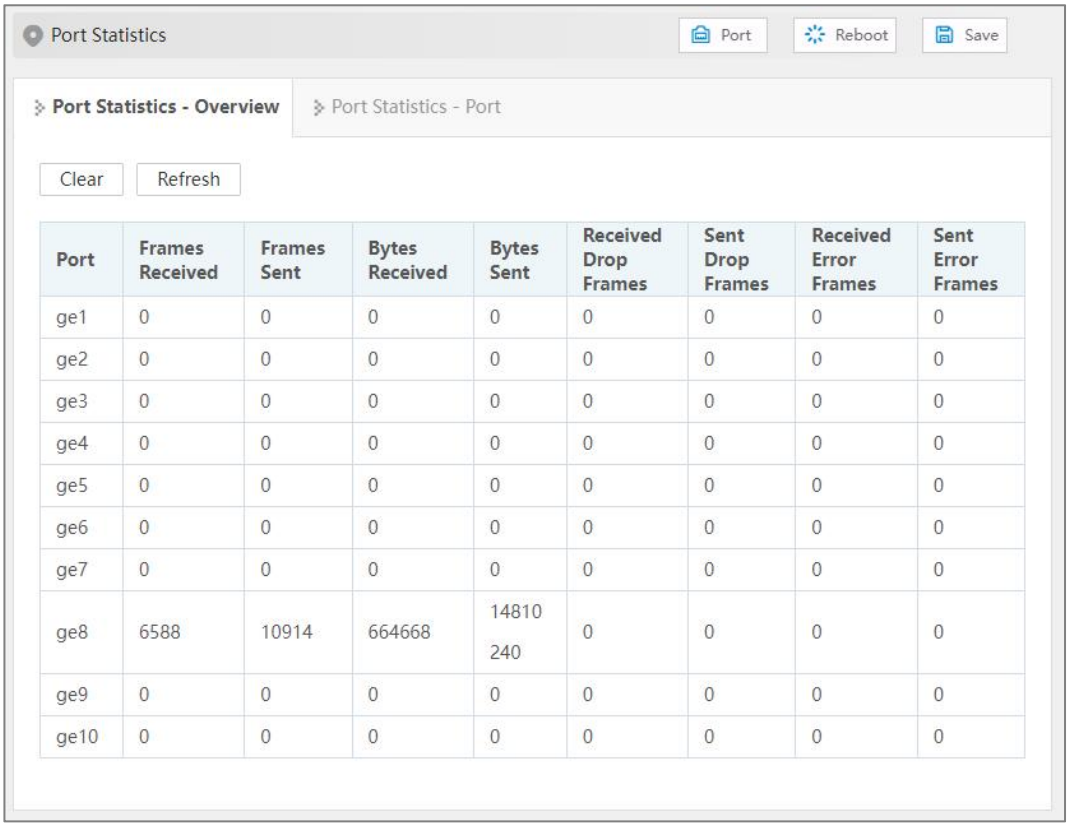
Check the number of messages and bytes, discarded messages and error messages sent and received by each port.

Operation Path

Open in order: "Port Configuration > Port statistics > Port Statistics-Overview".

Interface Description

Port Statistics-Overview interface as follows:



Port	Frames Received	Frames Sent	Bytes Received	Bytes Sent	Received Drop Frames	Sent Drop Frames	Received Error Frames	Sent Error Frames
ge1	0	0	0	0	0	0	0	0
ge2	0	0	0	0	0	0	0	0
ge3	0	0	0	0	0	0	0	0
ge4	0	0	0	0	0	0	0	0
ge5	0	0	0	0	0	0	0	0
ge6	0	0	0	0	0	0	0	0
ge7	0	0	0	0	0	0	0	0
ge8	6588	10914	664668	14810240	0	0	0	0
ge9	0	0	0	0	0	0	0	0
ge10	0	0	0	0	0	0	0	0

4.7.2 Port Statistics-Port

Function Description

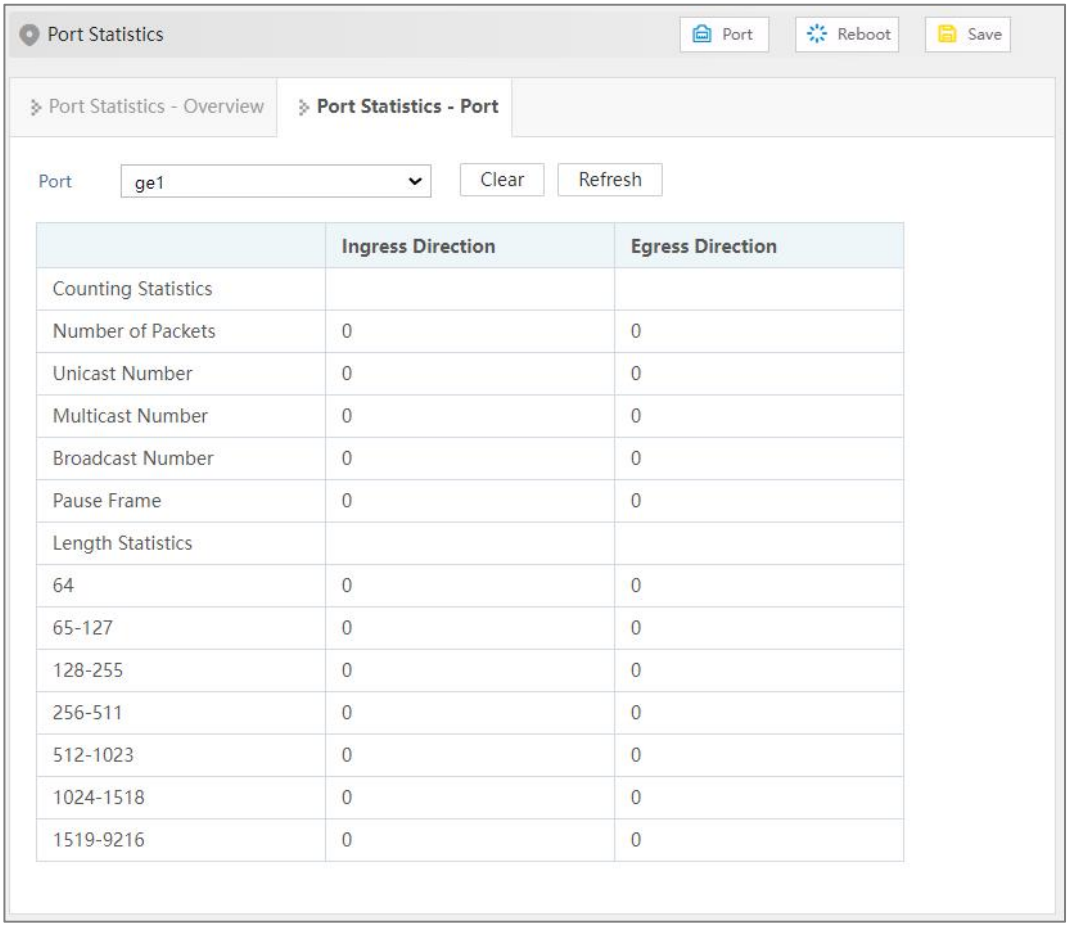
Check the classification statistics of the total number of messages sent and received by the designated port and the number of bytes of messages.

Operation Path

Open in order: "Port Configuration > Port statistics > Port Statistics-Port".

Interface Description

Port Statistics-Port interface as follows:



	Ingress Direction	Egress Direction
Counting Statistics		
Number of Packets	0	0
Unicast Number	0	0
Multicast Number	0	0
Broadcast Number	0	0
Pause Frame	0	0
Length Statistics		
64	0	0
65-127	0	0
128-255	0	0
256-511	0	0
512-1023	0	0
1024-1518	0	0
1519-9216	0	0

4.8 POE Management

PoE (Power over Ethernet) means supplying power through Ethernet. It's a wired Ethernet power supply technology that allows electric power to be transmitted to terminal device through data line or free line.

PoE power supply system includes:

- PSE (Power-sourcing Equipment): PoE device that supplies powered device with power through Ethernet.
- PD (Powered Device): powered device like wireless AP (Access Point), POS machine, camera and so on.
- PoE power supply: PoE power supply powers the whole PoE system. The quantity of PD that connects to PSE is limited by the power of PoE power supply.

4.8.1 Global Configuration

Function Description

On the "Global Config" page, user can configure the maximum PoE output power of the device.

Operation Path

Open in order: "Port Configuration > PoE Management > Global Configuration".

Interface Description

Global configuration interface is as follows:

The main element configuration description of global configuration interface:

Interface Element	Description (check the power checkbox, click “config” to configure it.)
PSE ID	PSE module ID display of the current device.
Current Total Power	The total output power display of current device’s PoE port, its unit is W.
Maximum Power	The maximum power limit of current device’s PoE output , the unit is W.

4.8.2 Port Configuration

Function Description

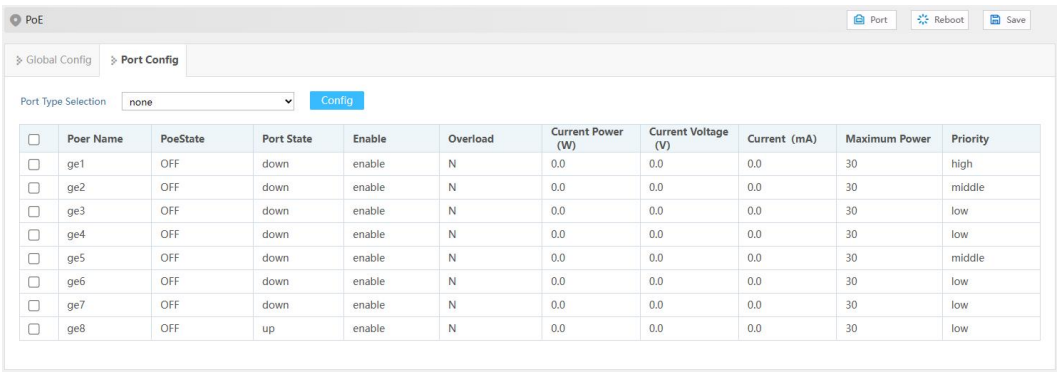
On the “Port Configuration” page, user can configure the device's PoE port enable, maximum output power, power supply priority etc.

Operation Path

Open in order: "Port Config > POE Management > Port Configuration”.

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
Port Name	The corresponding port name of the device PoE Ethernet port.
PoE State	The port PoE work state of current device, display state as follows: • ON: PoE port supplies power to PD; • OFF: PoE port is not powered or PD is not connected.
Port State	Ethernet port connection status, display status as follows: • down: represent the port is disconnected; • up: represent the port is connected.
Enable	Port enable check box, check the check box to enable the PoE port; not check this check box, the PoE port would be disabled.
Overload	The overload status of current device's PoE port, display items as follows: • Y: The current PoE port output power is greater than the maximum power. • N: The current PoE port output power is smaller than or equal to the maximum power.
Current Power (W)	The output power display of current device's PoE port, its unit is W.
Current Voltage (V)	The output voltage display of current device's PoE port, its unit is V.
Current (mA)	The current display of current device's PoE port, its unit is mA.
Maximum Power	The maximum power value configuration of PoE output of

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
	current device, and the value range is 0-30, and the unit is W.
Priority	The priority configuration of PoE port power supply. Priority is assigned to the port power under the total power limit. The priority drop-down list can be selected as follows: • High: high priority; • Medium: medium priority; • Low: low priority. Note: When the switch supplies power at nearly full capacity, it would first supply power to the PD device that connects to the port with High priority; then the PD device that connects to port with Medium priority.

5 Layer 2 Configuration

5.1 VLAN

VLAN is Virtual Local Area Network. VLAN is the data switching technology that logically (note: not physically) divides the LAN device into each network segment (or smaller LAN) to achieve the virtual working group (unit).

VLAN advantages mainly include:

- Port isolation. Ports in different VLAN, even in the same switch, can't intercommunicate. Such a physical switch can be used as multiple logical switches.
- Network security. Different VLAN can't directly communicate with each other, which has eradicated the insecurity of broadcast information.
- Flexible management. Changing the network user belongs to needn't to change ports or connection; only needs to change the firmware configuration.

That is, ports within the same VLAN can intercommunicate; otherwise, ports can't communicate with each other. A VLAN is identified with VLAN ID, and ports with the same VLAN ID belong to a same VLAN.

5.1.1 VLAN Configuration

Function Description

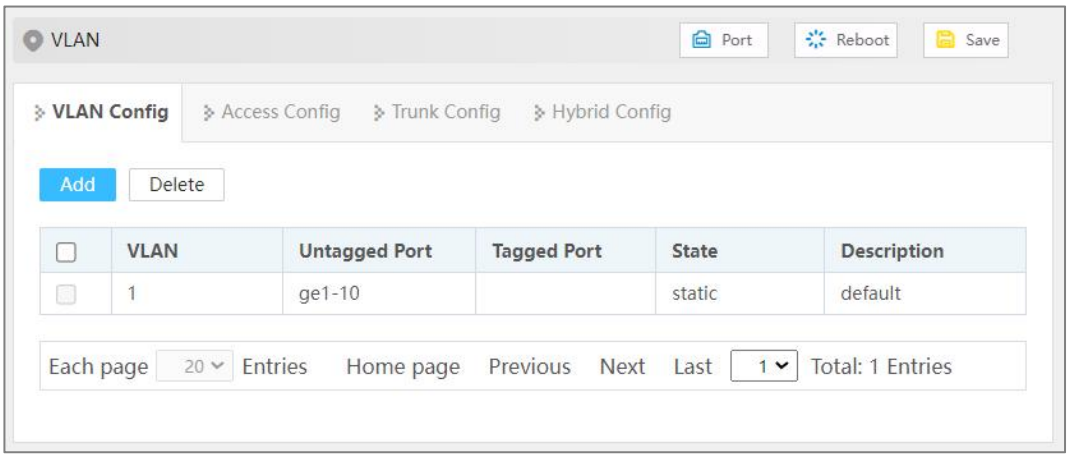
Create VLAN and edit VLAN description.

Operation Path

Open in order: "Layer 2 Configuration > VLAN > VLAN-config".

Interface Description

Vlan configuration interface as follows:



The main element configuration description of Vlan configuration interface.

Interface Element	Description
VLAN	VLAN ID number, value range is 1-4094.
Untagged Port	Untagged port member to conduct untagged process to sending data frame.
Tagged Port	Tag port member to conduct tagged process to sending data frame.
State	VLAN Status: • Static: static VLAN • Dynamic: dynamic VLAN
Description	VLAN description information, which supports 0-32 characters and consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).

5.1.2 Access Configuration

Function Description

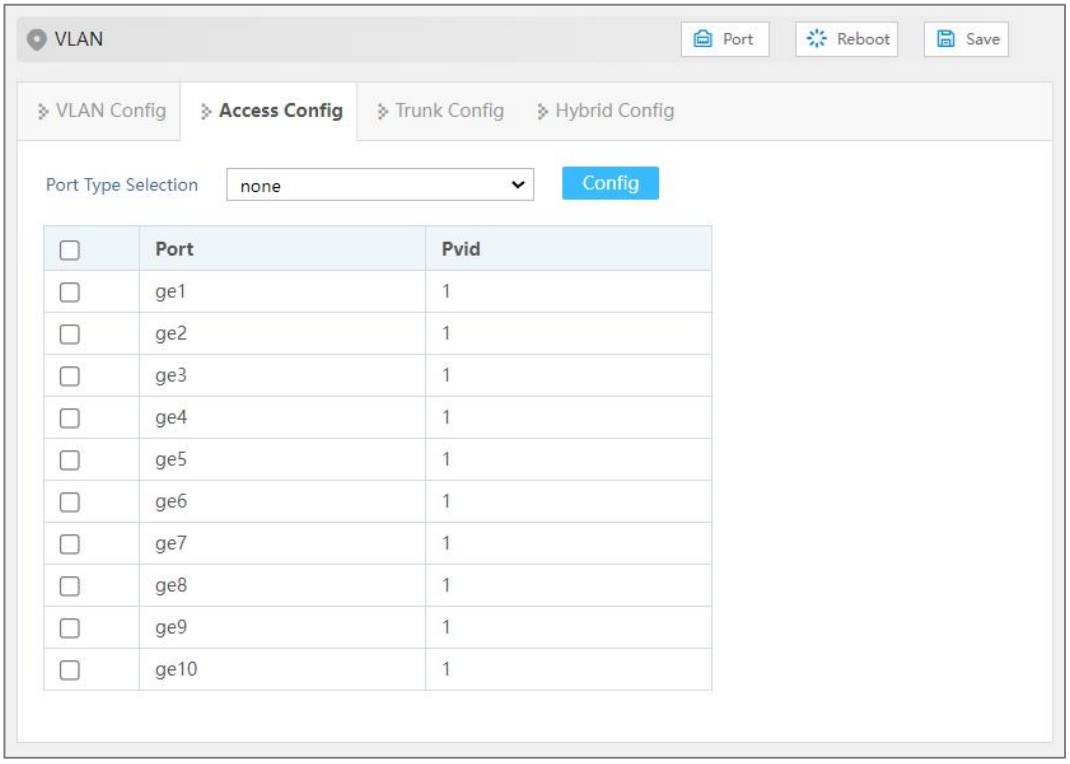
Configure the PVID (Port Default VLAN ID) of the Access interface, or modify it to Trunk/Hybrid interface.

Operation Path

Open in order: "Layer 2 Configuration > VLAN > Access Configuration".

Interface Description

Access configuration interface as follow:



The main element configuration description of Access configuration interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Pvid	Port Default VLAN ID, which is the default VLAN of the port. Default is 1, value range is 1-4094. Note: Each port has a PVID property, when the port receives Untag messages, it adds Tag mark on them according to PVID. When the port transmits data message with the same Tag mark as PVID, it would erase the Tag mark and then transmit the message. The PVID of all ports default to 1.
Configuration	Check the port and click “Configure” to reset PVID and port mode. • Access: port only belongs to 1 VLAN (which is the default VLAN), all ports of the switch are Access mode by default and all PVID are 1. • Trunk: port can belong to multiple VLAN, Trunk port can allow the messages of multiple VLANs to pass with Tag, but only allow the messages of one VLAN to transmit without tag (strip Tag) from this kind of interface.

Interface Element	Description
	Commonly used in the connection between network devices. • Hybrid: port can belong to multiple VLANs. Hybrid port allows messages of multiple VLANs to pass with tag, and allows the messages sent from this kind of interface to configure whether the messages of some VLANs is with tag (not strip Tag) or not (strip Tag). It could be used in the connection between network devices, as well as user devices.

5.1.3 Trunk Configuration

Function Description

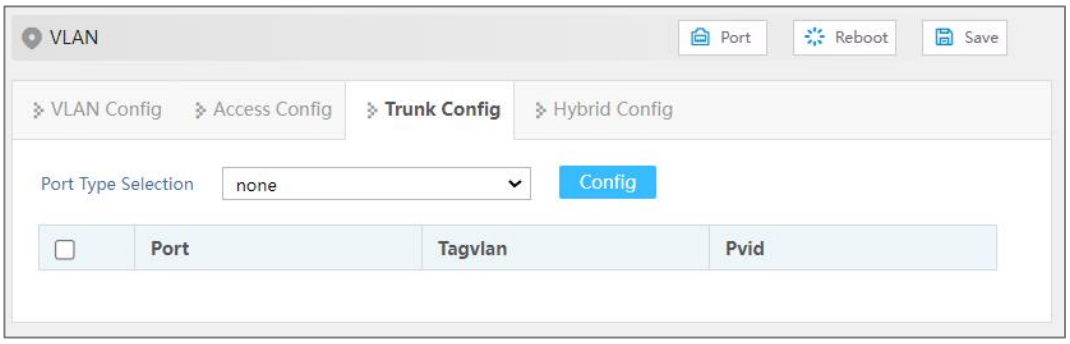
Configure the pvid value and tagvlan of Trunk port, or modify it to Access/Hybrid interface.

Operation Path

Open in order: "Layer 2 Configuration > VLAN > Trunk Configuration".

Interface Description

Trunk configuration interface as follows:



The main element configuration description of Trunk configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Tagvlan	The VLAN ID number that the port allows to pass.
Pvid	Port Default Vlan ID, which is the default VLAN of the port. Default is 1, value range is 1-4094.
Configuration	Check the port and click “Configure” to configure the VLAN

Interface Element	Description
	and PVID of the port, as well as the processing of PVID when sending messages.

