28-Port Series

Layer 2 Managed Industrial Ethernet Switch

User Manual

Document Version: 03

Issue Date: 7/26/2024

Preface

This Switch User Manual has introduced:

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

Note

The reference model for the screenshot in this manual is 16 100M copper ports + 8 100M fiber ports + 4 Gigabit COMBO ports, in addition to the differences in the supported port number, the interface functions and operation of other models in this series are similar.

Audience

This manual applies to the following engineers:

- Network administrators responsible for network configuration and maintenance
- On-site technical support and maintenance personnel
- 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

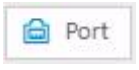
Format	Description
" "	Words with “” represent the interface words. Such as: “Port No.”.
>	Multi-level path is separated by ">". Such as opening the local

Format	Description
	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' provides links to various sections of this chapter, as well as links to the Principles/Operations Section of this chapter.

Icon Convention

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 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

Format	Description
	user to save the configuration, so as to avoid losing unsaved configuration information due to restart and other operations.
Add	Click the Add button to add a line of configuration. Note that repeated configuration may result in data overwrite.
Delete	Check the line to be deleted, and then click the Delete button to delete the configuration.
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 Apply 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.	Revision Date	Revision Note
01	01/31/2023	Product release
02	7/26/2024	Software upgrade

Contents

1 Login to 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	Above Internet Explorer 9.0
Operating system	Windows 7/8/10 or above

1.2 Set the IP Address of PC

The default management IP address of the device is 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.

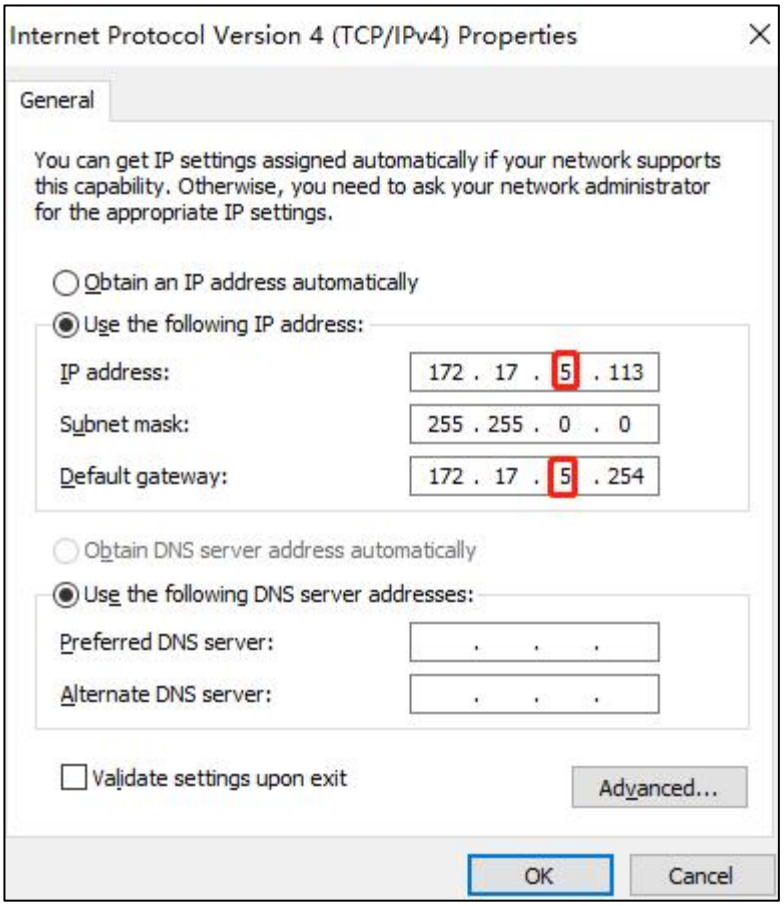
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps are as follows:

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

Step 2 Change the "5" selected by the red frame in the figure to "1".



Step 3 Click "OK", modification is successful.

Step 4 End.

1.3 Login to the WEB Configuration Interface

Operation Steps

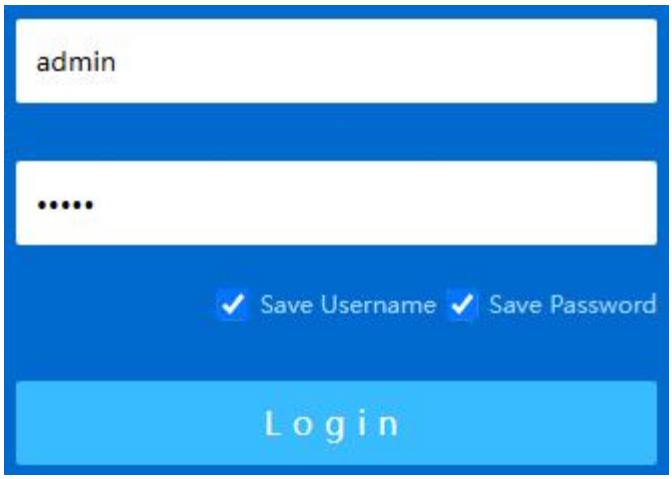
Log in to the WEB configuration interface as follows:

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 “admin”; 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 login successfully, user can configure relative parameters and information of WEB interface according to demands.

2 System Information

Function Description

View port status such as port type and connection status.

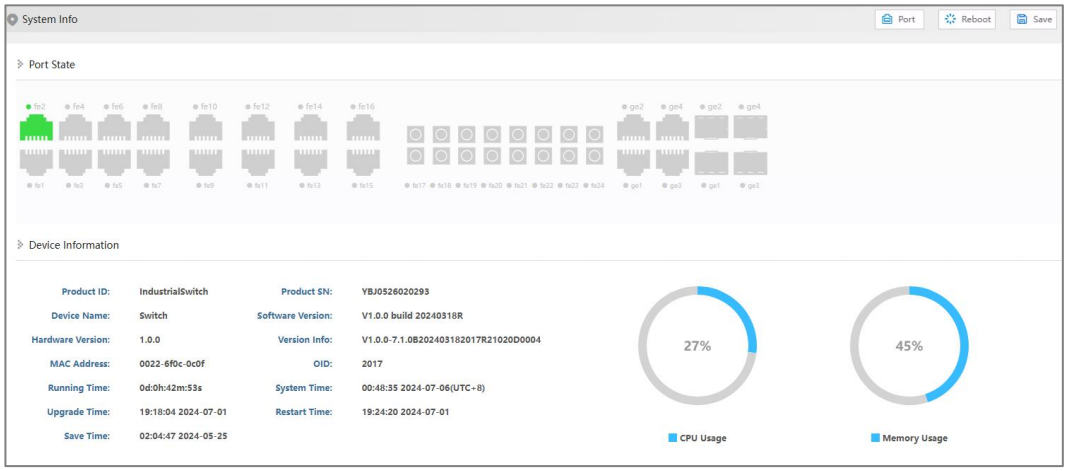
Check device information such as product model, software and hardware version, etc.

Operation Path

Open in the navigation bar: “System Information”.

Interface Description

System information interface is as follows:



The main element configuration description of System Info 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 port is not connected or disabled.

Interface Element	Description
	•  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 Info • OID • Running Time • 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: After modifying the IP of the device, re-enter the corresponding IP address to access the WEB interface.

3.2 Users

Function Description

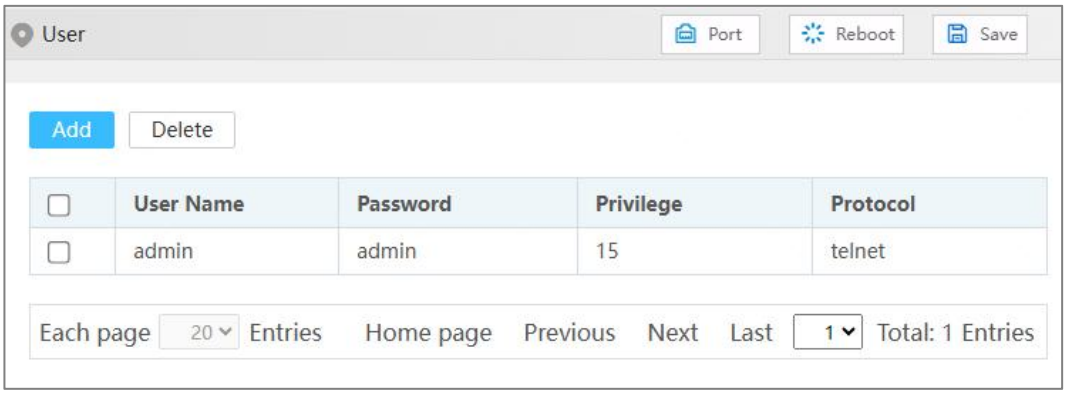
To add and delete user, user needs to enter username and password to access the device, the initial username and password are: admin.

Operation Path

Open in order: "Login Configuration > User".

Interface Description

User interface is as follows:



The main element configuration description of user interface:

Interface Element	Description
User Name	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 (~! @ # $% _-.). • 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,

Interface Element	Description
	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	Provide Telnet protocol for users, with the following options: • Telnet • SSH

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. TELNE

T 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 Switch	TELNET service enable switch button, which is enabled by default.
SSH Enable Switch	SSH service enable switch button, which is disabled by default.