5.1.4 Hybrid Configuration

Function Description

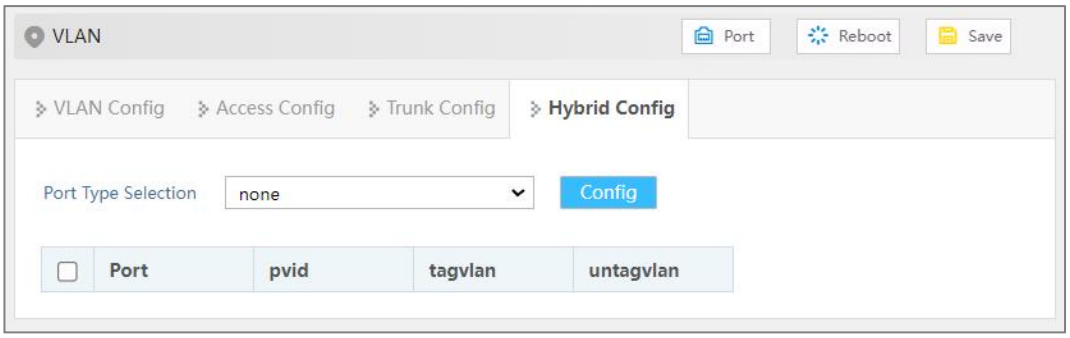
Configure the PVID value, Untagvlan and Tagvlan of Hybrid port, or modify it to Access/Trunk interface.

Operation Path

Open in order: "Layer 2 Configuration > VLAN Configuration > Hybrid Configuration".

Interface Description

Hybrid configuration interface as follow:



The main element configuration description of Hybrid configuration interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Pvid	VLAN ID number, value range is 1-4094.
Tagvlan	The VLAN ID number without TAG that the port allows to pass, a single value or range (the range is indicated by "-"), such as: 9 or 10-15.
Untagvlan	The VLAN ID number that the port allows to pass, a single value or range (the range is indicated by "-"), such as: 9 or 10-15.

Process for Port Receiving Message

Interface type	Process for Receiving Untagged Message	Process for Receiving Tagged Message
Access	Receive this message and tag it with default VLAN ID.	• Receive the message when the VLAN ID is the same as default VLAN ID. • Discard the message when the VLAN ID is different from the default VLAN ID.
Trunk Hybrid	Receive this message and tag it with default VLAN ID.	• Receive this message when the VLAN ID is in the list of VLAN ID that allow to pass through the interface. • Discard this message when the VLAN ID is not in the list of VLAN ID that allow to pass through the interface.

Process for Sending Message

Interface type	The process of transmit frame
Access	Strip the PVID Tag of the message first, then transmit it.
Trunk	• When the VLAN ID is the same as the default VLAN ID, and it is the VLAN ID allowed to pass through the interface, it would strip the Tag and send this message. • When the VLAN ID is different from the default VLAN ID, and it's the VLAN ID allowed to pass through the interface, it would remain its original Tag and send the message.
Hybrid	When the VLAN ID is the one allowed to pass through the interface, it would send this message. It could be set to whether to carry Tag during transmission.

5.2 MAC

MAC (Media Access Control) address is the hardware identity of network device; the switch forwards the message according to MAC address. MAC address has uniqueness, which has guaranteed the correct retransmission of message. Each switch is maintaining a MAC address table. In the table, MAC address is corresponding to the switch port. When the switch receives data frames, it decides

whether to filter them or forward them to the corresponding port according to the MAC address table. MAC address is the foundation and premise that switch achieves fast forwarding.

5.2.1 Global Configuration

Function Description

Set the aging time of dynamic MAC addresses.

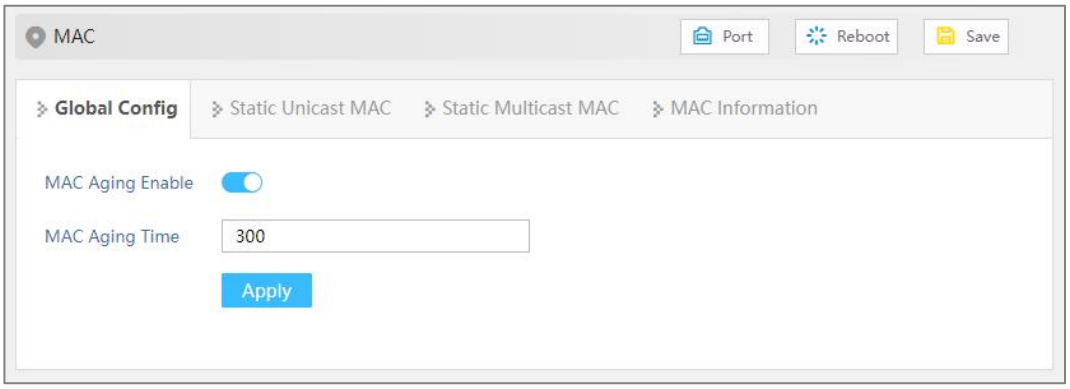
Each port in the switch is equipped with automatic address learning function, it stores the frame source address (source MAC address, switch port number) that port sends and receives in the address table. Ageing time is a parameter influencing the switch learning process; the default value is 300 seconds. When the timekeeping starts after an address record is added to the address table, if each port doesn't receive the frame whose source address is the MAC address within the ageing time, then these addresses will be deleted from dynamic forwarding address table (source MAC address, destination MAC address and their corresponding switch port number).

Operation Path

Open in order: "Layer 2 Config > MAC > Global Config".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
MAC Aging Enable	Enable switch of MAC address aging.
MAC Aging Time	MAC address aging-time, unit is second, default value is 300, and range is 10-1000000.

5.2.2 Static MAC

Function Description

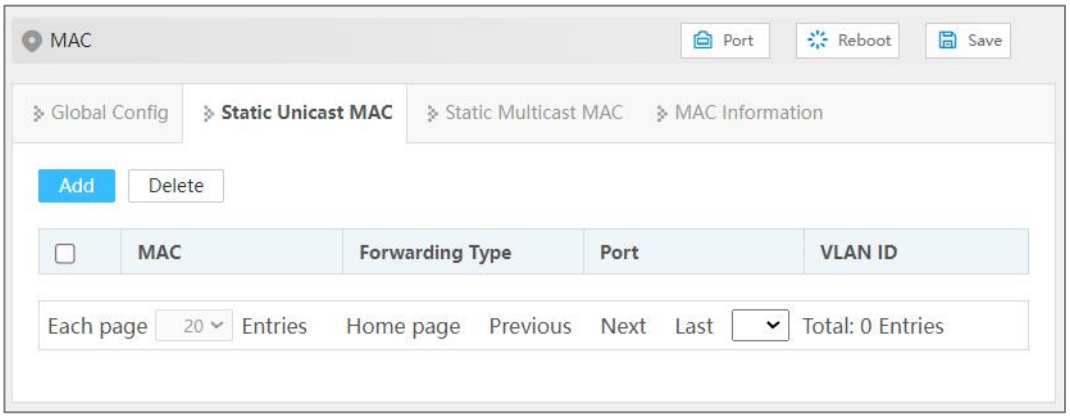
Source unicast MAC address binding and filtering will not age.

Operation Path

Open in order: "Layer 2 Configuration > MAC > Static Mac".

Interface Description

Static MAC interface as follows:



The main element configuration description of static MAC interface:

Interface Element	Description
MAC	The unicast MAC address bound by the interface, such as 0001.0001.0001.
Forwarding Type	MAC forwarding type, as shown below: • Discard • Forward
Port	The Binding Port Number.
VLAN ID	The VLAN ID number to which the data sent by this MAC address belongs, for example, 1-4094. Note: Input VLAN ID is the existing ID.

Note

- The function is a sort of security mechanism, please carefully confirm the setting, otherwise, part of the devices won't be able to communicate;
- Please don't adopt multicast address as the entering address;
- Please don't enter reserved MAC address, such as the local MAC address.

5.2.3 Static Multicast MAC

Function Description

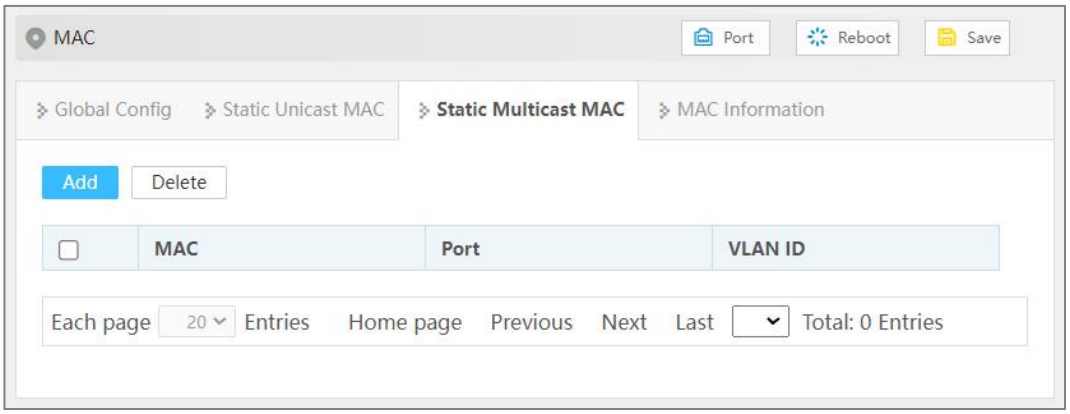
Source multicast MAC address binding will not age.

Operation Path

Open in order: "Layer 2 Configuration > MAC > Static Multicast MAC".

Interface Description

Static multicast MAC interface as follows:



The main element configuration description of static multicast MAC interface:

Interface Element	Description
MAC	Multicast MAC address bound to the interface, for example: 0100.5e01.0001.
Port	The Binding Port Number.
VLAN ID	The VLAN ID number to which the data sent by this MAC address belongs, for example, 1-4094. Note: Input VLAN ID is the existing ID.

5.2.4 MAC Information

Function Description

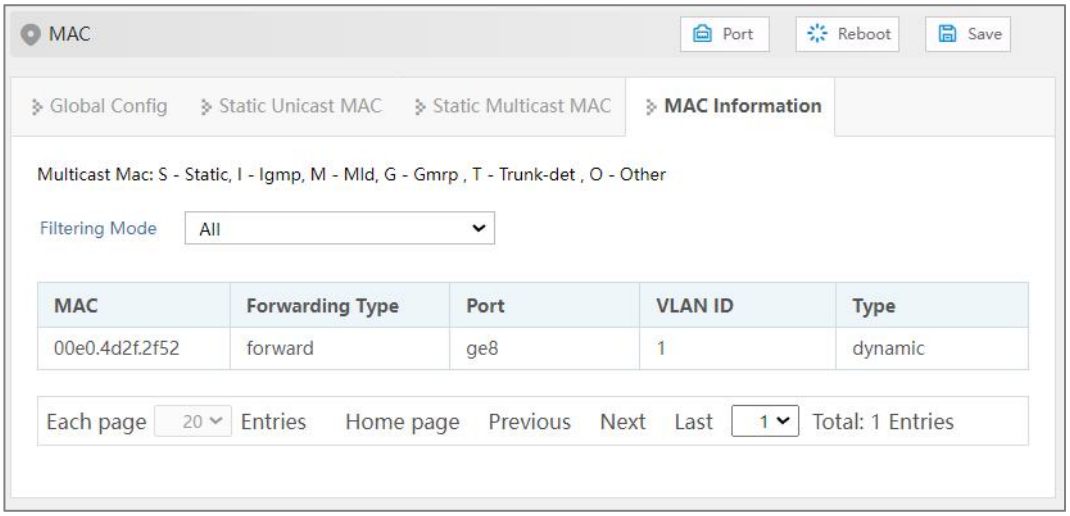
Check the MAC address table information.

Operation Path

Open in order: "Layer 2 Configuration > MAC > MAC Information".

Interface Description

MAC Information interface is as follow:



The main element configuration description of MAC information interface:

Interface Element	Description
Filtering Mode	Drop-down list of MAC mode to filter the display of the MAC address list of the specified type. The options are as follows: • All • Dynamic Unicast • Dynamic Multicast • Static Multicast • Static Unicast
MAC	The dynamic MAC addresses that the device have learned or the static MAC address information that user has configured.
Forwarding Type	MAC forwarding type, as shown below: • Discard • Forward
Port	Corresponding port number of the MAC address.
VLAN ID	VLAN ID number the data MAC address sending belongs to.
Type	The type of MAC address, it displays as follows: • dynamic • static

5.3 Spanning Tree

Spanning-tree protocol is a sort of layer 2 management protocol; it can eliminate the network layer 2 circuit via selectively obstructing the network redundant links. At the same time, it has link backup function. Here are three kinds of spanning-tree protocols:

- STP (Spanning Tree Protocol)
- RSTP (Rapid Spanning Tree Protocol)
- MSTP (Multiple Spanning Tree Protocol)

Spanning-tree protocol has two main functions:

- First function is utilizing spanning-tree algorithm to establish a spanning-tree that takes a port of a switch as the root to avoid ring circuit in Ethernet.
- Second function is achieving the convergence protection purpose via spanning-tree protocol when Ethernet topology changes.

Compared to STP, RSTP, MSTP can converge the network more quickly when network structure changes; MSTP is compatible with STP and RSTP, and is better than STP and RSTP. It can not only quickly converge but also send different VLAN along each path to provide better load sharing system for redundant link.

5.3.1 Global Configuration

Function Description

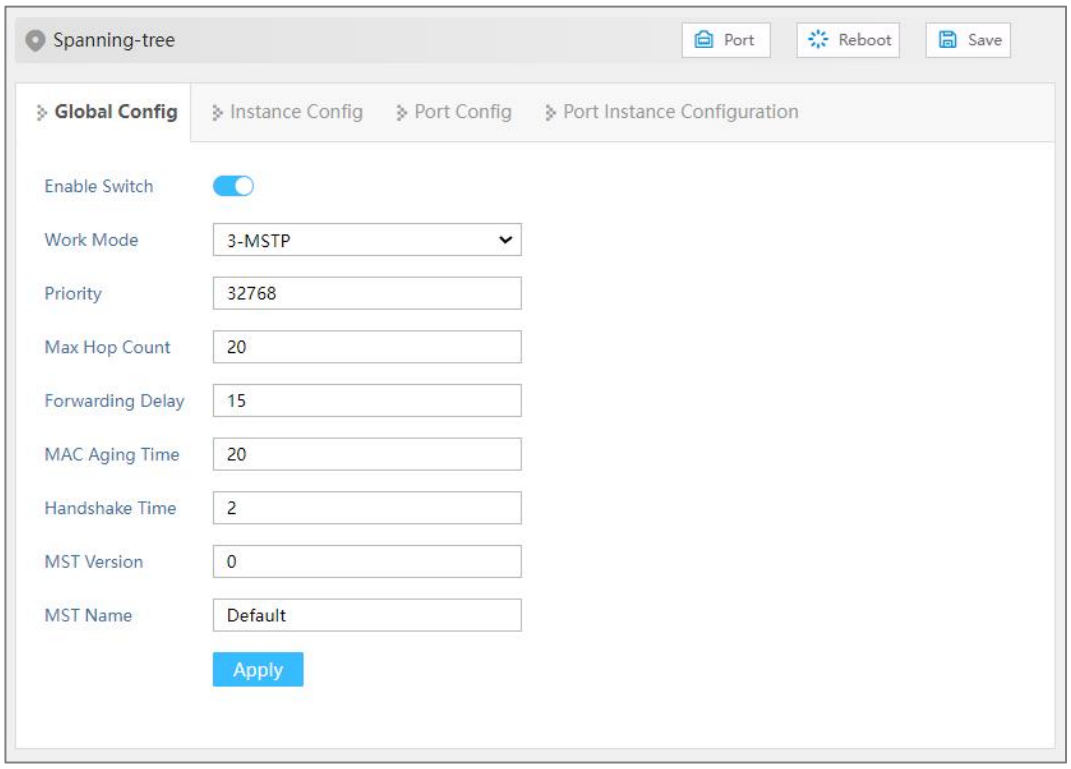
Configure the relevant parameters of spanning tree.

Operation Path

Open in order: "Layer 2 Configuration > Spanning-tree > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Enable	Spanning-tree enable switch. Disable by default
Work mode	Defaults to MSTP, there are three modes for spanning-tree protocol choice: • 0-STP: Spanning-tree • 2-RSTP: Rapid spanning tree • 3-MSTP: Multiple spanning-trees Note: In RSTP or MSTP mode, when the connection with STP device is found, the port will automatically migrate to STP compatible mode to work.
Priority	Bridge priority level, value range is 0-61440. Note: Smaller the priority level value is, higher the priority level is. It must be a multiple of 4096.
Max Hop Count	The maximum hop in MST region, defaults to 20, the value range is 1-40. Note: The maximum hop in MST region has limited the size of MST region. The maximum hop configured on a domain root will be used as the maximum hop in MST region.
Forwarding Delay	Port state transition delay, defaults to 15s, the value range is 4-30.
MAC Aging Time	The maximum lifetime of the message in the device, defaults

Interface Element	Description
	to 20s, the value range is 6-40. It's used to determine whether the configuration message times out.
Handshake Time	Message sending cycle, defaults to 2s, the value range is 1-10. Note: • The spanning tree protocol sends configuration information every Hello time to check whether the link is faulty. • In order to avoid frequent network flap, forwarding delay, aging time and handshake time should satisfy the following formula: 2× (forwarding delay -1)≥ aging time ≥2× (handshake time -1).
MST Version	MSTP revision level, defaults to 0, the value range is 0-65535. Note: When the MST region name, revision level, instance-to-VLAN mapping relation are the same, the two or more bridges will belong to a same MST region.
MST Name	MST domain name, defaults to Default, up to 32 characters.

5.3.2 Instance Configuration

Function Description

Configure instance-to-VLAN mapping.

Multiple Spanning Tree Regions (MST Regions) are composed of multiple devices in the switched network and the network segments between them.

In a MST region, multiple spanning trees can be generated through MSTP. Each spanning tree is independent to others and corresponding to special VLAN. Each spanning tree is called an MSTI (Multiple Spanning Tree Instance).

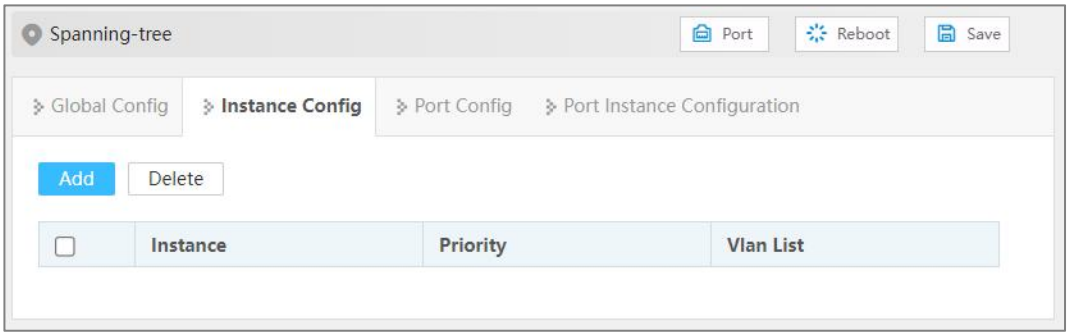
VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI.

Operation Path

Open in order: "Layer 2 Configuration > Spanning-tree > Instance Configuration".

Interface Description

Instance configuration interface as follows:



The main element configuration description of instance configuration interface:

Interface Element	Description
Instance	Instance ID number of Multiple Spanning-tree. The value range is 1-16.
Priority	Device priority level, value range is 0-61440, default to 32769, step is 4096. During adding, choose a priority based on 0-15 times the value on the 4096. Note: The priority of a device participates in spanning tree calculation. Its size determines whether the device can be selected as the root bridge of a spanning tree.
VLAN List	The list of VLANs mapped to MSTI instances, each VLAN can only correspond to one MSTI. Note: VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI. MSTP achieves load balancing based on the VLAN mapping table.

5.3.3 Port Configuration

Function Description

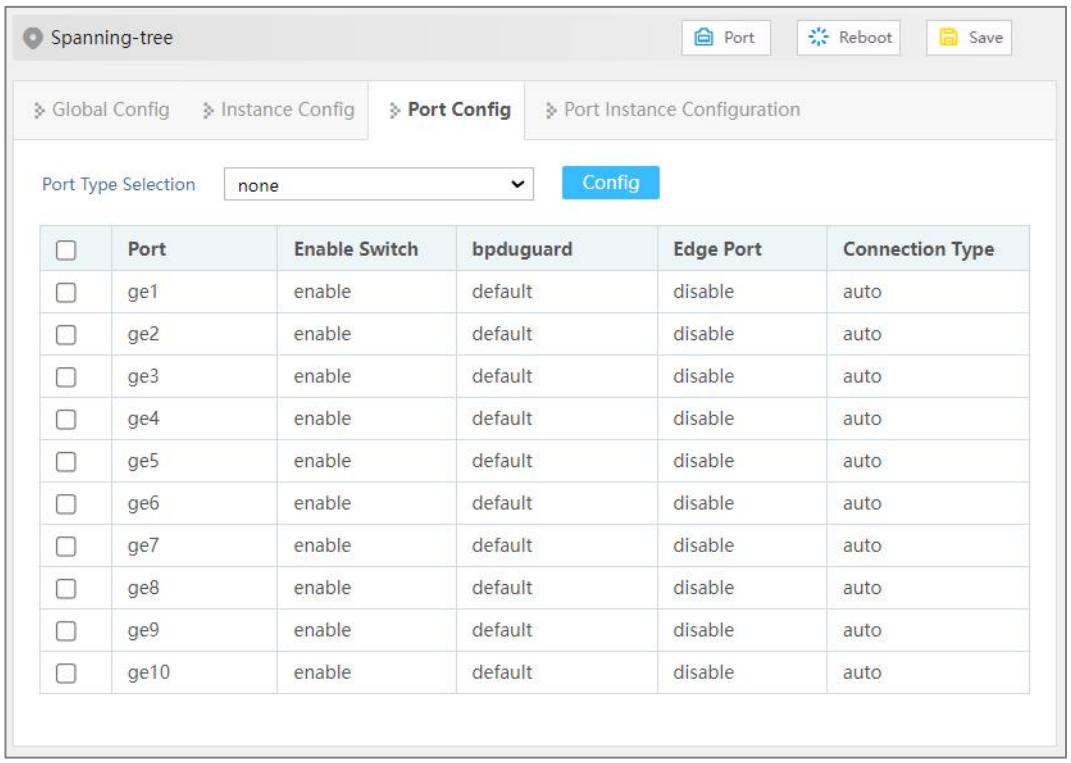
Enable port to participate in spanning-tree and configure port type, link type and BPDU protection function.