4 Port Configuration

4.1 Port Settings

Function Description

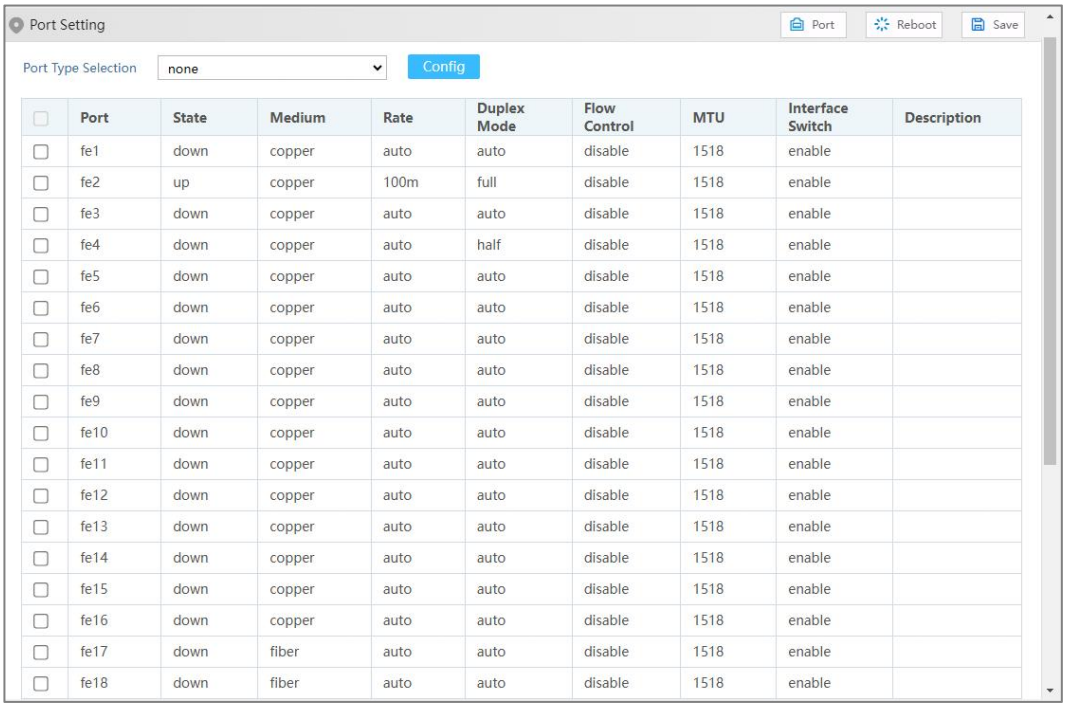
Set port parameters individually or in batches.

Operation Path

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

Interface Description

Port setting interface is as follows:



Port	State	Medium	Rate	Duplex Mode	Flow Control	MTU	Interface Switch	Description
fe1	down	copper	auto	auto	disable	1518	enable	
fe2	up	copper	100m	full	disable	1518	enable	
fe3	down	copper	auto	auto	disable	1518	enable	
fe4	down	copper	auto	half	disable	1518	enable	
fe5	down	copper	auto	auto	disable	1518	enable	
fe6	down	copper	auto	auto	disable	1518	enable	
fe7	down	copper	auto	auto	disable	1518	enable	
fe8	down	copper	auto	auto	disable	1518	enable	
fe9	down	copper	auto	auto	disable	1518	enable	
fe10	down	copper	auto	auto	disable	1518	enable	
fe11	down	copper	auto	auto	disable	1518	enable	
fe12	down	copper	auto	auto	disable	1518	enable	
fe13	down	copper	auto	auto	disable	1518	enable	
fe14	down	copper	auto	auto	disable	1518	enable	
fe15	down	copper	auto	auto	disable	1518	enable	
fe16	down	copper	auto	auto	disable	1518	enable	
fe17	down	fiber	auto	auto	disable	1518	enable	
fe18	down	fiber	auto	auto	disable	1518	enable	

Main elements configuration description of port setting interface:

Interface Element	Description

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. • Unconnected combo ports are displayed as copper ports by default.
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 • 2500m: 2.5G • 10g: 10 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.
MTU	Ethernet port transmitted maximum data frame length, the value range is 64-10240.

Interface Element	Description
Interface Switch	Enable or disable Ethernet port. Options are as follows: • enable • disable
Description	Port description information, which supports 0-32 characters 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.

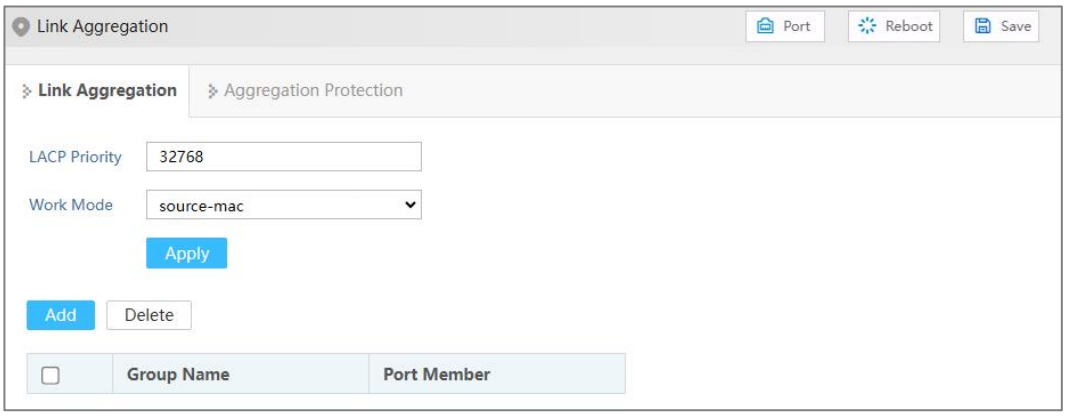
Based on the enabling or disabling of LACP protocol, the link aggregation can be divided into two modes, static aggregation and dynamic aggregation.

Operation Path

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

Interface Description

Link Aggregation interface is as below:

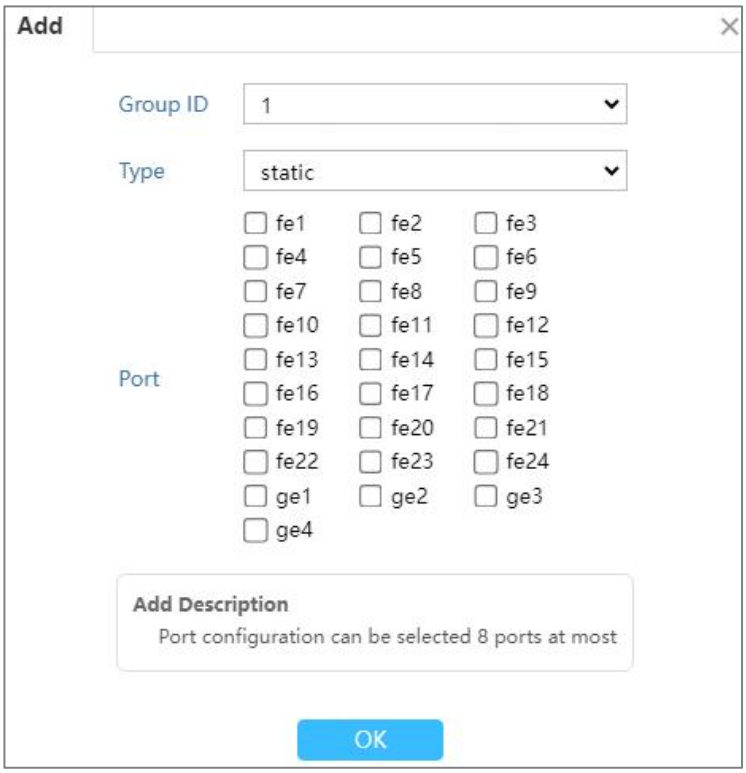


The main element configuration description of Link Aggregation interface:

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: • source-mac: Load balance mode based on source MAC • destination-mac: Load balance mode based on destination MAC • 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 ports to join aggregation.
Port Member	Port member in the link aggregation group.

Interface Description: Add

The Link Aggregation-Add interface is 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. • 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.
Aggregation Protection	The enabled state of the aggregation protection. • Enable • Disable
Default VLAN ID	The VLAN where that aggregate group port resides.
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

Interface Element	Description
	• Loop: forming a loop • Link error (such as generating a large number of error frames).