Operation Path

Open in order: "Layer 2 Configuration > Spanning-tree > Port Configuration".

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Enable	The enable status of ports participating in spanning tree can be shown as follows: • Enable • Disable: disable
BPDU Guard	BPDU (Bridge Protocol Data Unit) protection function. After starting the BPDU protection, if the edge port receives the BPDU message that should not exist, the edge port will be closed, and it can return to normal after a certain time. Edge Port BPDU Guard State: • Default: global configuration protection status • Enable • Disable: disable
Edge port	The port that directly connects to terminal instead of other switches. The edge port does not participate in the spanning tree operation, and can be directly transferred to the Forwarding state by Disable. Enable state of edge port: • Enable • Disable: disable

Interface Element	Description
Connection Type	Fast entry of the port into the forwarding state requires that the port must be a point-to-point link, not a shared media link. Port link type: • Auto: if the port is full duplex, it is judged as a point-to-point link; If it is half-duplex, it is judged as a non-point-to-point link. • Point-to-point: point-to-point link. • Shared: Non point-to-point link.

5.3.4 Instance Port Configuration

Function Description

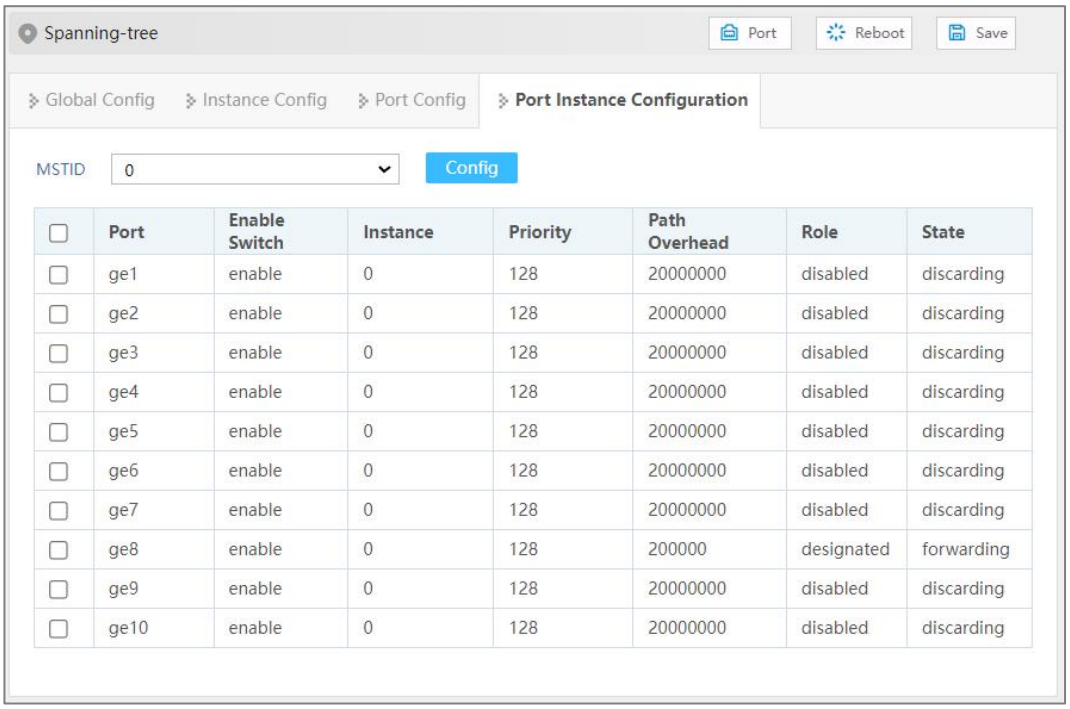
Configure port priority and cost

Operation Path

Open in order: "Layer 2 Configuration > Spanning-tree > Inst Port Configuration".

Interface Description

Instance port configuration interface as follows:



Port	Enable Switch	Instance	Priority	Path Overhead	Role	State
ge1	enable	0	128	20000000	disabled	discarding
ge2	enable	0	128	20000000	disabled	discarding
ge3	enable	0	128	20000000	disabled	discarding
ge4	enable	0	128	20000000	disabled	discarding
ge5	enable	0	128	20000000	disabled	discarding
ge6	enable	0	128	20000000	disabled	discarding
ge7	enable	0	128	20000000	disabled	discarding
ge8	enable	0	128	200000	designated	forwarding
ge9	enable	0	128	20000000	disabled	discarding
ge10	enable	0	128	20000000	disabled	discarding

The main element configuration description of instance port configuration interface:

Interface Element	Description
MSTID	Choose multiple Spanning-tree ID number.
Port	The corresponding port name of the device Ethernet port.
Enable	Port enable status: • Enable: participate in spanning-tree; • Disable: not participate in spanning-tree.
Instance	Instance ID number port belongs to.
Priority	Port priority, the value range is 0-240, the step size is 16, the default value is 128, and the priority based on 0-15 times the value of 16 can be selected. Note: Port priority level in bridge, port priority level is higher when the value is smaller. The higher the priority, the more likely it is to be a root port.
Path Overhead	The path cost from network bridge to root bridge, defaults to 20000000. Value range: 1-200000000. Note: When the configuration cost is the default value, the actual cost of link up port is converted according to the port rate, the rate of 10M corresponds to the cost of 2000000, and 100M corresponds to the cost of 200000.
Role	Role • unkn: Unknown; • root: Root port; • desg: Designated port; • altn: Alternate port; • back: Backup port; • disa: Disable port.
State	Port status in spanning-tree: • Disable: Port close status; • Blocking: Blocked state; • Listening: Monitoring state. • Discarding: Discarding status • Learning: Learning state; • Forwarding: Forwarding state;

5.4 Ring

Ring is a private ring network algorithm developed and designed for highly reliable industrial control network applications that require link redundancy backup. Its design concept is completely in accordance with international standards (STP and RSTP)

implementation, and do the necessary for industrial control application optimization, with Ethernet link redundancy, fault fast automatic recovery ability.

Ring adopts the design of no master station. The devices running the Ring protocol discover the loop in the network by exchanging information with each other, and block a certain port. Finally, the ring network structure is trimmed into a tree network structure without loop, thus preventing messages from circulating continuously in the ring network, and avoiding the reduction of processing capacity caused by repeated reception of the same message. In a multi-Ring network composed of 250 switches, when the network is interrupted or fails, the ring can ensure that the user network automatically resumes link communication within 20 ms.

Ring needs to manually divide the ring network ports in advance, support multiple ring network types such as single ring, coupled ring, chain and Dual Homing, and provide visual management of network topology. In a single Ring, Ring supports master/slave and no master configuration to meet various network environment requirements.

Function Description

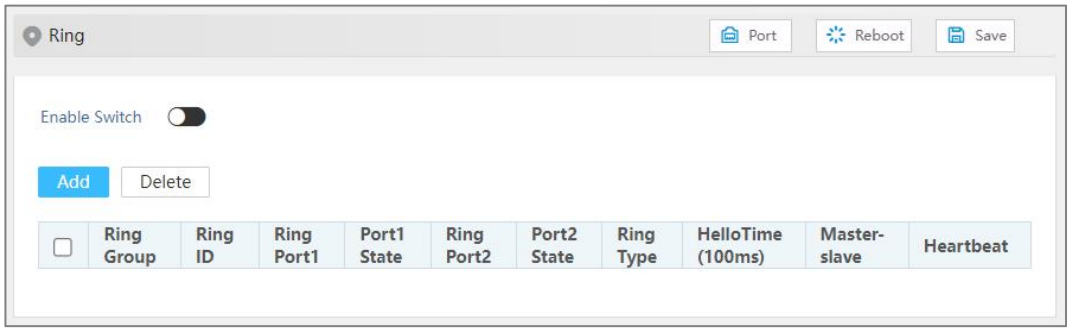
Configure Ring private protocol ring network.

Operation Path

Open in order: "Layer 2 Configuration > Ring".

Interface Description

Ping interface as follows:



The main element configuration description of Ring interface.

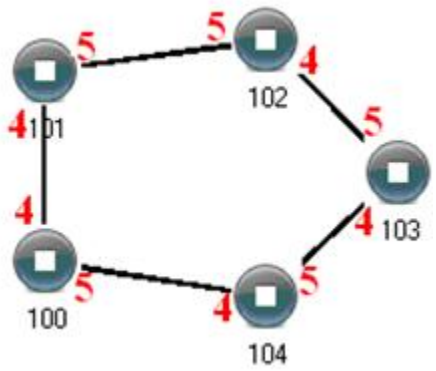
Interface Element	Description
Enable	Enable switch, which can enable the Ring network function after being enabled.
Ring Group	Support ring group 1-12, it can create multiple ring networks at the same time.
Ring ID	When multiple switches form a ring, the current ring ID would

Interface Element	Description
	be network ID. Different ring network has different ID. Value range is 1-255. Note: The ring network identification must remain the same in one ring network.
Ring Port 1	Port 1 can be used for the formation of ring network in switch. Note: When the ring network type is "Couple", ring port 1 is the "Coupled Port". Coupling port is the port that connects different network identities.
Port1 State	Conduction state of ring network port 1.
Ring Port 2	The network port 2 on the switch used to form a ring. Note: When the ring network type is “Couple”, ring port 2 is the “console port”. Console port is the port in the chain where two rings intersect.
Port2 Status	Conduction state of port 2 of ring network.
Ring Type	According to the requirement in the scene, user can choose different ring type. • Single: single ring, using a continuous ring to connect all device together. • Couple: couple ring is a redundant structure used for connecting two independent networks. • Chain: chain can enhance user’s flexibility in constructing all types of redundant network topology via an advanced software technology. • Dual-homing: two adjacent rings share one switch. User could put one switch in two different networks or two different switching equipments in one network.
Hello Time (100ms)	Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends information packet to adjacent device for confirming the connection is normal or not. The value range is 0-300, unit: 100ms.
Master-slave	Single ring supports no master station and one master and multiple slave modes (optional): • No-master station mode: When all the single-loop devices are slave stations, the single-loop structure is no-master station. • One-Master Multi-Slave mode: When the device is set as master device and one end of it is backup link, it can enable backup link to ensure the normal operation of the

Interface Element	Description
	network when failure occurs in ring network.
Heartbeat	Heartbeat detection mechanism. When this configuration is enabled, the network association will periodically send heartbeat messages to detect whether the corresponding devices are in live state, thus enhancing the reliability of the network.

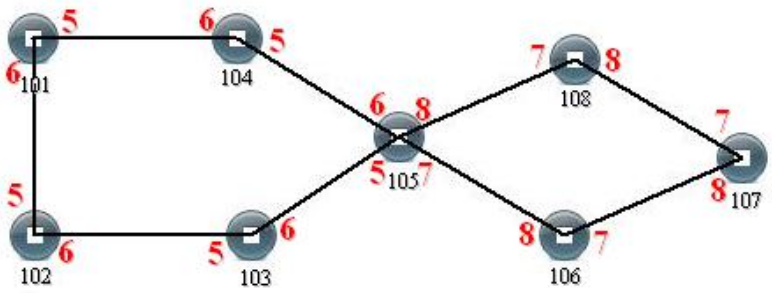
Single Ring Configuration

Enable Single, enable ring group 1 (other ring group is OK), Set the device port 4 and port 5 to ring port, and set other switches to the same configuration as the switch above, Enable these devices, and adopt network cable to connect port 4 and port 5 of the switch, then search it via network management software, the ring topology structure picture as below:



Double Ring Configuration

Double ring as shown below, in the figure, double ring is the tangency between two rings, and the point of tangency is NO. 105 switch.



Configuration Method:

Step 1 Adopt single ring configuration method to configure port 5 and port 6 of NO. 101, 102,

103, 104, 105 switches as the ring port, and the ring group is 1;

Step 2 Adopt single ring configuration method to configure port 7 and port 8 of NO. 105, 106, 107 and 108 switches as the ring ports and the ring group 2;

Step 3 Adopt network cable to connect the ring group 1;

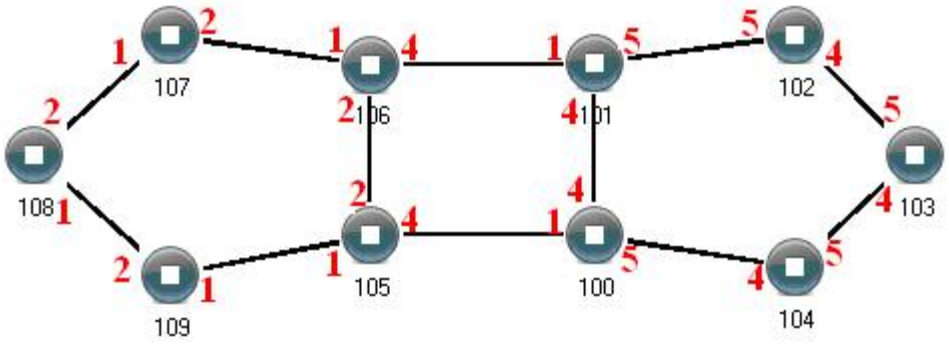
Step 4 Adopt network cable to connect the ring group 2;

Step 5 Search the topology structure picture via network management software;

Since NO. 105 devices belong to two ring groups, the network IDs of the two ring groups cannot be the same.

Coupling Ring Configuration

Coupling ring basic framework as the picture below:



Operation method:

Step 1 Enable ring network group 1 and 2: (Hello_time could be disabled, but the time could not be set to make Hello packet send too fast, otherwise it would effect CPU processing speed seriously);

Step 2 Set the ring port of NO. 105, 106 device ring group to port 1 and port 2, network identification to 1, ring type to Single; Set the coupling port of ring group 2 to port 4, console port to 2, ring identification to 3, ring type to Coupling.

Step 3 Set the ring port of NO. 100, 101 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single; Set the coupling port of ring group 2 to port 1, console port to port 4, ring identification to 3, ring type to Coupling.

Step 4 Set the ring port of NO. 107, 108 and 109 device ring group 1 to port 1 and port 2, network identification to 1, ring type to Single; Set the ring port of NO. 102, 103 and 104 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single.

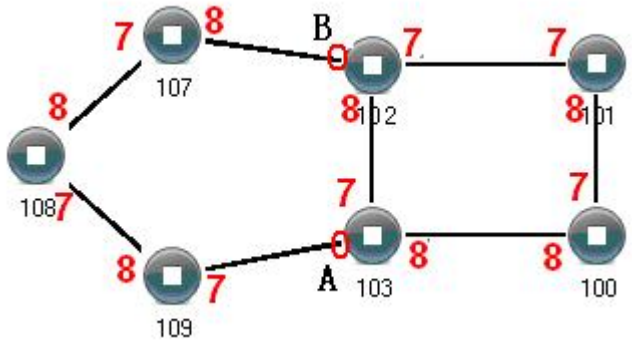
Step 5 Connect the port 4 and port 5 of five devices NO. 100-104 to the single ring in turn, adopt network cable to connect the port 1 and port 2 of four devices NO. 105-109 to the single ring in turn, Then adopt Ethernet cable to connect port 4 of NO. 106 device to port 1 of NO. 101 device, port 4 of NO. 105 device to port 1 of NO. 100 device,

coupling ring combination is completed.

Console ports are two ports connected to NO. 105 device and NO. 106 device in the above picture. The two ports connected to NO. 100 device and NO. 101 device are also called console ports.

Chain Configuration

Chain basic framework as the picture below:



Operation method:

Step 1 Enable ring group1: (Hello_time could be disabled, but the time shouldn't be set to send Hello packet too fast, otherwise it would affect the processing speed of CPU seriously).

Step 2 Set the ring port of NO. 100, 101, 102 and 103 device ring group 1 to port 7 and port 8, network identification to 1, ring type to Single. Set the ring port of NO. 107, 108 and 109 devices ring group 1 to port 7 and port 8, network identification to 2, ring type to Chain.

Step 3 Adopt network cable to connect the port 7 and port 8 of three devices NO. 107-109, adopt network cable to connect the port 7 and port 8 of four devices NO. 100-103 to the single ring in turn, Then adopt network cable to connect port 7 of NO. 107 device and port 7 of NO. 109 device to normal ports of NO. 102 and 103 device, chain combination is complete.

Note

- Port that has been set to port aggregation can't be set to rapid ring port, and one port can't belong to multiple rings;
- Network identification in the same single ring must be consistent, otherwise it cannot form a normal ring or normal communicate;
- Network identification in different ring must be different;
- When forming double ring and other complex ring, user should notice whether the

network identification in the same single ring is consistent, and network identification in different single ring is different.

5.5 MRP

MRP (Media Redundancy Protocol), in MRP ring network, one device is regarded as redundancy manager, and the others are redundancy client. MRP supports up to 50 devices, and when the loop network is interrupted, the loop reconfiguration time is less than 200ms.

Function Description

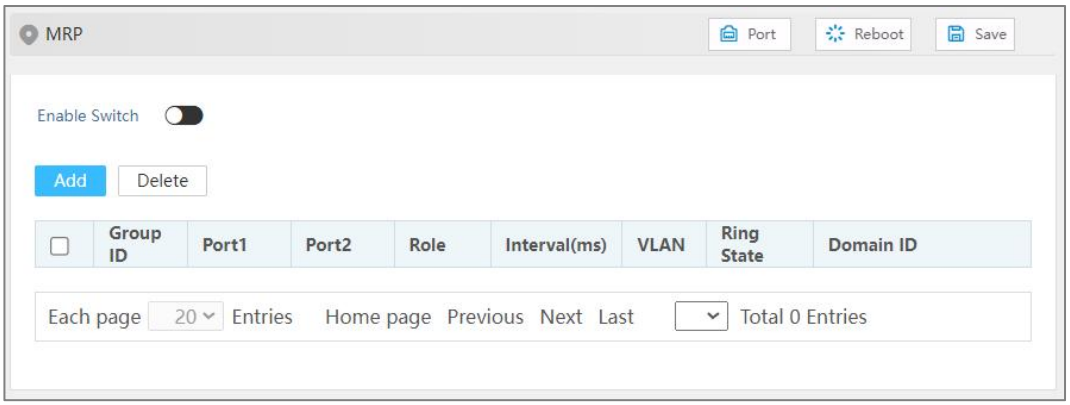
Configure MRP ring network.

Operation Path

Open in order: "Layer 2 Configuration > MRP".

Interface Description

The MRP interface is as below:



The main element configuration descriptions of MRP interface:

Interface Element	Description
Enable	Enable switch, which can enable the MRP ring network function after being enabled.
Group ID	The ID of ring network, its value range is 1-50.
Port1	Ring network port 1, the ports that make up the ring network and the forwarding state of port data.
Port2	Ring network port 2, the ports that make up the ring network and the forwarding state of port data.
Role	The redundant role of device in the ring network can be

Interface Element	Description
	selected as follows: • manager: media redundancy manager • client: media redundancy client
Interval (ms)	When the MRP ring network is disconnected, the ring network reconfigures the convergence time. The options are as follows: • 10ms • 30ms • 200ms • 500ms
VLAN	VLAN ID used by MRP management message, its value range is 1-4094.
Ring Network State	Status of MRP ring network, Open or Close.
Domain ID	MRP ring network group domain ID, the format is x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.x.

5.6 ERPS

Ethernet Ring Protection Switching (ERPS) is the Ethernet Ring Network Link Layer Technology with high reliability and stability. ERPS is a protocol defined by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) to eliminate loops at layer 2. Because the standard number is ITU-T G.8032/Y1344, ERPS is also called G.8032. ERPS defines Ring Auto Protection Switching (RAPS) Protocol Message and protection switching mechanisms. It can prevent the broadcast storm caused by data loop when the Ethernet ring is intact. When the Ethernet ring link failure occurs, it has high convergence speed that can rapidly recover the communication path between each node in the ring network.

5.6.1 Timer Configuration

Function Description

Configure the parameters of ERPS ring network timer. After the failure of the node device or link in the ERPS ring is restored, in order to prevent the flap, the timer to the ERPS ring will be enabled to help reduce the interruption time of traffic flow.

In ERPS protocol, timers used mainly include WTR (Wait to Restore) Timer, Guard and Hold Timer.

- WTR timer

  If an RPL owner port is unblocked due to a link or node fault, the involved port may not go Up immediately after the link or node recovers. Blocking the RPL owner port may cause network flapping. Blocking the RPL owner port may cause network flapping. To prevent this problem, the node where the RPL owner port resides starts the wait to restore (WTR) timer after receiving an RAPS (NR) message. The WTR Timer will be turned off if SF (Signal Fail) RAPS messages are received from other ports before the timer expires. If the node does not receive any RAPS (SF) message before the timer expires, it blocks the RPL owner port when the timer expires and sends NR-RB (RPL Block, RPL) RAPS message. After receiving this RAPS (NR, RB) message, the nodes set their recovered ports on the ring to the Forwarding state.

- Guard timer

  Device involved in link failure or node failure sends NR(No Request) RAPS message to other device after failure recovery or clearing operation, and starts Guard Timer at the same time, and does not process NR RAPS message before the timer expires, in order to prevent receiving expired NR RAPS message. Before the Guard timer expires, the device does not process any RAPS (NR) messages to avoid receiving out-of-date RAPS (NR) messages. After the Guard timer expires, if the device still receives an RAPS (NR) message, the local port enters the Forwarding state.

- Hold Timer

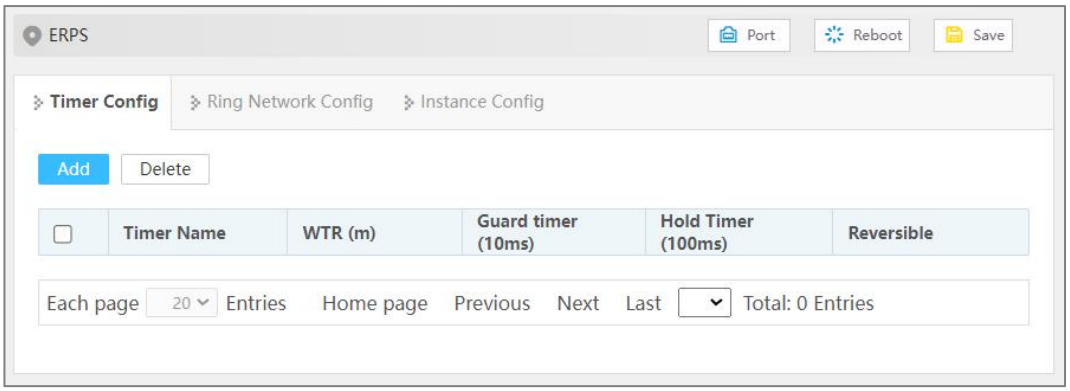
  On Layer 2 networks running ERPS, there may be different requirements for protection switching. For example, on a network where multi-layer services are provided, after a server fails, users may require a period of time to rectify the server fault so that clients do not detect the fault. Users can set the Hold timer. If the fault occurs, the fault is not immediately sent to ERPS until the Hold Timer expires and the fault is still not recovered.

Operation Path

Open in order: "Layer 2 Configuration > ERPS > Timer Configuration".

Interface Description

Timer configuration interface as follows:



Main elements configuration description of timer configuration interface:

Interface Element	Description
Timer Name	The name of ERPS timer, which supports 1-32 characters and consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).
WTR	WTR timer, value range is 1-12, unit: minute.
Guard Timer (10ms)	Guard timer, its value range is 1-200, unit 10ms.
Hold Timer (100ms)	Hold timer, its value range is 0-100, unit 100ms.
Reversible	ERPS reversible mode status, options as follows: • enable If the failed link recovers, the RPL owner port will be blocked again after waiting for WTR time. Blocked links are switched back to RPL. • disable If the failed link recovers, the WTR timer is not started, and the original faulty link is still blocked and will be switched to RPL.

5.6.2 Ring Configuration

Function Description

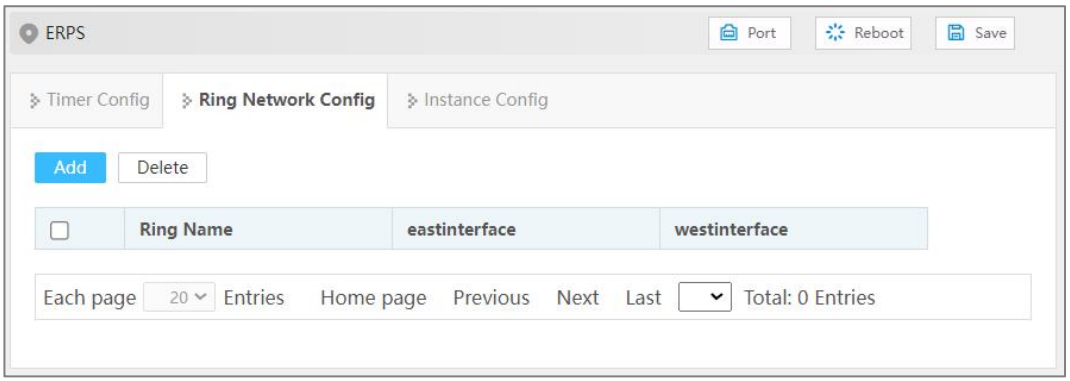
Configure ERPS ring port.

Operation Path

Open in order: "Layer 2 Configuration > ERPS Configuration > Ring Configuration".

Interface Description

Ring configuration interface as follows:



The main element configuration description of ring configuration interface:

Interface Element	Description
Ring Name	The name of ERPS ring network, which supports 1-32 characters, consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).
East Interface	ERPS ring port. Note: When the device is an intersecting node, only EastInterface can be configured for some ports of the sub-ring.
West Interface	ERPS ring port. Notice: • ERPS ring ports can be normal physical ports or static aggregation groups. • ERPS ring port cannot be opened at the same time with other layer 2 ring network protocols, when ERPS guard instance is not 0, it can be opened at the same time with MSTP. • ERPS ring ports can't be the same ports. • ERPS ring ports must be trunk ports and allow the ring instance VLAN to pass.

5.6.3 Instance Configuration

Function Description

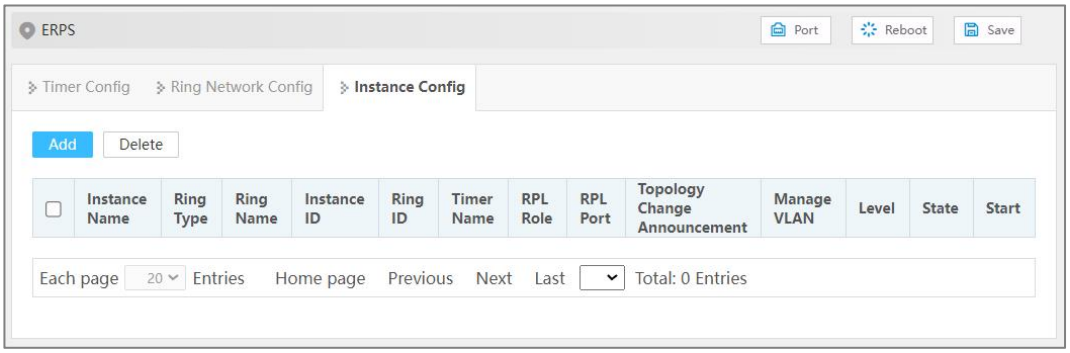
Configure ERPS ring network instance.

Operation Path

Open in order: "Layer 2 Configuration >ERPS Configuration > Instance Configuration".

Interface Description

Instance configuration interface as follows:



The main element configuration description of instance configuration interface:

Interface Element	Description
Instance Name	The name of the ERPS instance, which supports 1-32 characters, consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).
Ring Type	ERPS instance ring network type, the options are as follows: • Major-ring: main ring, closed ring. • Sub-ring: a sub-ring, an unclosed ring, forms a multi-ring network such as an intersecting ring with the main ring.
Ring Name	ERPS Ring Name. Note: The ring name should be created in advance in ERPS "Ring Network Configuration", and the ring network port should be specified.
Instance ID	The ID of ERPS protection instance, its value range is 0-16. The VLAN in which RAPS PDUs and data packets are transmitted must be mapped to an Ethernet Ring Protection (ERP) instance so that ERPS forwards or blocks the packets based on configured rules. Note: • By default, all VLAN in MST domain are mapped to instance 0. • The mapping with VLAN instance can be created in spanning tree instance configuration.
Ring ID	The ID of ERPS ring network, its value range is 1-239. The

Interface Element	Description
	ring ID is used to uniquely identify an ERPS ring, and all nodes on the same ERPS ring should be configured with the same ring ID. Note: ERPS ring ID will be the last byte of the MAC destination of the RAPS message.
Timer Name	The name of the timer, which supports the default parameter timer or customization in the timer configuration.
RPL Role	Each device in ERPS ring is called a node. The node role is decided by user configuration, they are divided into following types: • owner: owner node is responsible for blocking and unblocking the port in RPL of the node to prevent loop forming and conduct link switching. • neighbor: neighbor node is connected to Owner node on RPL. Cooperating to the Owner node, it blocks and unblocks the ports on RPL of the node and conduct link switching. • non-owner: non-owner node is responsible for receiving and forwarding the protocol packet and data packet in the link.
RPL-Port	Port connected by RPL link, the options are as follows: • West-interface • East-interface
Topology Change Announcement	Notify the network topology change of this ERPS ring to other ERPS rings, and the enabling status is as follows: • Enable • Disable: disable
Manage VLAN	The VLAN channel of protocol packet, its value range is 1-4094.
Level	ERPS ring network level, the value range is 0-7. The higher the ring network level, the greater the value. When the R-APS message needs to be transmitted across the ring, it can only be crossed by the ring with high rank to low rank.
State	The instance statuses of ERPS are as follows: • ERPS_INIT: initial state, which is the initialized state when the protocol starts. • ERPS__IDLE: idle state, it would enter this state when

Interface Element	Description
	the ring topology is complete; • ERPS_FS: force-switch state, it would enter this state when force-switch command is implemented. • ERPS_MS: manual-switch state, it would enter this state when manual-switch command is implemented. • ERPS_PROTECTION: protection state, it would enter this state when the ring link has failure. • ERPS_PENDING: pending state, it would enter this state when the ring link has recovered from failure.
Start	ERPS instance startup status: • start • stop

5.7 IGMP-Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is a kind of IPv4 layer-2 multicast protocol. It maintains the outgoing information of multicast messages by snooping the multicast protocol messages transmitted between layer 3 multicast device and user host, so as to manage and control the forwarding of multicast data messages in data link layer.

5.7.1 Global Configuration

Function Description

Enable/disable IGMP-Snooping and resident multicast.

Operation Path

Open in order: "Layer 2 Configuration > IGMP-Snooping > Global Configuration".

Interface Description

Global configuration interface is as follows:

The main element configuration description of global configuration interface:

Interface Element	Description
Global Enable Switch	Global enable configuration of IGMP-Snooping. By enabling IGMP Snooping, layer 2 devices can dynamically establish layer 2 multicast forwarding entries by listening to the IGMP protocol messages between the IGMP querier and the user host, thus realizing layer 2 multicast.
Permanent Multicast	Do not age the received IGMP report member groups.

5.7.2 Interface Configuration

Function Description

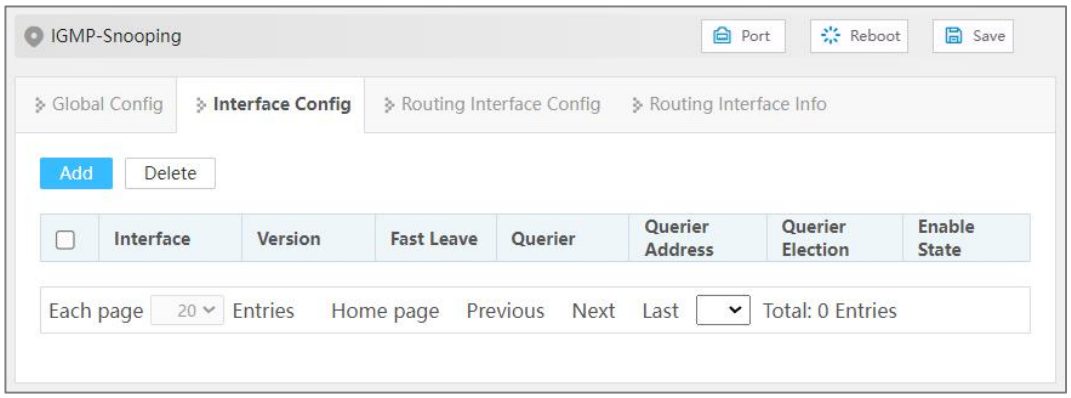
Configure parameters related to IGMP Snooping of VLANIF interface.

Operation Path

Open in order: "Layer 2 Config > IGMP-snooping > Interface Config".

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	VLANIF interface, the value range is 1-4094.
Version	Different versions of IGMP Snooping can handle corresponding versions of IGMP protocol. IGMP Snooping protocol version, with the following options: • 1 • 2 • 3
Fast Leave	The enable state of the multicast group fast leave. After enabling fast leave, when the switch receives the IGMP Leave message sent by the host from a certain port and leaves a certain multicast group, it directly deletes the port from the multicast forwarding table without waiting for the port aging, which can save bandwidth and resources. Note: When there are multiple receivers under the port, this function will cause other receivers in the same multicast group to interrupt receiving multicast data. It is recommended to configure this function on a port with only one receiver connected.
Querier	Enable status of IGMP Snooping inquirer. After the IGMP Snooping querier function is enabled, the switch will regularly send IGMP querier messages to all interfaces (including router ports) in the VLAN by broadcast. If the IGMP querier already exists in the multicast network, it will cause the IGMP querier to be re-elected.
Querier Address	The source IP address of IGMP Snooping querier when sending inquiry message.
Querier Election	Enable election status of IGMP Snooping querier. IGMPv2 uses an independent inquirer election mechanism. When there are multiple multicast routers on the shared network segment, the router with the smallest IP address becomes an inquirer, while the non-inquirer no longer sends universal group inquiry messages.
Enable State	IGMP Snooping enable status, enabling IGMP snooping on global or VLAN interface. Note: Only when IGMP snooping is enabled on the global and VLAN interfaces can the configuration of the other IGMP snooping properties on that interface take effect.

5.7.3 Routing Port Configuration

Function Description

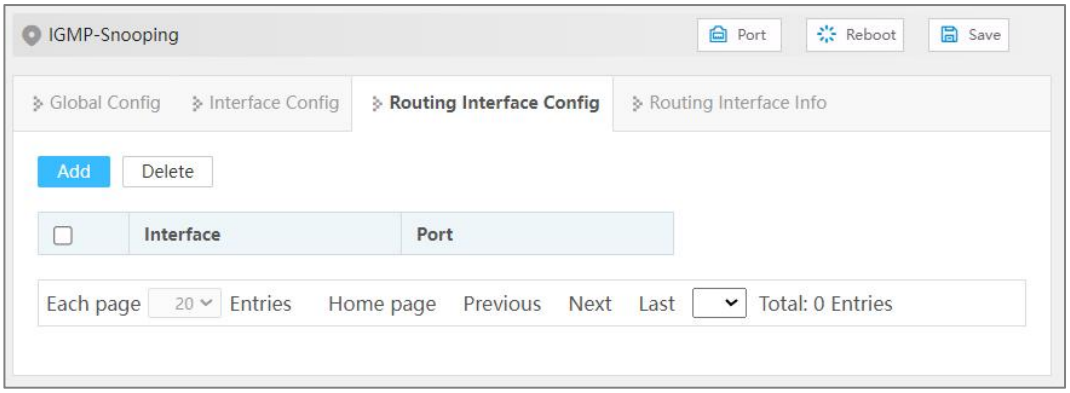
Configure multicast router ports.

Operation Path

Open in order: "Layer 2 Config > IGMP Snooping > Routing Interface Configuration".

Interface Description

Routing interface configuration interface is as below:



Main elements configuration description of routing interface configuration interface:

Interface Element	Description
Interface	VLANIF interface, the value range is 1-4094.
Port	The static router port in VLAN is generally the interface of Layer 2 device towards the upstream Layer 3 multicast device. If it is necessary to forward the IGMP Report/Leave message from an interface to the upstream IGMP querier stably for a long time, the interface can be configured as a static router port.

5.7.4 Routing Interface Information

Function Description

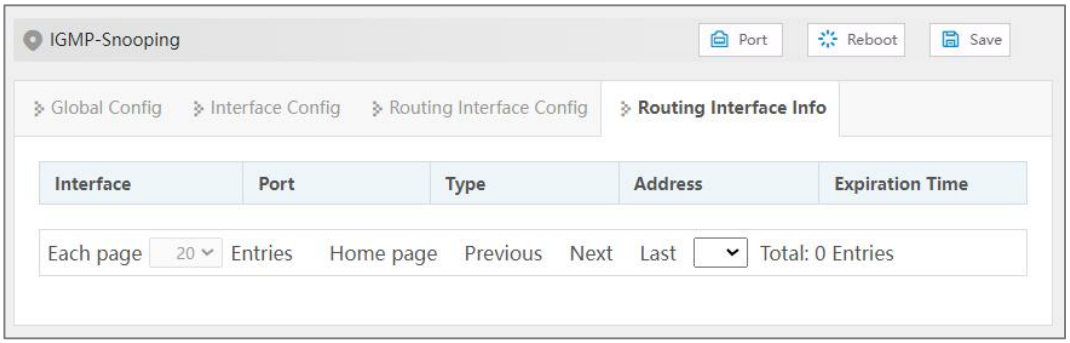
Check the router port information of IGMP Snooping in VLAN, including static router port and dynamic router port.

Operation Path

Open in order: "Layer 2 Config > IGMP Snooping Configuration > Routing Interface Information".

Interface Description

Routing interface information interface is as follows:



Configuration description of main elements of routing port information interface:

Interface Element	Description
Interface	VLANIF interface, the value range is 1-4094.
Port	Router port in VLAN.
Type	The type of router port, including dynamic and static.
Address	IP Address.
Expiration Time	The remaining aging time of dynamic router port.

5.8 Link Flapping Protection

Network jitter or network cable failure will cause frequent Up/Down changes in the physical state of device interface, which will lead to link flapping and frequent changes in network topology, thus affecting user communication. For example, in the application of active-standby link, when the physical Up/Down state of the main link interface changes frequently, the service will switch back and forth between the active-standby link, which will not only increase the device burden, but also cause the loss of service data.

In order to solve the above problems, users can configure the link flapping protection function, and close the interface whose physical Up/Down state changes frequently to keep it remain Down, so that the network topology will stop changing frequently back and forth.

5.8.1 Global Configuration

Function Description

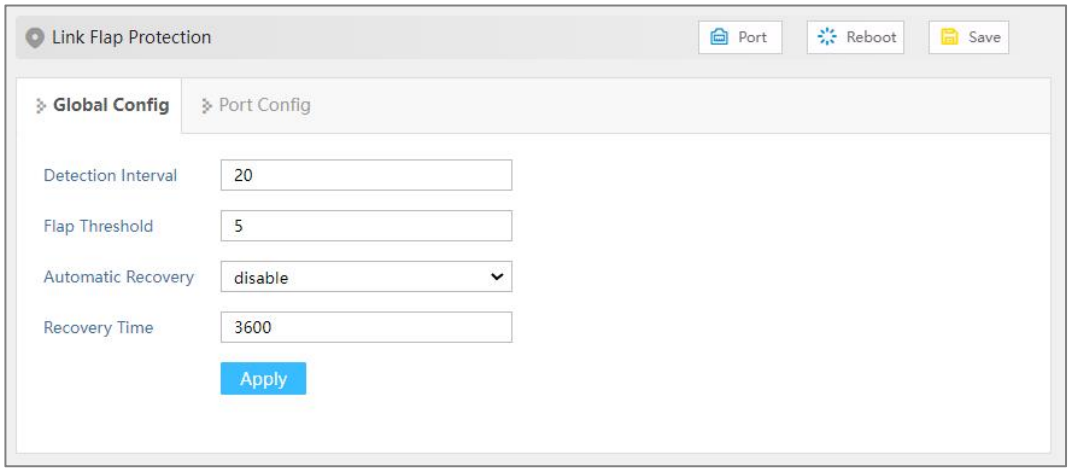
Configure relative parameters of link flapping protection.

Operation Path

Open in order: "Layer 2 Configuration > Link Flapping Protection > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Detection interval	The value range of link detection interval is 10-100s, and the default value is 20s.
Flap Threshold	The threshold value of the number of oscillations detected by the link. If the number of oscillations exceeds the threshold value within the time specified by the "detection interval", an alarm log will be generated and the port will be set to shutdown. The range is from 3 to 100, default value is 5.
Automatic Recovery	Automatic recovery enable configuration. After being enabled, the port will automatically return to normal within the specified time.
Recovery Time	The value range of the time when the port automatically returns to normal is 30-86400s, and the default value is 3600s.