4.3 Port Speed Limit

Function Description

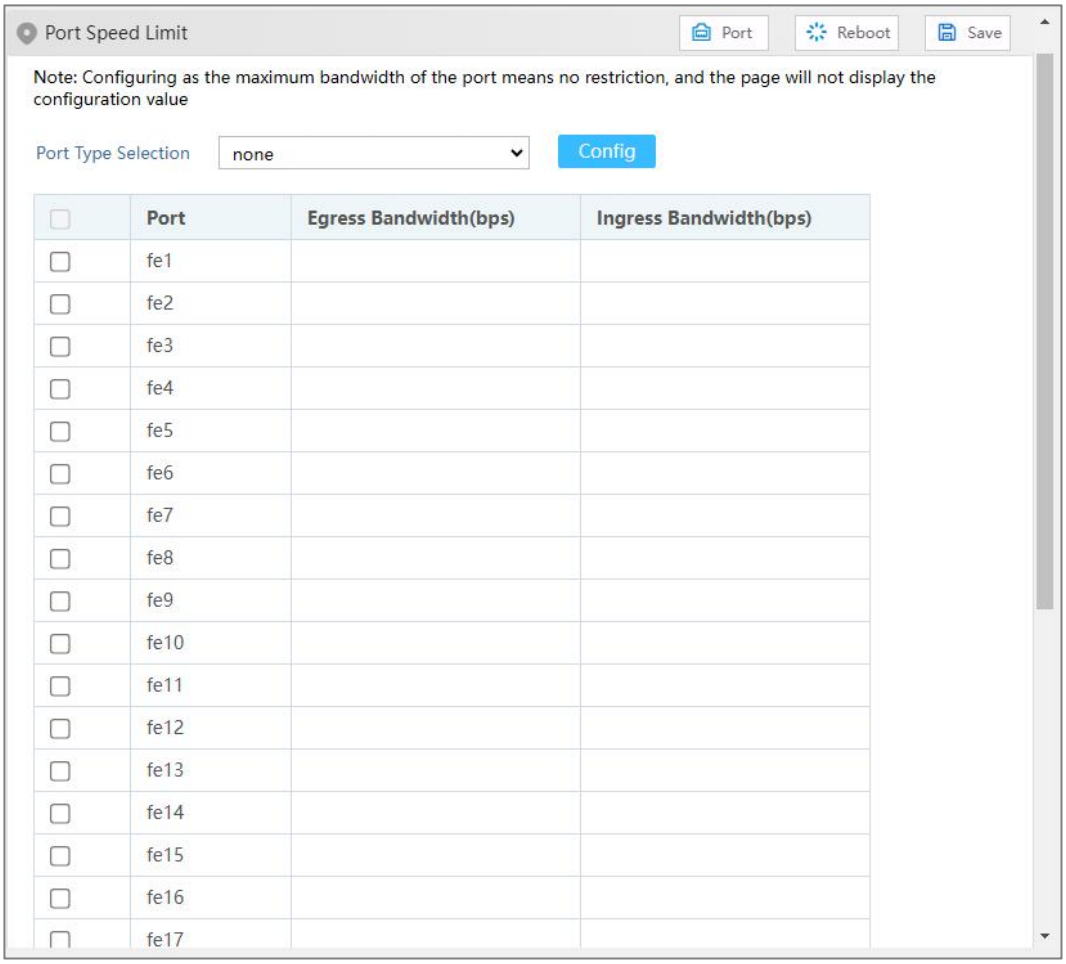
Limit the egress bandwidth and ingress bandwidth of the port.

Operation Path

Open in order: "Port Configuration > Port Speed Limit".

Interface Description

Port speed limit interface is as follows:



The main element configuration description of port speed 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.

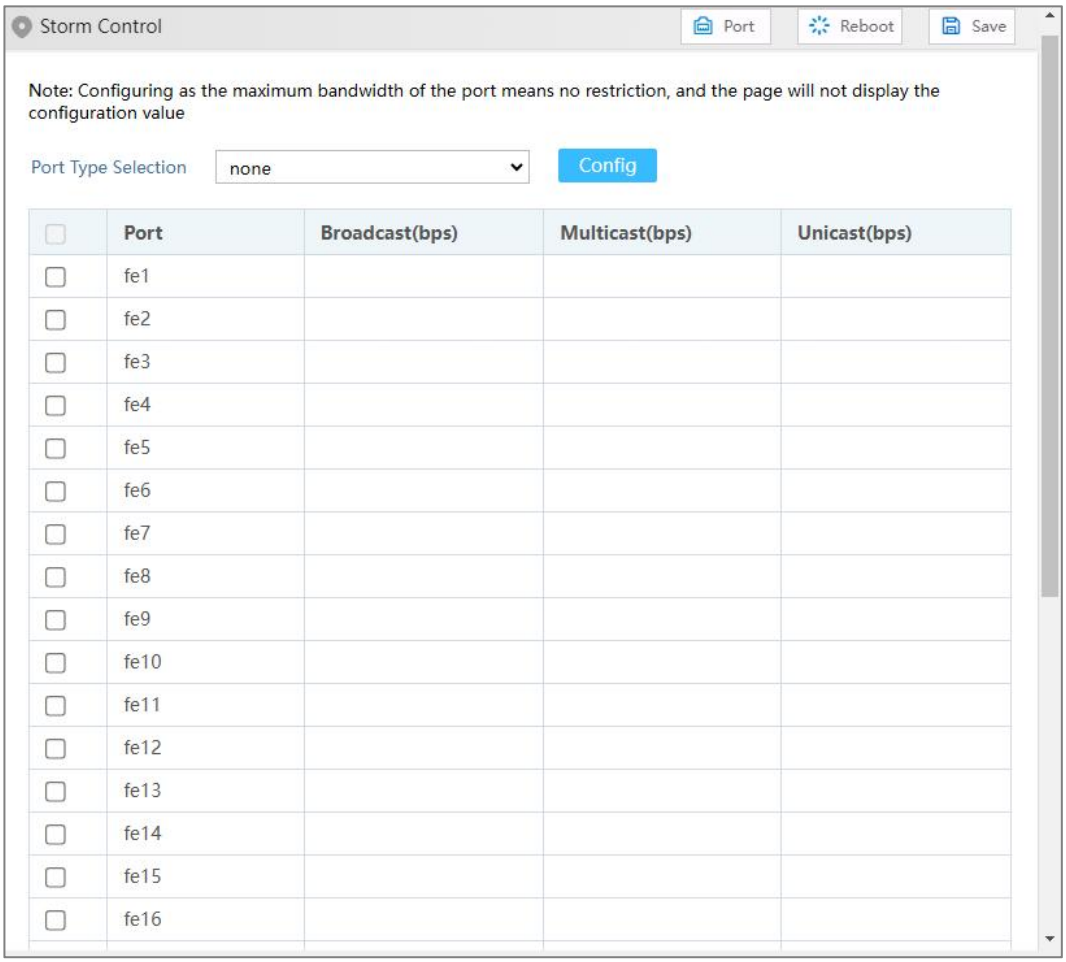
When the sum of each port broadcast, unknown multicast or unknown unicast flow achieves the value user sets, the system will discard the packets beyond the broadcast, unknown multicast or unknown unicast flow limit, so that the proportion of overall broadcast, unknown multicast or unknown unicast flow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