5.8.2 Port Configuration

Function Description

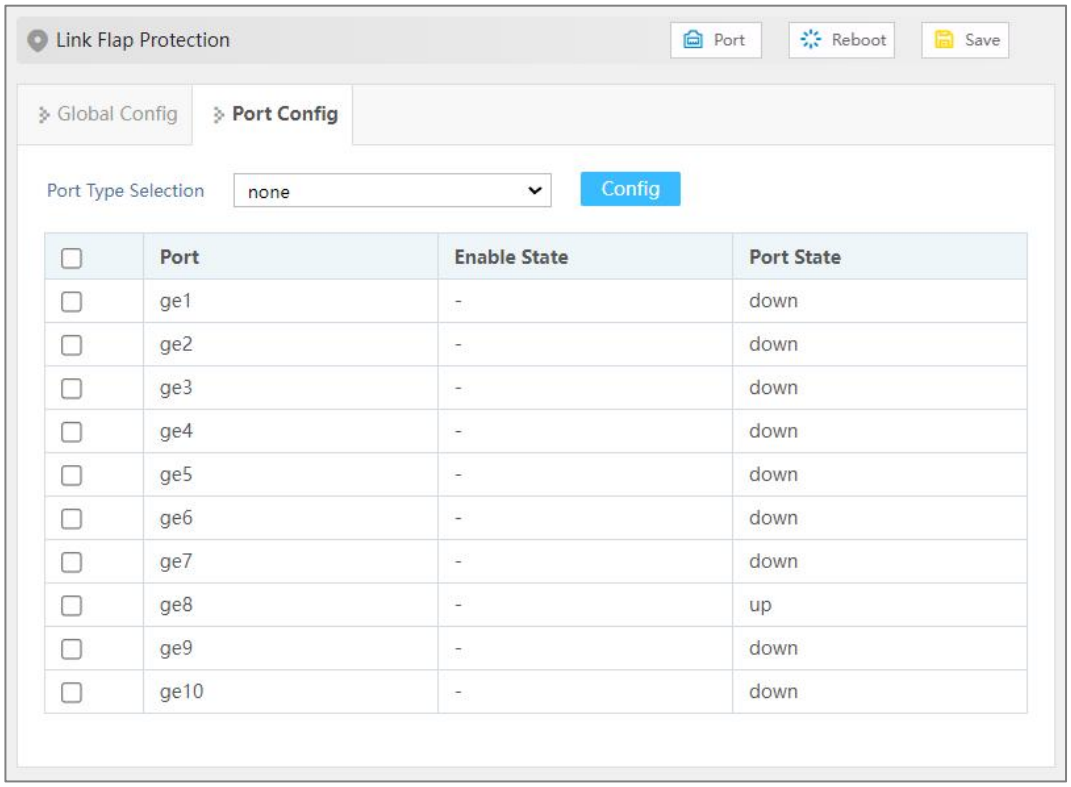
Enable link oscillation protection for this port.

Operation Path

Open in order: "Layer 2 Configuration > Link Flapping Protection > Port Configuration".

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port number of this device's Ethernet port.
Enable State	The enable status of port link flapping protection can be shown as follows: • ON: means enabled; • -:means disable
Port State	Ethernet port connection status, display as follows: • down: the port is not connected or forced to shutdown • up: port is connected.

5.9 Port Loopback Detection

The function of loop detection is to detect whether loop exists in external network of single port of switch. If it does, it would lead to address learning errors and broadcast storm easily, even switch and network breakdown in severe case. The influence created by port loop could be effectively eradicated when enabling port protocol and closing port with loop.

Function Description

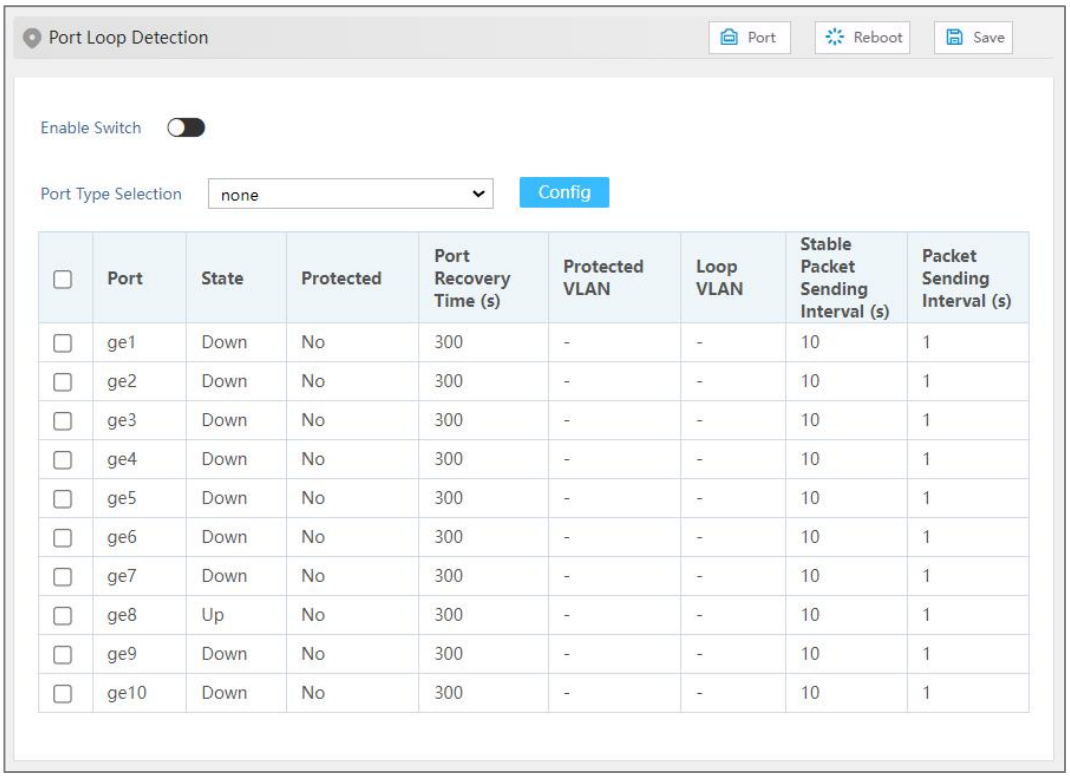
Enable port loop detection.

Operation Path

Open in order: "Layer 2 Config > Port Loop Detection".

Interface Description

Port loop detection interface is as follows:



The main element configuration description of port loop detection interface:

Interface Element	Description
Enable	Global enable configuration of port loop detection.

Interface Element	Description
Port	The corresponding port number of this device's Ethernet port.
State	The connection status of this port, values are: • Down: the port is physically disconnected • Up: the port is connected • Shutdown: the port is closed • No Shutdown: the port is not closed
Protected	The protected status of the port can be shown as follows: • Yes • No
Port Recovery Time (s)	The delay time for the shutdown port to automatically return to normal after detecting the loop, ranging from 300-776000 seconds.
Protected VLAN	The VLAN ID of loop protection. The value range: 1-4094, the number of VLAN ID is ≤16. Note: This parameter must be configured, otherwise there would be errors in down sending the data.
Loop VLAN	The VLAN ID of the currently generated loop.
Stable Packet Sending Interval (s)	The normal interval time of loop detection data packet sending, value range: 10-300 seconds.
Packet sending interval (s)	After the port is connected, the interval between sending loop detection packets. In this interval, three detection messages will be sent out, and then the packet-sending interval will return to the normal packet-sending interval.

5.10 Smart-link

Smart Link, also known as backup link. A Smart Link consists of two interfaces, one of which is the backup of the other. Smart Link is commonly used in dual uplink networking, providing reliable and efficient backup and fast switching mechanism.

5.10.1 Global Configuration

Function Description

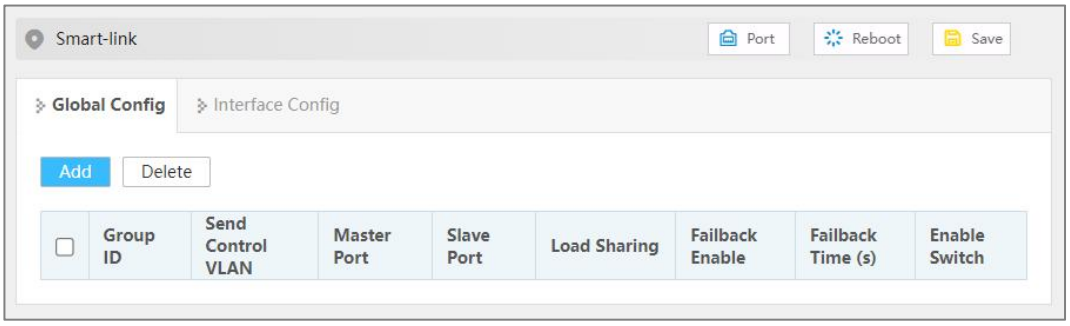
Configure Smart-link related parameters.

Operation Path

Open in order: "Layer 2 Config > Smart-link > Global Config".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Group ID	Smart Link Group ID, the value range is 1-16.
Send Control VLAN	Sending control VLAN is the VLAN used by Smart Link group to broadcast Flush message, and its value range is 1-4094. When Smart Link switches links, Smart Link notifies related devices to refresh MAC table and ARP table entries by sending Flush message. Note: • If the sending control VLAN is configured, the peer device needs to configure the receiving control VLAN. • Different device manufacturers may have different definitions of Flush message format, so it is recommended to use this function between the device of the same manufacturer.
Master Port	When both interfaces in the Smart Link group are in the Up state, the master interface will enter the forwarding state first, while the slave interface will remain in the standby state. Note: Smart Link group port cannot be used as a member port of ring network, aggregation group, etc.
Slave Port	Slave interfaces in the Smart Link group will be blocked after the Smart Link group is started. When the link where the master interface is located fails, the slave interface will switch to the forwarding state.
Load Sharing	Load sharing instance ID, the value range is 0-16. In the load sharing mode, the backup link forwards the VLAN data traffic

Interface Element	Description
	mapped in the specified load sharing instance, which can improve the utilization rate of the link.
Failback Enable	When the original main link recovers from faults, it will remain at the block state to keep the traffic stable without preemption. If you need to restore it to the main link, you can enable the failback function of the Smart Link group, the main link would be automatically switched after the failback timer expires. Switch-back enable status, which can be displayed as follows: • Enable • Disable: disable
Failback Time (s)	Failback delay time, it can inhibit Smart Link switching caused by link flash, the value range is 30~1200 seconds.
Enable	Smart Link function enable status can be displayed as follows: • Enable • Disable: disable

5.10.2 Interface Configuration

Function Description

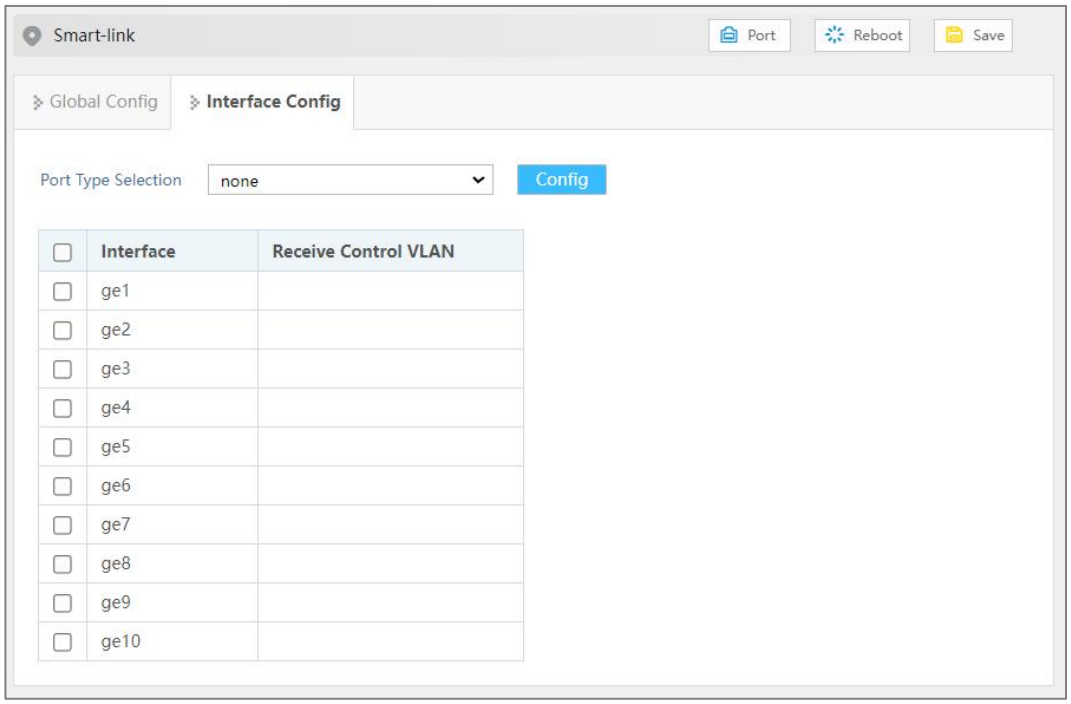
Configure Smart-link interface to receive control VLAN.

Operation Path

Open in order: "Layer 2 Config > Smart-link > Interface Config".

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	The corresponding port number of this device's Ethernet port.
Receive Control VLAN	Receive control VLAN is used to receive and handle the VLAN of Flush messages, the value range is 1-4094. When Smart Link has switched links, the device would handle the Flush messages received that belong to receive control VLAN, thus refreshing MAC table and ARP table.

6 IP Network Configuration

6.1 Interface

6.1.1 Layer 3 Interface

Function Description

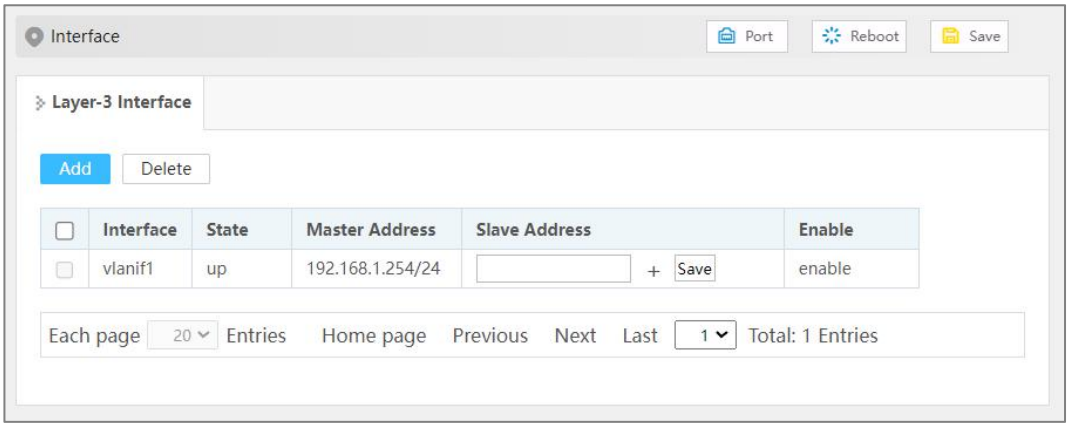
Create layer 3 VIANIF Interfaces and configure interface IP address.

Operation Path

Open in order: "IP Network Configuration > Interface > L3 Interface".

Interface Description

L3 interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	VLANIF interface, the value range is 1-4094. VLANIF interface is a logical interface with layer 3 features that can be used to realize inter-VLAN access and Layer 3 task

Interface Element	Description
	deployment by configuring the IP address of VLANIF Interfaces.
State	The connection state of the VLANIF port, which can be displayed as follows: • Up: connection is normal. • Down: disconnected
Master Address	Master IPv4 address and subnet mask of VLANIF interface, such as 192.168.1.1/24.
Slave Address	Slave IPv4 address and subnet mask of VLANIF interface, such as 192.168.8.1/24. In order to connect one interface of the switch with multiple subnets, user can configure multiple IP addresses on one interface, one as the master IP address and the rest as the slave IP address.
Interface switch	The VLANIF interface enabled status can be displayed as follows: • enable • disable

6.2 ARP

ARP (Address Resolution Protocol) is the protocol that resolves IP address into Ethernet MAC address (or physical address).

In local area network, when the host or other network device sends data to another host or device, it must know the network layer address (IP address) and MAC address of the opposite side. So it needs a mapping from IP address to the physical address. ARP is the protocol to achieve the function.

6.2.1 ARP Information

Function Description

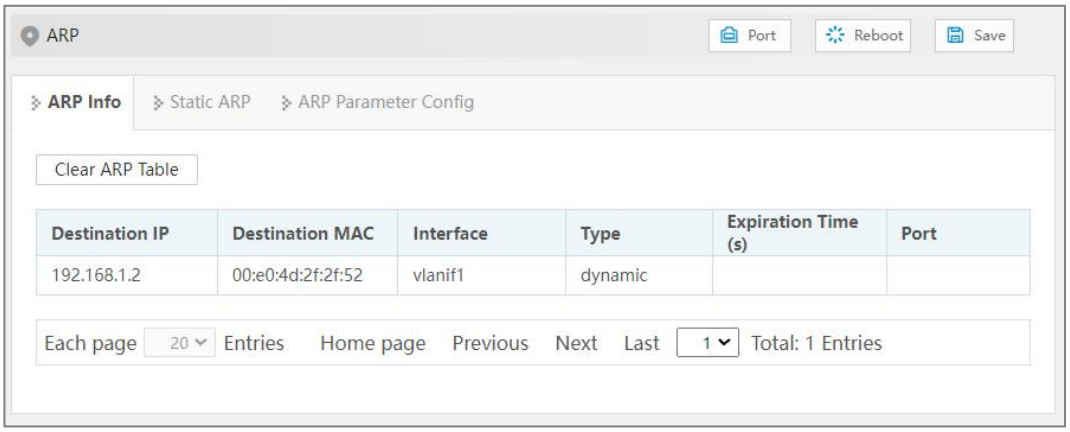
Check information such as IP address, MAC address and interface of the user via ARP table entries.

Operation Path

Open in order: "IP Network Configuration > ARP > ARP Information".

Interface Description

ARP Information interface as follow:



The main element configuration description of ARP information interface:

Interface Element	Description
Destination IP	Static binding or ARP resolves dynamically learned IP addresses.
Destination MAC	Static binding or ARP resolves dynamically learned MAC addresses.
Interface	VLANIF Interface to which ARP entry belongs.
Type	ARP table entry type, as shown below: • Static • Dynamic
Expiration Time (s)	The remaining survive time of dynamic ARP table entries, unit: second.
Port	Ports learned to ARP table entry.

6.2.2 Static ARP

Function Description

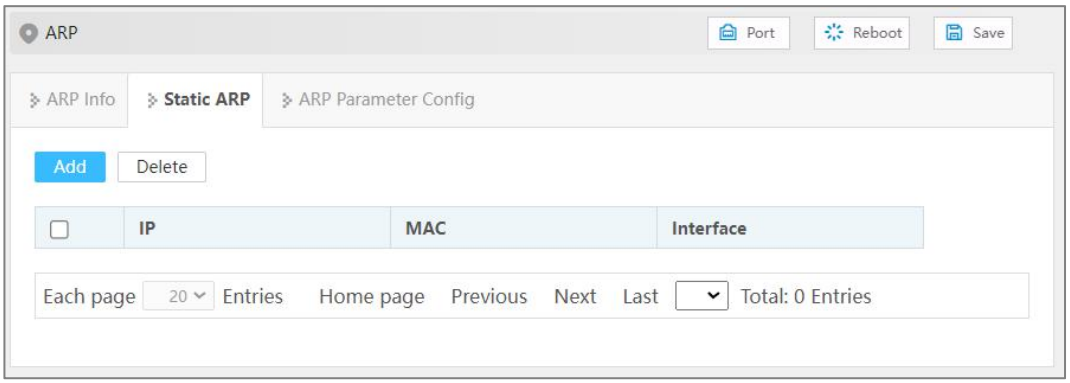
Configure static ARP entries, bind IP address and MAC address to avoid aging and prevent ARP attacks.

Operation Path

Open in order: "IP Network Configuration > ARP > Static ARP".

Interface Description

Static ARP interface as follows:



The main element configuration description of static ARP interface:

Interface Element	Description
IP	IP address of static ARP table entry, such as 192.168.1.1.
MAC	MAC address bound to static IP address such as 0001.0001.0001.
Interface	Display VLANIF Interface to which static ARP entry belongs.