Operation Path

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

Interface Description

Storm control interface is as follows:



Main elements configuration description of storm control 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 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 mirroring interface is 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

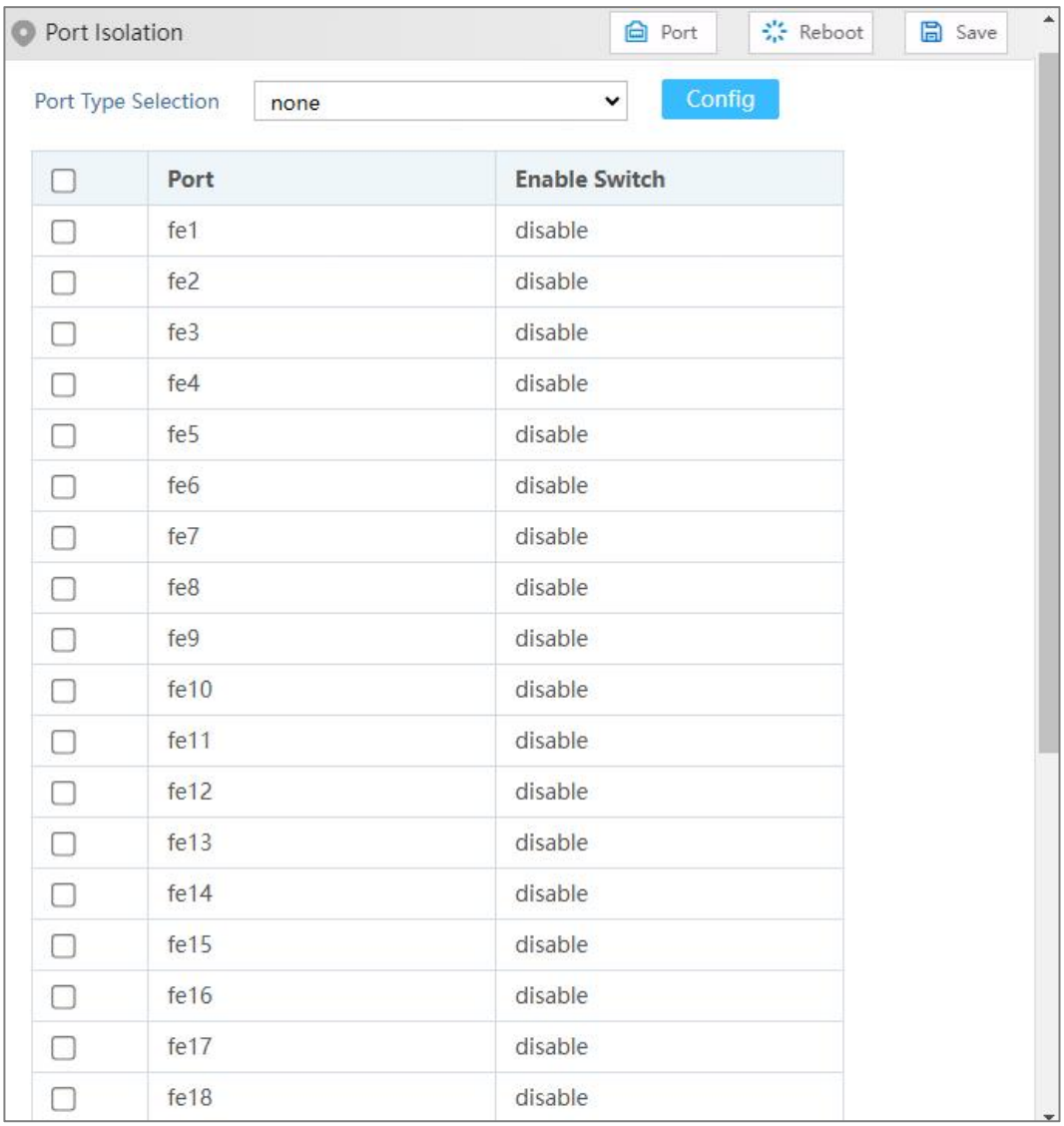
Port isolation is used for the layer 2 isolation between messages. It could add different ports to different VLANs, but waste limited VLAN resources. Adopting isolate-port characteristics can achieve isolation of ports within the same VLAN. After adding the ports to isolation group, user can achieve 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 Switch	Port isolation enable status can be displayed as follows: • disable • enable

4.7 Port Statistics

4.7.1 Port Statistics-Overview

Function Description

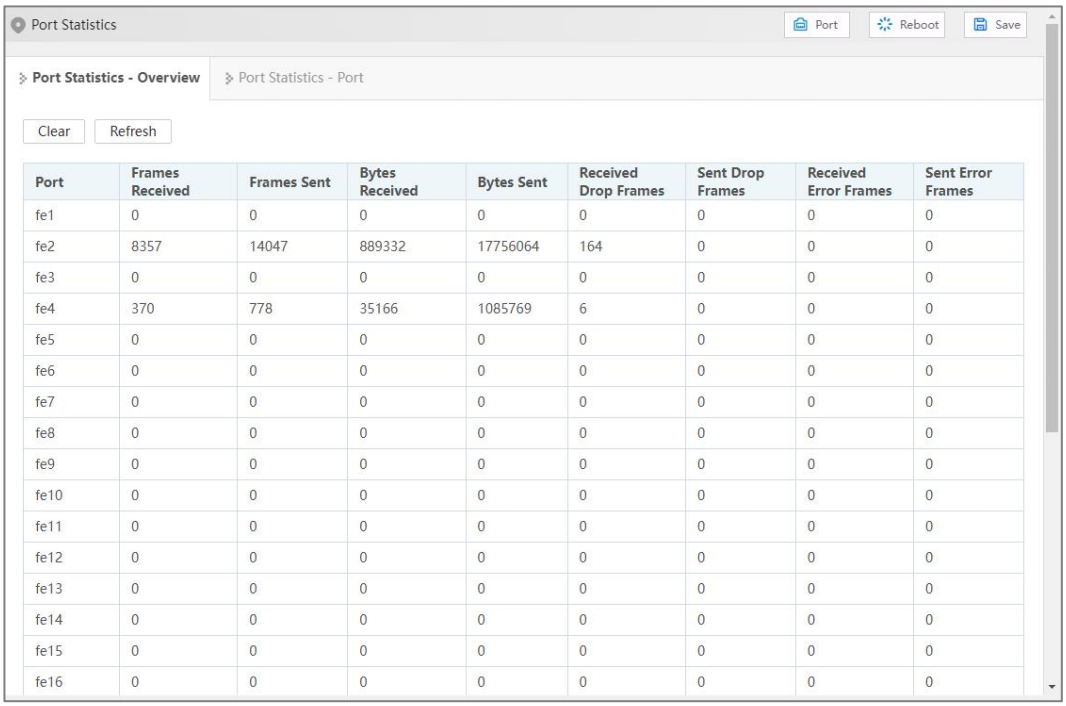
Check the number of messages and bytes, discarded messages and error messages sent and received by each port.

Operation Path

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

Interface Description

Port Statistics-Overview interface is as follows:



Port	Frames Received	Frames Sent	Bytes Received	Bytes Sent	Received Drop Frames	Sent Drop Frames	Received Error Frames	Sent Error Frames
fe1	0	0	0	0	0	0	0	0
fe2	8357	14047	889332	17756064	164	0	0	0
fe3	0	0	0	0	0	0	0	0
fe4	370	778	35166	1085769	6	0	0	0
fe5	0	0	0	0	0	0	0	0
fe6	0	0	0	0	0	0	0	0
fe7	0	0	0	0	0	0	0	0
fe8	0	0	0	0	0	0	0	0
fe9	0	0	0	0	0	0	0	0
fe10	0	0	0	0	0	0	0	0
fe11	0	0	0	0	0	0	0	0
fe12	0	0	0	0	0	0	0	0
fe13	0	0	0	0	0	0	0	0
fe14	0	0	0	0	0	0	0	0
fe15	0	0	0	0	0	0	0	0
fe16	0	0	0	0	0	0	0	0