6.2.3 ARP Parameter Configuration

Function Description

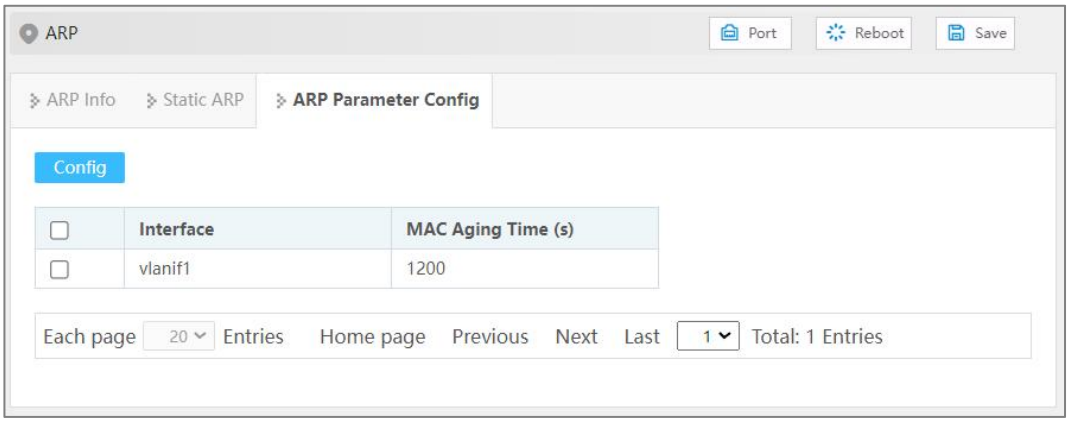
Configure the aging time of dynamic ARP.

Operation Path

Open in order: "IP Network Configuration > ARP > ARP Parameters Configuration".

Interface Description

ARP parameter configuration interface as follows:



The main element configuration description of ARP parameter configuration interface:

Interface Element	Description

Interface Element	Description
Interface	Display VLANIF Interface name in ARP entry.
MAC Aging Time	Configure aging time of dynamic ARP table entries, the value range is 1-3000 seconds.

6.3 IPv4

6.3.1 IPv4 Routing Table

Function Description

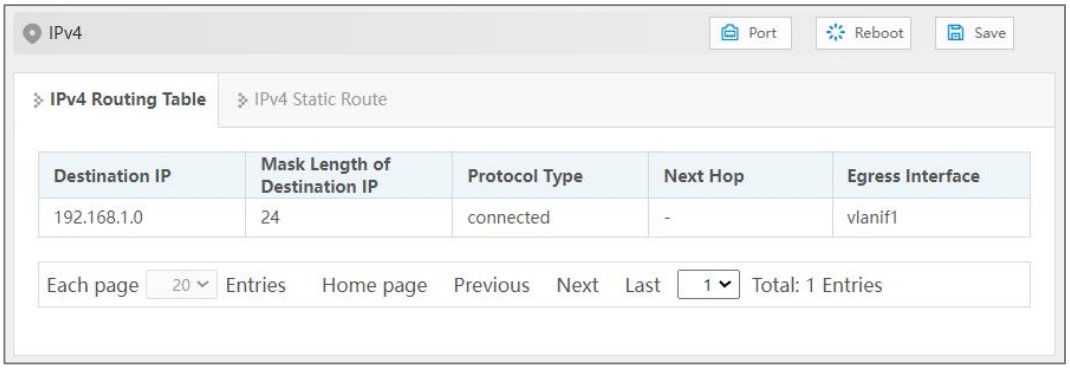
Check IPv4 routing table information.

Operation Path

Open in order: "IP Network Configuration > IPv4 > IPv4 Routing Table".

Interface Description

The IPv4 routing table interface as follows:



The main elements configuration description of IPv4 routing interface:

Interface Element	Description
Destination IP	Destination IP addresses.
Mask Length of Destination IP	The length of destination subnet mask.
Protocol Type	The routing protocol type of the current connection.
Next Hop	Gateway address information of next hop.
Egress Interface	Interface Name.

6.3.2 IPv4 Static Route

Static route refers to the route information that user or network administrator manually configures. When the network topology structure or link status changes, network administrator needs to manually modify relative static route information in the routing table. Static route usually adapts to simple network environment, under this environment, network administrator can clearly know the network topology structure, which is convenient for setting correct route information.

Function Description

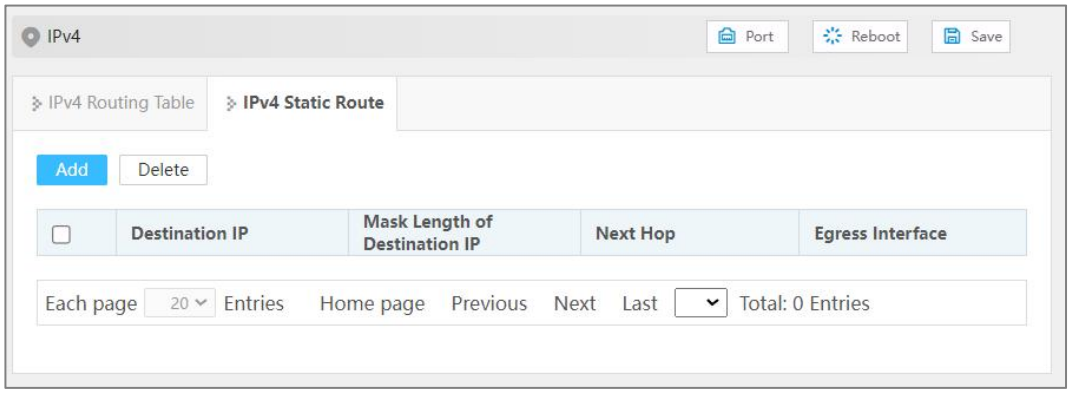
Configure IPv4 static routing.

Operation Path

Open in order: "IP Network Configuration > IPv4 > IPv4 Static Route".

Interface Description

The IPv4 Static Route interface as follows:



The main element configuration description of IPv4 Static Route interface:

Interface Element	Description
Destination IP	Destination network IP address, such as destination address is 10.1.1.0.
Mask Length of Destination IP	Destination IP mask length. Value range is 0-32.
Next Hop	The gateway address of the next hop, format: no input or 192.3.3.3.
Egress Interface	Interface Name.

7 Network Management

7.1 SNMP

Now, the broadest network management protocol in network is SNMP (Simple Network Management Protocol). SNMP is the industrial standard that is widely accepted and comes into use, it's used for guaranteeing the management information transmission between two points in network, and is convenient for network manager search information, modify information, locate faults, complete fault diagnosis, conduct capacity plan and generate a report. SNMP adopts polling mechanism and only provides the most basic function library, especially suit for using in minitype, rapid and low price environment. SNMP implementation is based on connectionless transmission layer protocol UDP, therefore, it can achieve barrier - free connection to many other products.

7.1.1 SNMP Switch

Function Description

Enable/disable SNMP function.

Operation Path

Open in order: "Network Management > SNMP > SNMP Switch".

Interface Description

SNMP switch interface is as follows:

The main element configuration description of SNMP switch interface:

Interface Element	Description
Enable	SNMP enable switch, which is enabled by default Note: If the agent side has opened, the SNMP server can't be closed.

7.1.2 View

Function Description

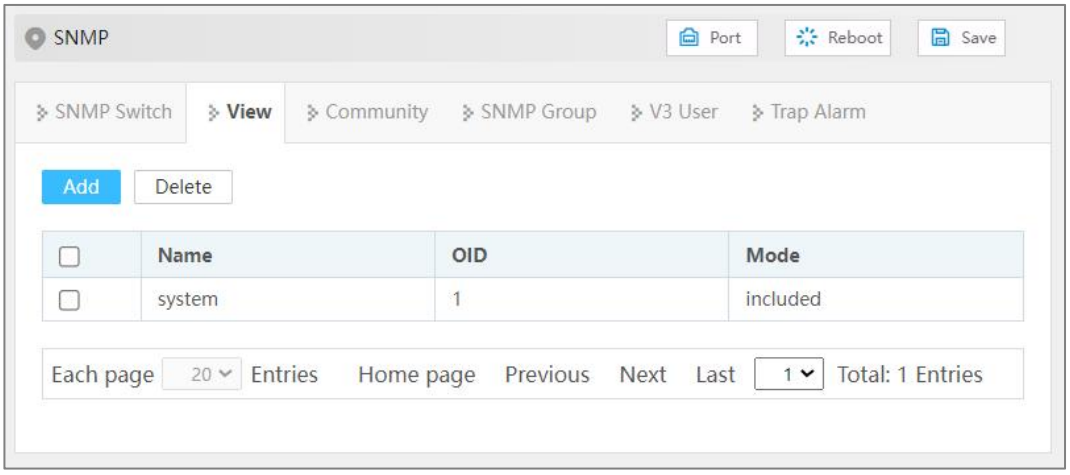
Add/delete SNMP view.

Operation Path

Open in order: "Network Management > SNMP > View".

Interface Description

View interface as below:



The main element configuration description of view interface:

Interface Element	Description
Name	SNMP view name definition, support 32 characters input.

Interface Element	Description
OID	Node location information of MIB tree where the device resides. Note: • OID object identifier, a component node of MIB, uniquely identified by a string of numbers that represent the path. • The information of OID could be viewed via the third-party software MG-SOFT MIB Browser.
Mode	Node OID dealing method, options as below: • Included: It contains all objects under the node subtree; • Excluded: Eliminate all objects beyond the node subtree.

7.1.3 Community

Function Description

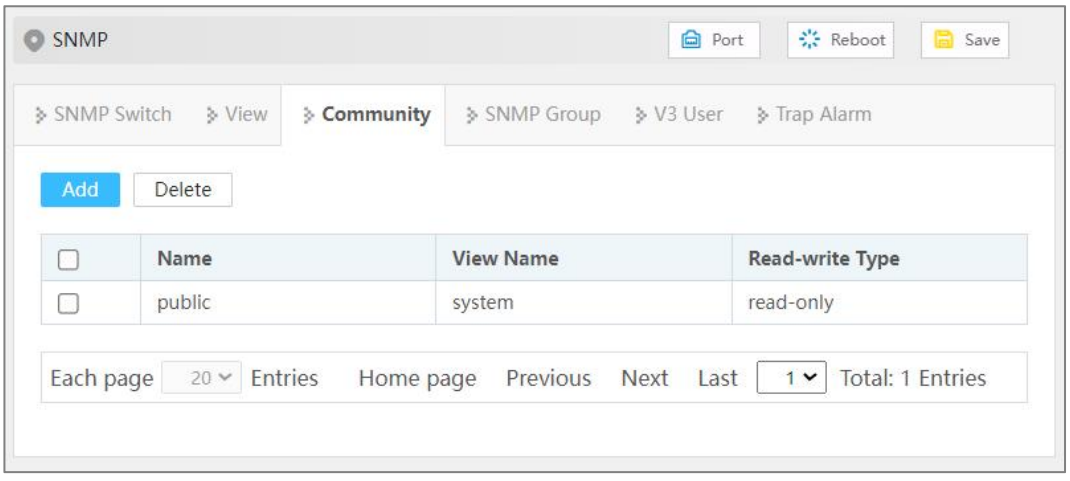
Add/delete SNMP community. Define MIB view that community name can access, set MIB object access privilege of community name as read-write privilege or read-only privilege.

Operation Path

Open in order: “Network Management > SNMP > Community”.

Interface Description

Community interface as below:



The main element configuration description of community interface:

Interface Element	Description
Name	Group name, including numbers or letters, with a length of

Interface Element	Description
	no more than 32 characters.
View Name	SNMP view name.
Read-Write Type	View read-write permissions, options are as follows: • Read only • Read and write

7.1.4 SNMP Group

Function Description

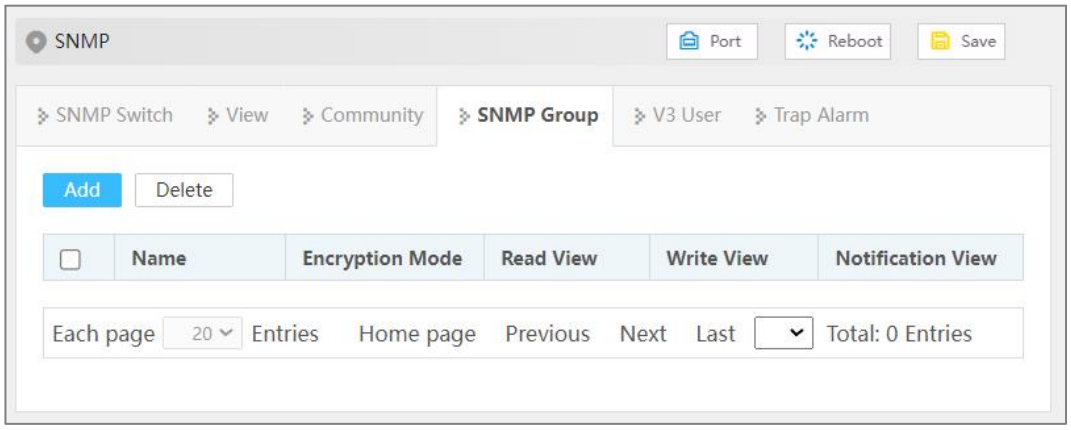
Configure a new SNMP group and set the secure mode and corresponding SNMP view of the SNMP group.

Operation Path

Open in order: “Network Management > SNMP > SNMP Group”.

Interface Description

SNMP Group interface as follows:



Main elements configuration description of SNMP Group interface:

Interface Element	Description
Name	SNMP group name, ranging from 1 to 32 bytes.
Encryption Mode	Whether to authenticate and encrypt the message, values: • auth: indicates that the message is authenticated but not encrypted; • noauth: indicates that the message is neither authenticated nor encrypted; • priv: indicates that the message is authenticated and

Interface Element	Description
	encrypted.
Read View	Specify the read view of the group.
Write View	Specify the write and read view of the group
Notification View	Specify the notification view of the group.

7.1.5 V3 User

Function Description

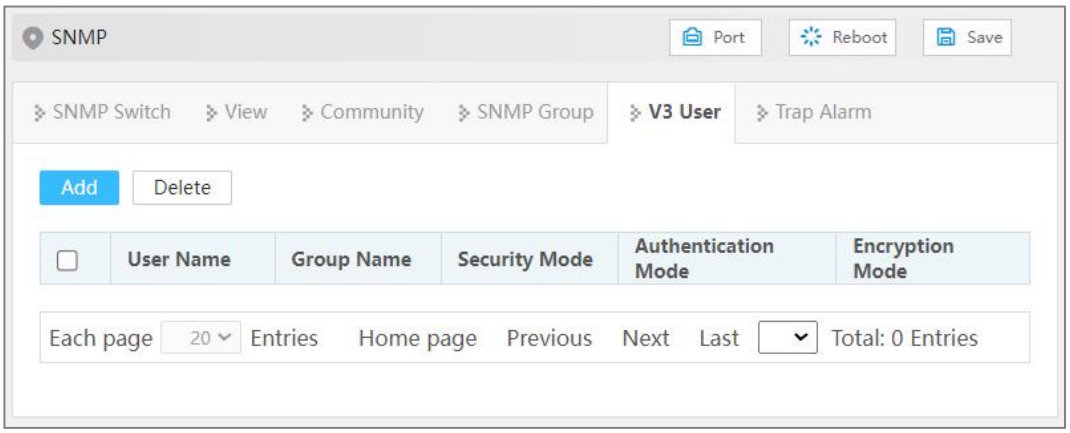
SNMPv3 adopts User-Based Security Model (USM) authentication mechanism. Network manager can configure authentication and encryption function. Authentication is used to verify the validity of the packet sender and prevent unauthorized users from accessing it. Encryption encrypts the transmission packet between NMS and Agent to prevent eavesdropping. It adopts authentication and encryption function to provide higher security for the communication between NMS and Agent.

Operation Path

Open in order: "Network Management > SNMP > V3 Users".

Interface Description

V3 user interface as follows:



The main element configuration description of V3 user interface:

Interface Element	Description
Username	SNMP v3 user name definition, can only contain numbers, letters, or @_! , no longer than 32 characters.

Interface Element	Description
Group Name	Group name, ranging from 1 to 32 bytes. Note: Group name must be created snmp group, and only created group can create SNMP v3 users.
Security Mode	Whether to authenticate and encrypt the message, values: • auth: indicates that the message is authenticated but not encrypted; • noauth: indicates that the message is neither authenticated nor encrypted; • priv: indicates that the message is authenticated and encrypted.
Authentication Mode	Authentication mode type, acceptable value: • Md5: Information abstract algorithm 5; • Sha: Secure hash algorithm.
Encryption Mode	V3 user data encryption algorithm, options as follows: • Des: Adopt data encryption algorithm; • Aes: Adopt advanced encryption standard.

7.1.6 Trap Alarm

Function Description

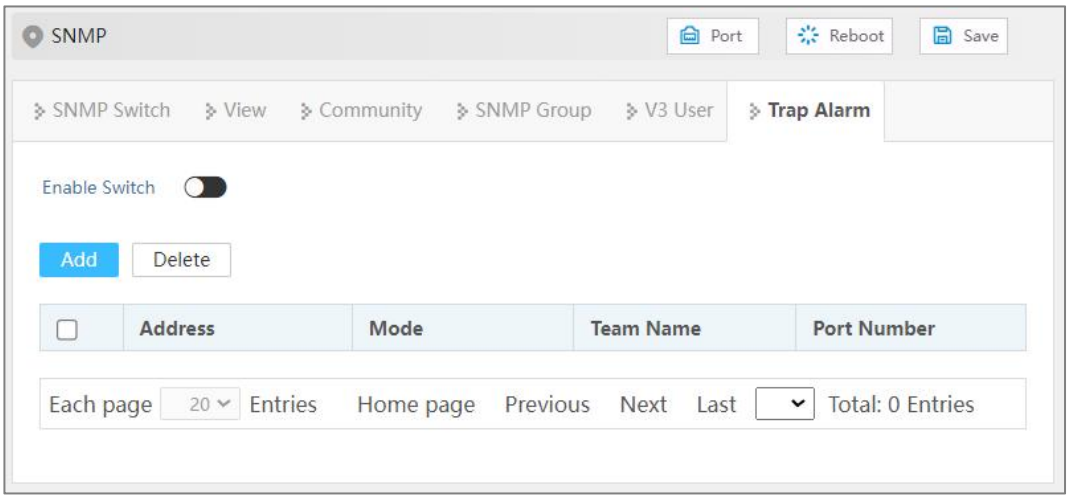
Base on TCP/IP protocol, SNMP usually adopts UDP port 161 (SNMP) and 162 (SNMP-traps), SNMP protocol agent exists in the network device and adopts information specific to the device (MIBs) as the device interface; these network devices can be monitored or controlled via Agent. When a trap event occurs, the message is transmitted by SNMP Trap. At this point, an available trap receiver can receive the trap message.

Operation Path

Open in order: "Network Management > SNMP > trap Alarm".

Interface Description

Trap alarm interface as below:



The main element configuration description of Trap alarm interface:

Interface Element	Description
Enable	SNMP Trap alarm enable switch.
Address	IP address of SNMP management device, used for receiving alarm information, such as PC.
Mode	SNMP management device version, options as below: • v1 • v2c
Team Name	Group name.
Port Number	Port number of Trap, it defaults to 162, the value range is 0～65535.

7.2 LLDP

LLDP (Link Layer Discovery Protocol) is a link layer discovery protocol defined in IEEE 802.1ab. LLDP is a standard layer-2 discovery method, which can organize the management address, device identification, interface identification and other information of local devices and publish it to its neighbor devices. After receiving the information, the neighbor devices save it in the form of standard MIB(Management Information Base) for the network management system to query and judge the communication status of links.

7.2.1 Global Configuration

Function Description

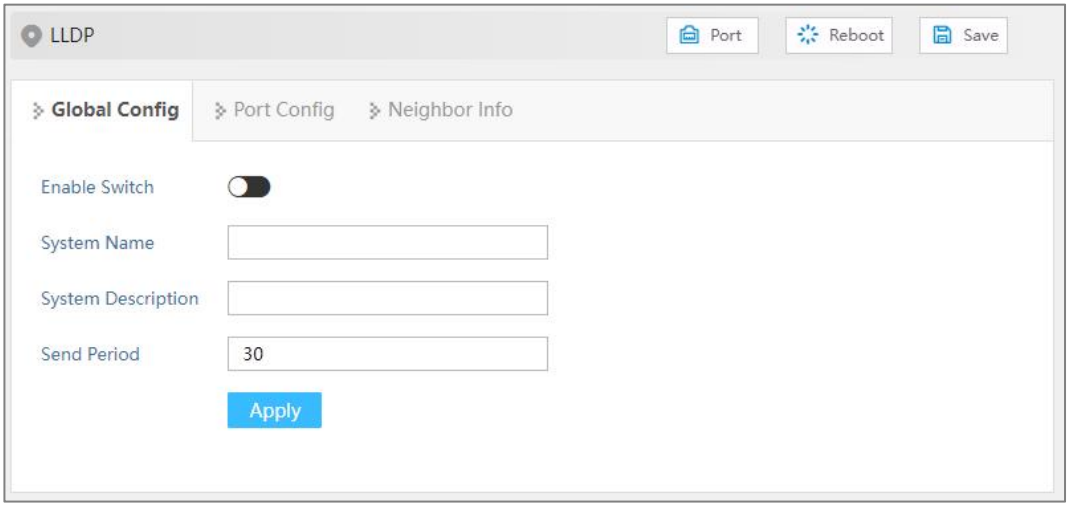
Configure LLDP global parameter.

Operation Path

Open in order: "Network Management > LLDP > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Enable	LLDP enable switch.
System Name	The system name, which supports 0-32 characters, consists of uppercase letters, lowercase letters, numbers or special characters (! @ _-).
System Description	The system description information, which supports 0-32 characters, consisting of uppercase letters, lowercase letters, numbers or special characters (! @ _-).
Send Period	LLDP message sending cycle, the value range is 5-32768. When no device status changes, the device periodically sends LLDP messages to its adjacent nodes. Note: Type of TLV (Type/Length/Value) encapsulated by LLDP message, which can include system name and system description.

7.2.2 Port Configuration

Function Description

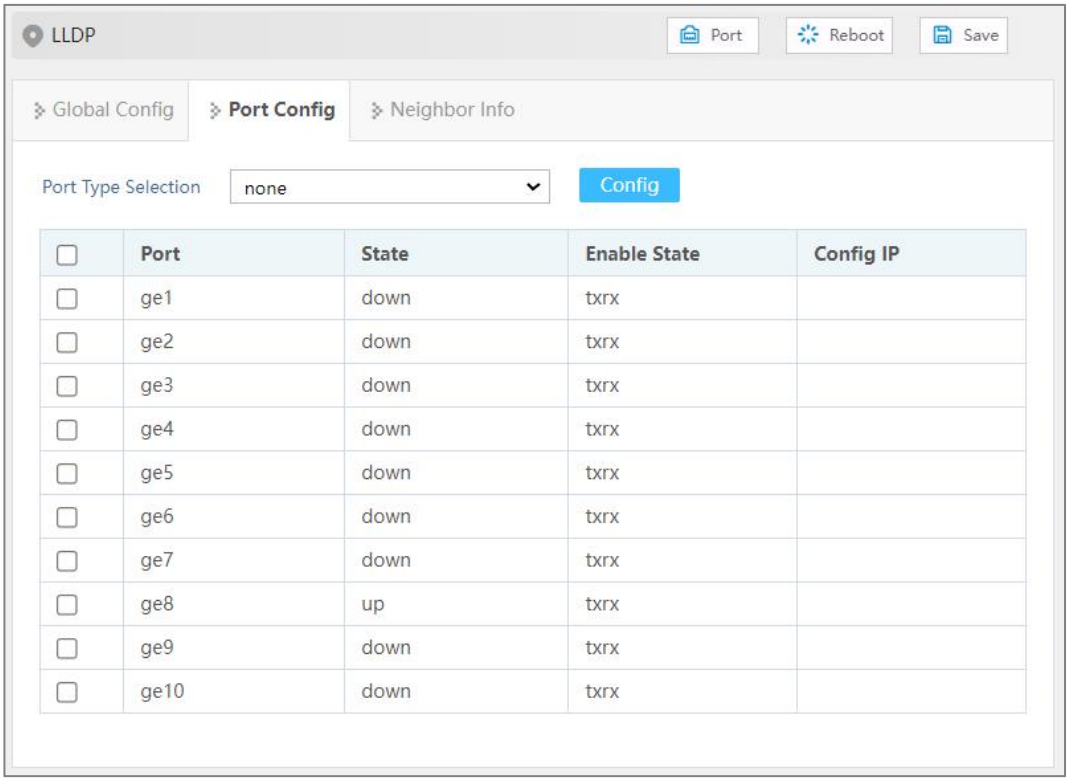
Configure the sending and receiving mode and management address of the port.

Operation Path

Open in order: "Network Management > LLDP > Port Configuration".

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
State	Ethernet port connection status, display status as follows: • down: port is disconnected • up: port is connected
Enable State	The options of LLDP working states of device port are as follows: • txonly: working mode is Tx, only sending and not receiving LLDP message. • rxonly: working mode Rx, only receiving and not sending LLDP message.

Interface Element	Description
	• txrx: working mode is TxRx, both sending and receiving LLDP message. • disable: work mode is Disable, it neither transmits nor receives LLDP message. Note: When global LLDP is enabled, the work mode of LLDP is TxRx by default.
Config IP	Corresponding LLDP management IP address of the port. Note: • LLDP management address is the address to be marked and managed by network management system. Management address can definitely mark a device, which is beneficial to the drawing of network topology and network management. Management address is encapsulated in Management Address TLV field of LLDP message and sent to adjacent nodes. • The management address released by the port in the LLDP message defaults to the main IP address of the smallest VLAN of the VLANs this port is in. If the VLAN is not configured with a main IP address, it will be 0.0.0.0.

7.2.3 Neighbor Information

Function Description

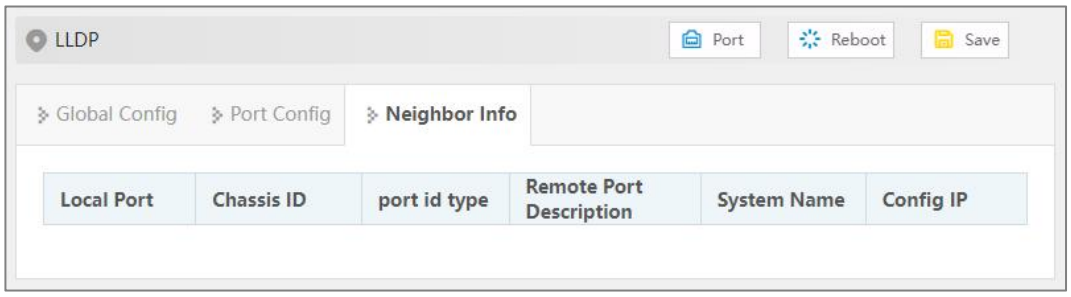
View neighbor-related information.

Operation Path

Open in order: " Network Management > LLDP > Neighbor Information".

Interface Description

Neighbor information interface as follows:



Main elements configuration description of neighbor information interface:

Interface Element	Description

Interface Element	Description
Local port	Local port number of local switch connected to adjacent devices.
Chassis ID	Neighbor device ID.
port id type	Subtype of neighbor port ID.
Remote Port Description	Port number of neighbor device.
System Name	System name of the neighbor device.
Config IP	Management IP address of neighbor device or port.

8 System Maintenance

8.1 Network Diagnosis

8.1.1 Ping

Function Description

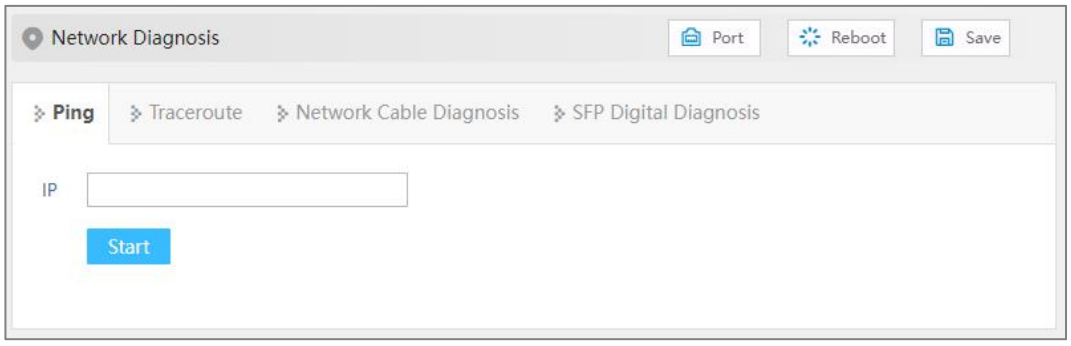
Ping is used to check whether the network is open or network connection speed. Ping utilizes the uniqueness of network machine IP address to send a data packet to the target IP address, and then ask the other side to return a similarly sized packet to determine whether two network machines are connected and communicated, and confirm the time delay.

Operation Path

Open in order: "System Maintenance > Network Diagnosis > Ping".

Interface Description

The Ping interface is as follows:



The main elements configuration description of Ping configuration interface:

Interface Element	Description
IP	The IPv4 address of the detected device, that is, the

Interface Element	Description
	destination address. The device can check the network intercommunity to other devices via the ping command.

8.1.2 Traceroute

Function Description

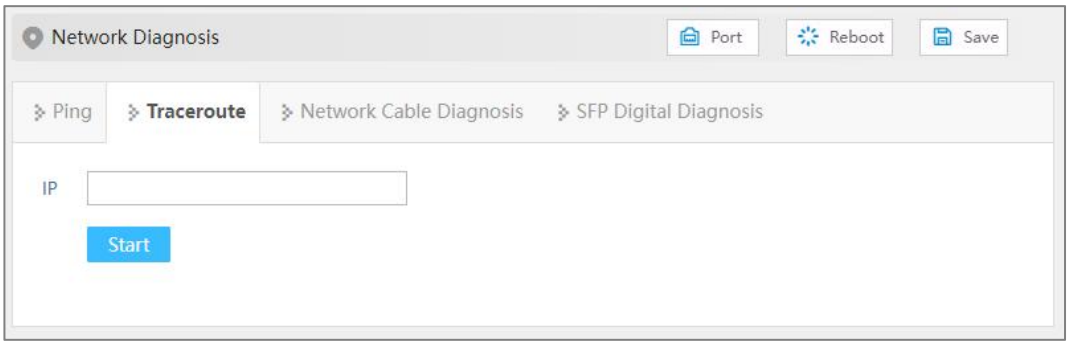
Test the network situation between the switch and the target host. Traceroute measures how long it takes by sending small packets to the destination device until they return. Each device on a path Traceroute returns three test results. Output result includes each test time (ms), device name (if exists) and the IP address.

Operation Path

Open in order: "System Maintenance > Network Diagnosis > Traceroute".

Interface Description

Traceroute interface as follows:



The main element configuration description of Traceroute interface:

Interface Element	Description
IP	Destination device IPv4 address, fill in the opposite device IP address that needs test.

8.1.3 Network Cable Diagnosis

Function Description

It can detect whether there is a fault in the cable used by the copper port of the device. When the cable is in normal condition, the length in the detection information refers to the total length of the cable. When the cable is in abnormal condition, the length in the

detection information refers to the length from this interface to the fault location. The 8-wire network cable has 4 groups of differential lines, and the device can detect the length and status of each group of differential lines.

Note

- The accuracy of detecting cable length is about 5 meters, and the test results are for reference only. The test results of different types or different manufacturers may be different.
- When testing, it will affect the normal use of the interface business in a short time, and may also cause the interface of UP to oscillate.

Operation Path

Open in order: "System Maintenance > Network Diagnosis > Network Cable Diagnosis".

Interface Description

Network cable diagnosis interface screenshot is as follows:

Main elements configuration description of network cable diagnosis interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
State of Pair A/B/C/D	The state of the differential line, such as OK (normal), OPEN (open circuit), SHORT (short circuit), CROSS (cross/crosstalk), etc.
Length of Pair A/B/C/D (m)	Length of the differential line, unit: meter.

8.1.4 SFP Digital Diagnosis

Function Description

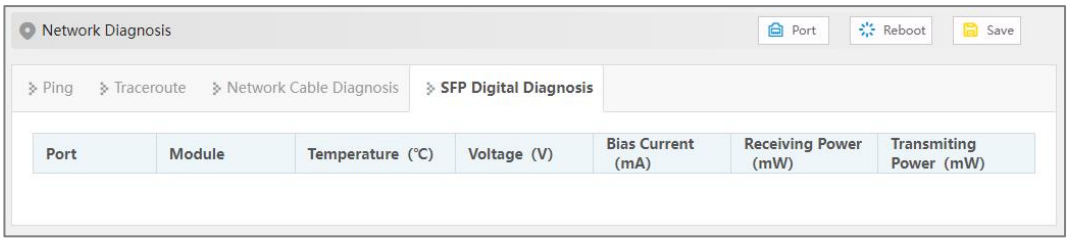
Monitor SFP parameters in real time. This function has greatly facilitated the troubleshooting process of optical fiber link and the cost of on-site debugging.

Operation Path

Open in order: "System Maintenance > Network Diagnosis > SFP Digital Diagnosis".

Interface Description

The SFP digital diagnostic interface is as follows:



The main element configuration description of SFP digital diagnosis interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Module	Parameter information of optical module:
Temperature(℃)	This device's SFP temperature. Its unit is ℃. The operating temperature of this SFP module should be within the temperature range of normal operation.
Voltage (V)	The voltage that this device offers SFP. Its unit is V. Overvoltage could lead to the breakdown of CMOS device; under voltage would disable the normal operation of lasers.
Bias Current (mA)	The bias current of laser.
Receiving Power (mW)	Optical input power, referring to the lowest optical power of receiving in certain rate and bit error rate.
Transmiting Power (mW)	Optical output power, referring to the output power of optical source in the sending end of optical module.

8.2 Time

8.2.1 NTP Configuration

NTP protocol refers to Network Time Protocol. Its destination is to transmit uniform and standard time in international Internet. Specific implementation scheme is appointing several clock source websites in the network to provide user with timing service, and these websites should be able to mutually compare to improve the accuracy. It can provide millisecond time correction, and is confirmed by the encrypted way to prevent malicious protocol attacks.

Function Description

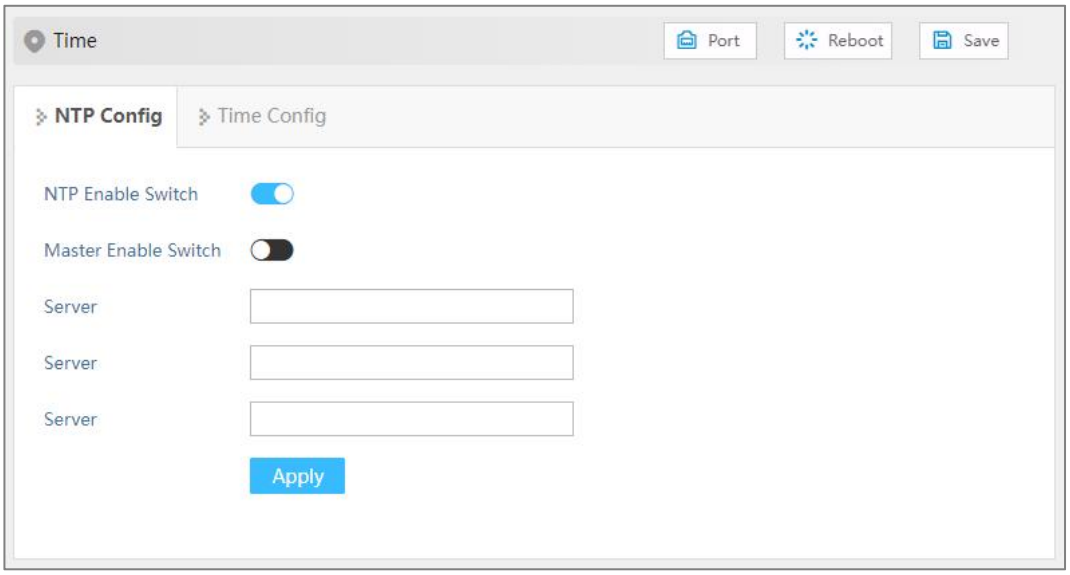
Configure the device time and NTP server information.

Operation Path

Open in order: "System Maintenance > Time > NTP Configuration".

Interface Description

The NTP configuration interface is as follows:



The main element configuration description of NTP configuration interface:

Interface Element	Description
NTP Enable	NTP protocol enable switch.
Master Enable Switch	Master enable switch, after enabled, the device starts NTP service, and uses the local clock of the device as NTP master clock to provide clock source for other devices.

Interface Element	Description
Server	IP address of NTP server, for example: 192.168.1.1. Note: As NTP client, the system will synchronize time with NTP server every 11 minutes.

8.2.2 Time Zone Configuration

Function Description

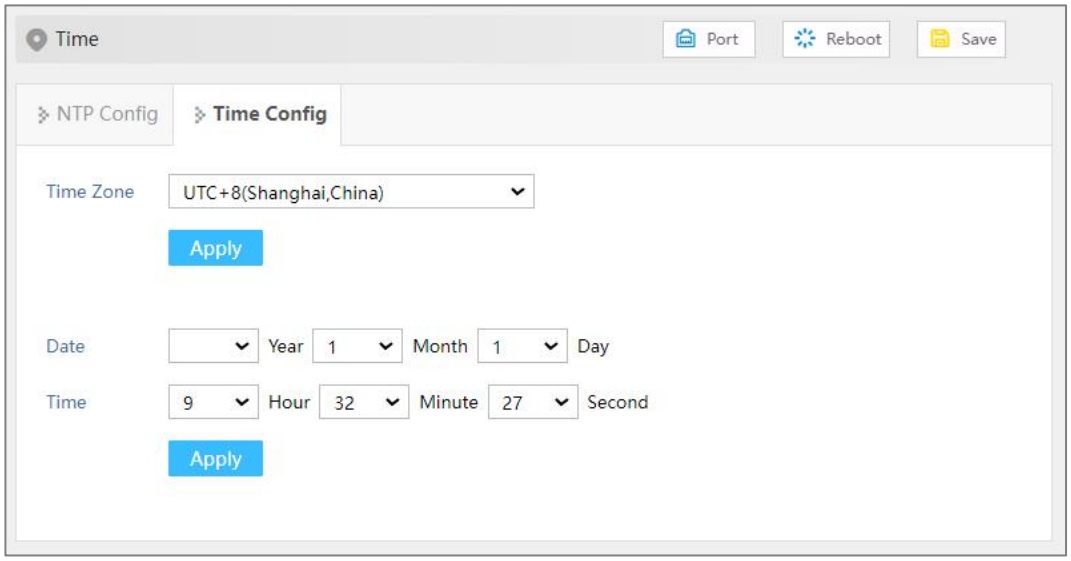
Configure the device time zone.

Operation Path

Open in order: "System Maintenance > Time > Time Zone Configuration".

Interface Description

Time Zone Configuration interface as follows:



Main elements configuration description of time zone configuration interface:

Interface Element	Description
Timezone	UTC (Universal Time Coordinated) time zone. Due to different regions, users can freely set the system clock according to the regulations of their own country or region.
Date	Data configuration, year/month/day.
Time	Time configuration, hour/minute/second.

8.3 Alarm

8.3.1 Port Alarm

Function Description

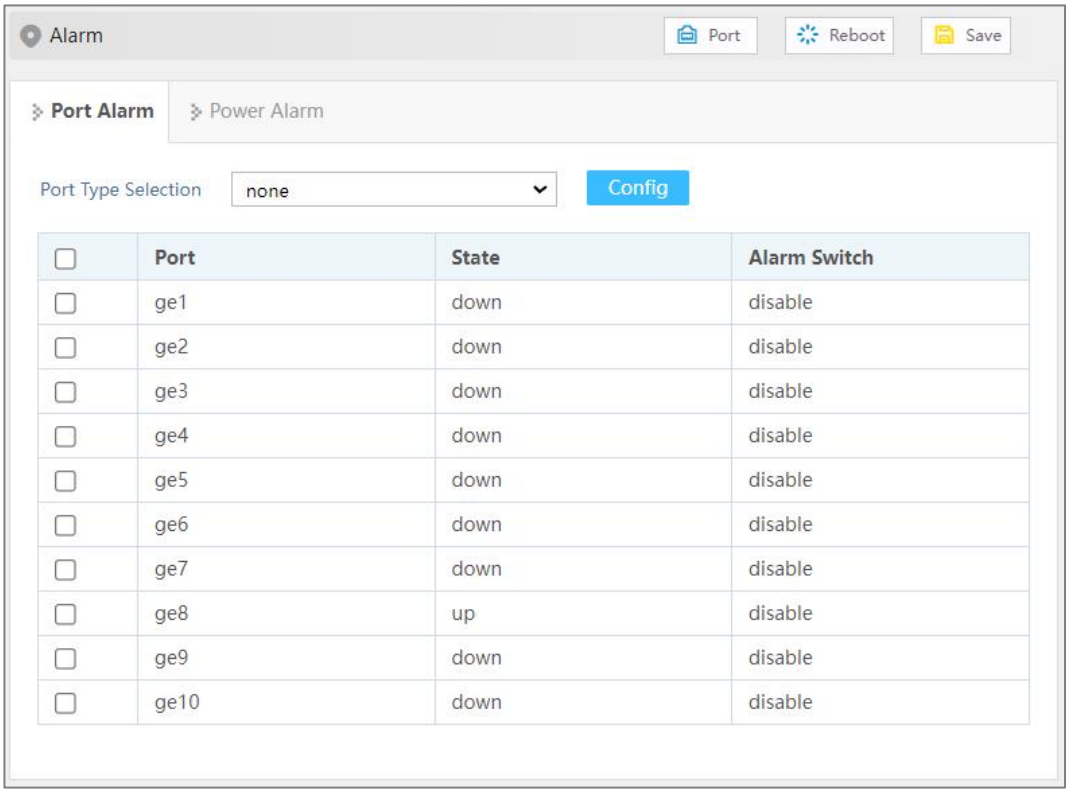
Configure the port alarm function. When the device port is in an abnormal state, the administrator can be informed in time, and the device state can be quickly repaired to avoid excessive loss.

Operation Path

Open in order: "System Maintenance > Alarm > Port Alarm".

Interface Description

Port alarm interface as below:



The main element configuration description of alarm information interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
State	Port link status, display items as follows: • up • down

Interface Element	Description
Alarm Switch	Port alarm function status, options as follows: • Enable • Disable Note: After enabling port alarm, when port occurs abnormal status, such as connection break down, the device will output a alarm signal to hint the abnormal operation of device via network management software, alarm indicator or relay.

8.4 Configuration File Management

8.4.1 Current Configuration

Function Description

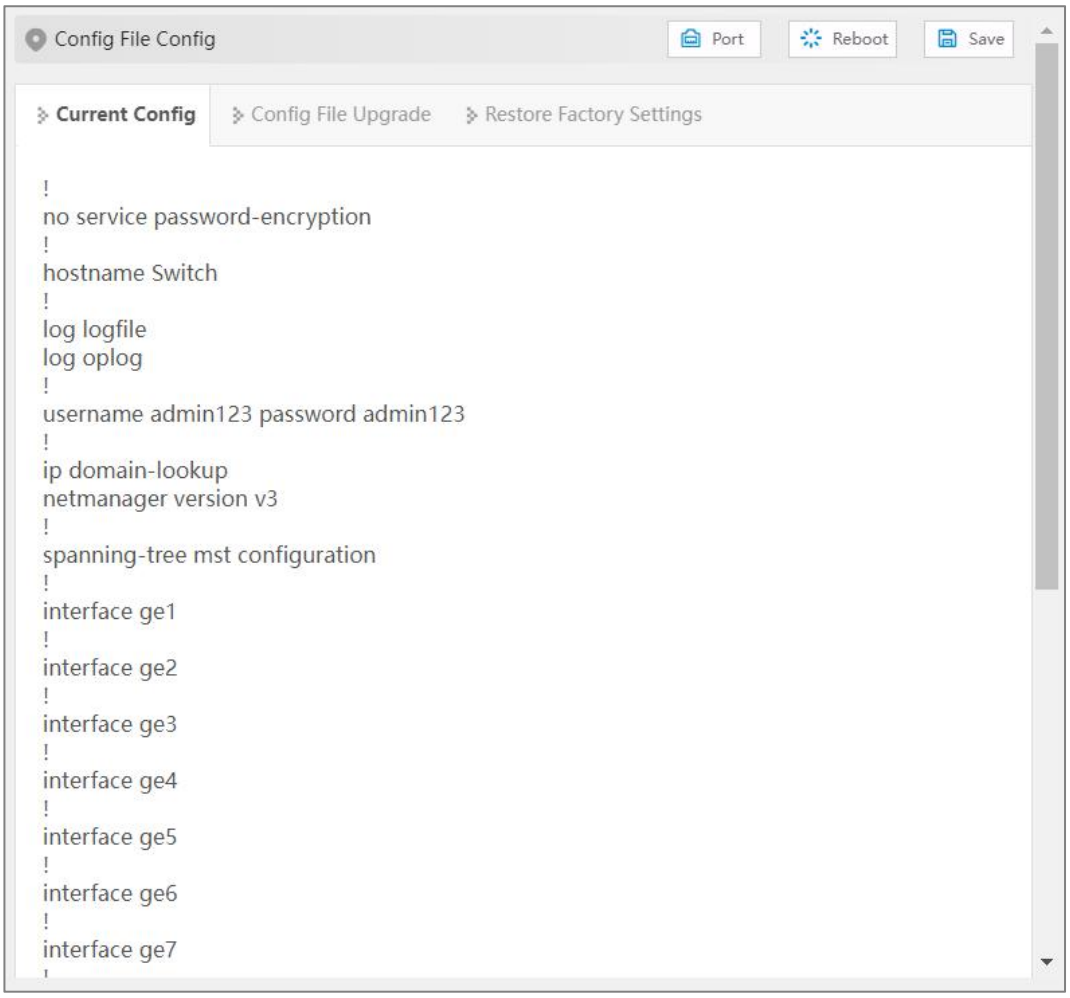
Check current configuration information.

Operation Path

Open in order: "System Management > Configuration File Settings > Current Configuration".

Interface Description

The current configuration interface is as follows:



8.4.2 Configuration File Update

Function Description

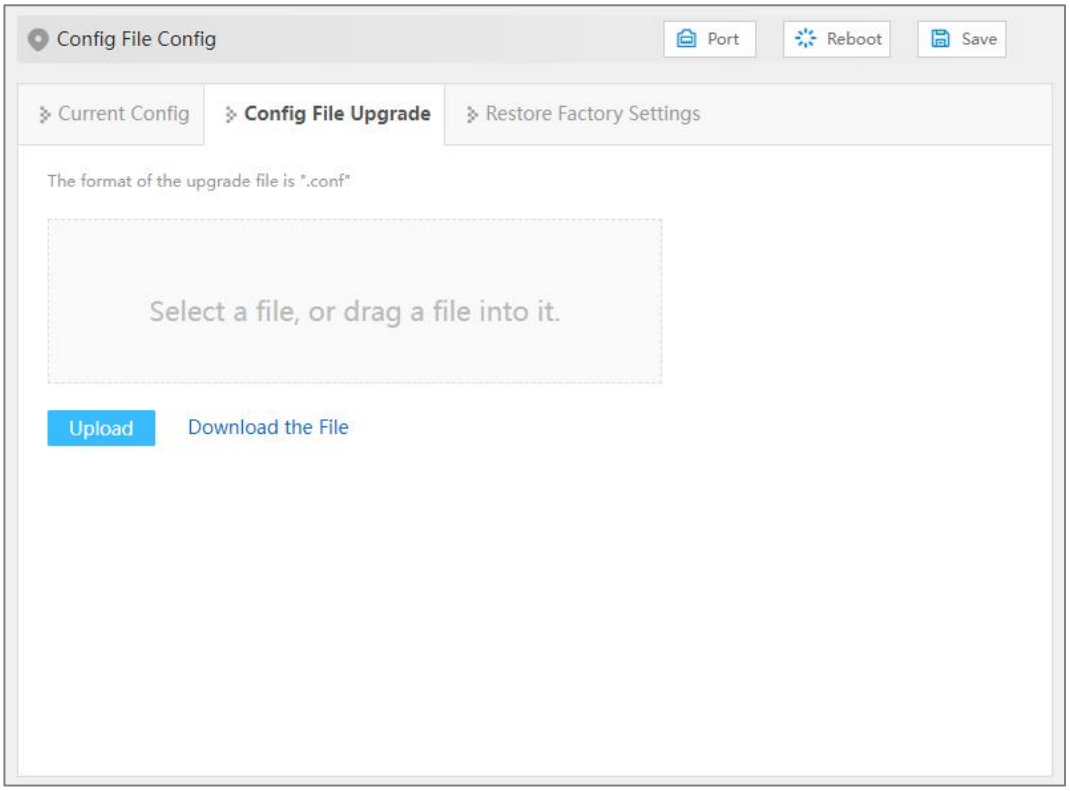
Upload and upload configuration file.

Operation Path

Open in order: "System Management > Configuration File Settings > Configuration File Upgrade".

Interface Description

Configuration file upgrade interface as follows:



The main element configuration description of configuration file upgrade interface:

Interface Element	Description
Select a file, or drag a file into it	To select the uploaded configuration file, click this area to select the local configuration file, or drag the local configuration file directly into this area.
Upload	After selecting the uploaded configuration file, click the "Upload" button to start uploading the configuration.
Download the File	Click to download the configuration file of the current device. The default file name is "device.conf".

8.4.3 Restore Factory Settings

Function Description

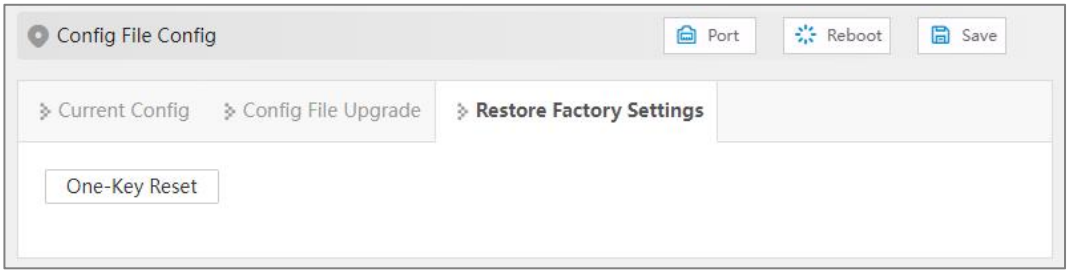
Restore device to factory settings.

Operation Path

Open in order: "System management > Configure Management > Restore Factory Setting".

Interface Description

Restore Factory Settings interface is as follows:



The main element configuration description of restore factory settings interface:

Interface Element	Description
One-Key Reset	Click "One-Key Reset" button, and the configuration file will be restored to the factory configuration.

8.5 Upgrade

Function Description

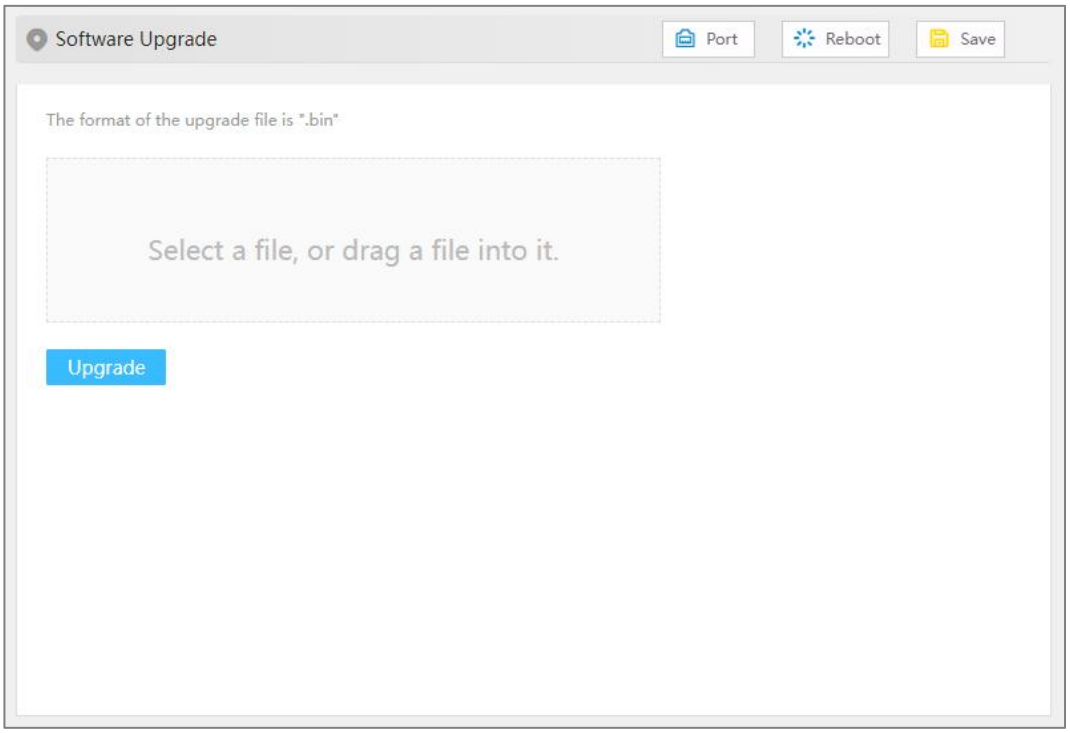
Update and upgrade the device program.

Operation Path

Open in order: "System management > Software Upgrade".

Interface Description

The software update interface as follows:



The main elements configuration description of software update interface:

Interface Element	Description
Select a file, or drag a file into it	For the upgrade files, click this area to select the local upgrade files, or drag the local upgrade files directly into this area.
Upgrade	After selecting the upgraded files, click the "Upgrade" button to start the upgrade process. Note: Generally, upgrade firmware is in ".bin" format.

8.6 Log Information

8.6.1 Log Information

Function Description

Check the log information of the device. Log information mainly records user operation, system failure, system safety and other information, including user log, security log and diagnostic log.

- User log: records user operations and system operation information.
- Security log: records information including account management, protocol, anti-attack and status.

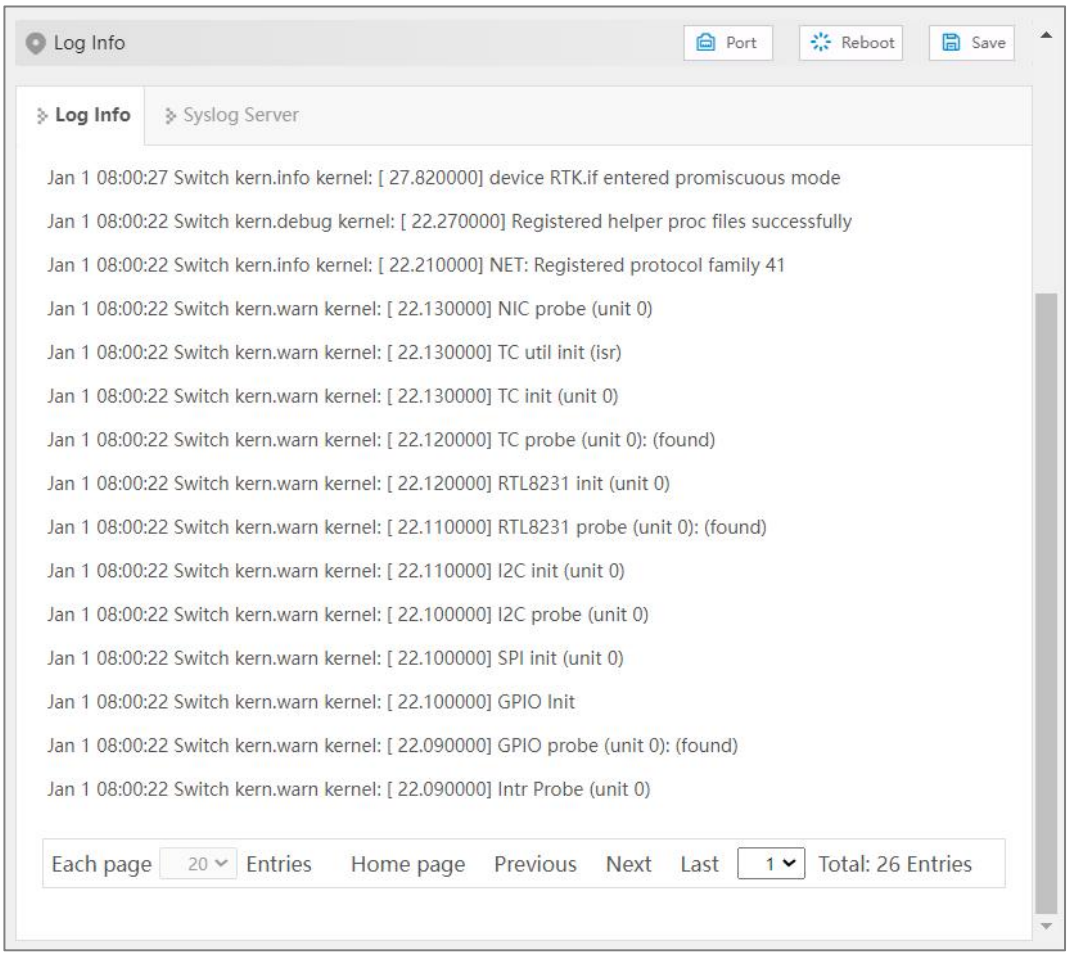
- Diagnostic log: records information that assists in problem identification.

Operation Path

Open in order: "System Maintenance > Log Information > Log Information".

Interface Description

Log information interface as follow:



Main elements configuration description of log information interface:

Interface Element	Description
Log power off storage	Log information is stored in FLASH, log information will not be lost after power failure.
Download log	Click the "Download Log" button to download the current log information to the local.
clear log	Click the “clear log” button to clear the current log information record.

8.6.2 Syslog Server

Function Description

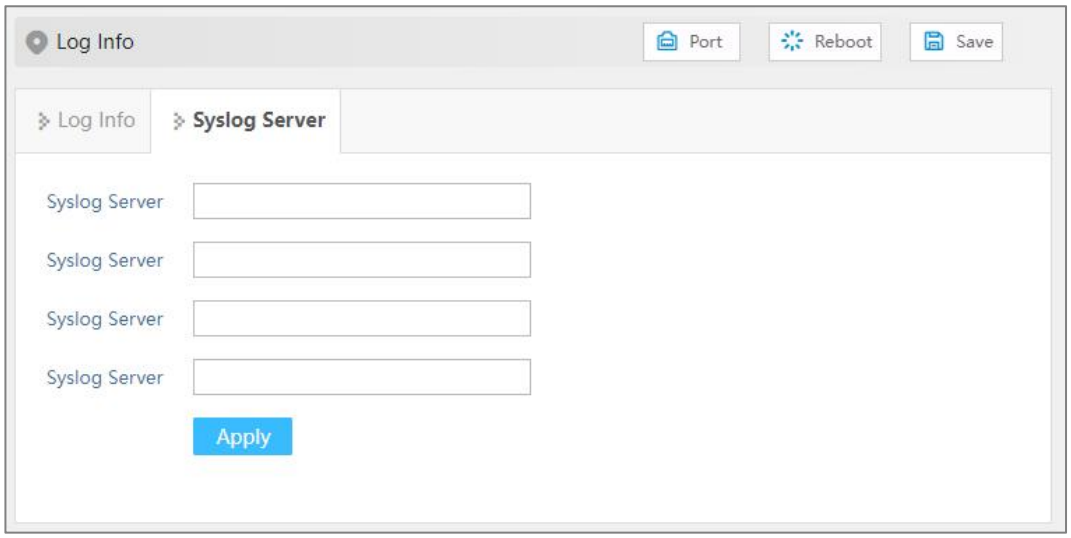
Configure the Syslog server IP address, and the system log information can be sent to the configured syslog server.

Operation Path

Open in order: "System Maintains > Log Information > Syslog Server".

Interface Description

The Syslog server interface as follows:



Syslog server interface main elements configuration instructions:

Interface Element	Description
Syslog Server	IP address of Syslog server Note: • Supports port configuration and the input format is IP: port, for example: 192.168.1.1:80. • Users can configure up to 4 syslog servers at a time. If the configuration of one or more syslog servers need to be canceled, delete the input box and click Set.

9 FAQ

9.1 Sign in Problems

1. **Why the web page display abnormally when browsing the configuration via WEB?**

   Before accessing the WEB, please eliminate IE cache buffer and cookies. Otherwise, the web page will display abnormally.

2. **What should I do if I forget my login password?**

   For forgetting the login password, the password can be initialized by restoring factory setting, specific method is adopt network management software to search and use restore factory setting function to initialize the password. Both of the initial user name and password are "admin123".

3. **Is configuring via WEB browser same to configuring via network management software?**

   Both configurations are the same, without conflict.

9.2 Configuration Problem

1. **Why the bandwidth can't be increased after configuring Trunking (port aggregation) function?**

   Check whether the port attributes set to Trunking are consistent, such as rate, duplex mode, VLAN and other attributes.

2. **How to deal with the problem that part of switch ports are impassable?**

   When some ports on the switch are impassable, it may be network cable, network

adapter and switch port faults. User can locate the faults via following tests:

- Keep connected computer and switch ports unchanged, change other network cables;
- Keep connected network cable and switch port unchanged, change other computers;
- Keep connected network cable and computer unchanged, change other switch port;
- If the switch port faults are confirmed, please contact supplier for maintenance.

3. **How about the order of port self-adaption state detection?**

   The port self-adaption state detection is conducted according to following order: 1000Mbps full duplex, 100Mbps full duplex, 100Mbps half-duplex, 10Mbps full duplex, 10Mbps half-duplex, detect in order from high to low, connect automatically in supported highest speed.

9.3 Indicator Problem

1. **Why is the power supply indicator off?**

   Possible reasons include:

   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Power supply or indicators faults; troubleshooting, change the power supply or device test.
   - Power supply voltage can't meet the device requirements; troubleshooting, configure the power supply voltage according to the device manual.

2. **Link/Act indicator isn't bright, what's the reason?**

   Possible reasons include:

   - The network cable portion of Ethernet copper port is disconnected or bad contact; troubleshooting, connect the network cable again.
   - Ethernet terminal device or network card works abnormally; troubleshooting, eliminate the terminal device fault.
   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Interface rate doesn't match the pattern; troubleshooting, examine whether the device transmission speed matches the duplex mode.

3. **Ethernet copper port and fiber port indicator are connected normally, but can't transmit data, what's the reason?**

   When the system is power on or network configuration changes, the device and switch configuration in the network will need some time. Troubleshooting, after the device and switch configuration are completed, Ethernet data can be transmitted; if it's impassable, power off the system, and power on again.

4. **Why does the communication crashes after a period of time, namely, it cannot communicate, and it returns to normal after restarting?**

   Reasons may include:

   - Surrounding environment disturbs the product; troubleshooting, product grounding adopts shielding line or shields the interference source.
   - Site wiring is not normative; Troubleshooting, optical fiber, network cable, optical cable cannot be arranged with power line and high-voltage line.
   - Network cable is disturbed by static electricity or surge; Troubleshooting, change the shielded cable or install a lightning protector.
   - High and low temperature influence; troubleshooting, check the device temperature usage range.