4.7.2 Port Statistics-Port

Function Description

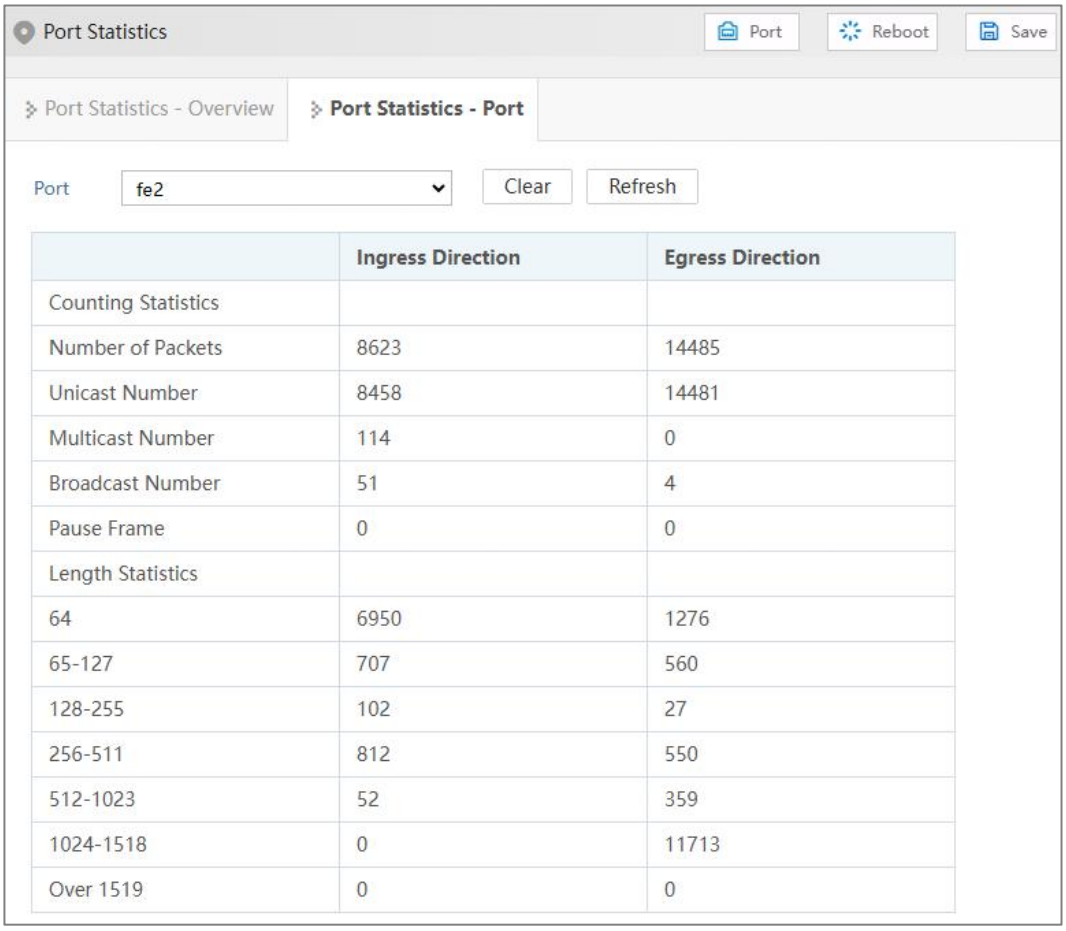
Check the classification statistics of the total number of messages sent and received by the designated port and the number of bytes of messages.

Operation Path

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

Interface Description

Port Statistics-Port interface is as follows:



	Ingress Direction	Egress Direction
Counting Statistics		
Number of Packets	8623	14485
Unicast Number	8458	14481
Multicast Number	114	0
Broadcast Number	51	4
Pause Frame	0	0
Length Statistics		
64	6950	1276
65-127	707	560
128-255	102	27
256-511	812	550
512-1023	52	359
1024-1518	0	11713
Over 1519	0	0

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 Config

Function Description

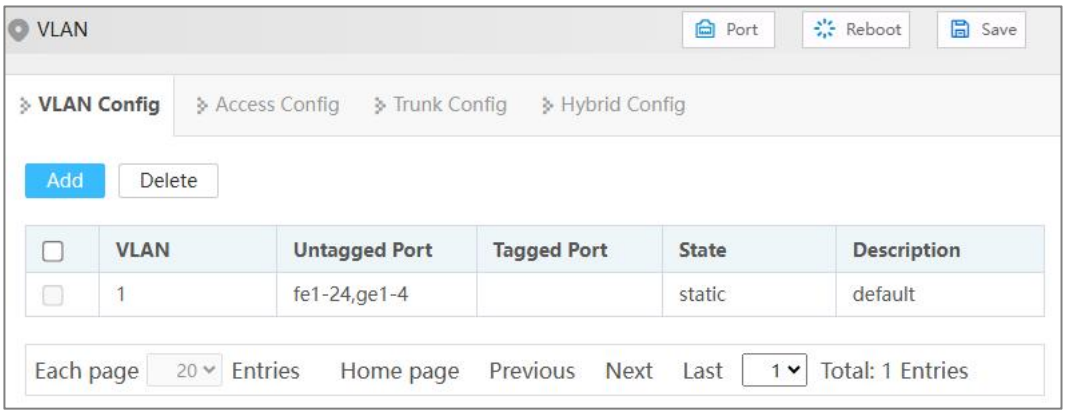
Create VLAN and edit VLAN description.

Operation Path

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

Interface Description

The VLAN config interface is as follows:



Main element configuration description of VLAN config 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 Config

Function Description

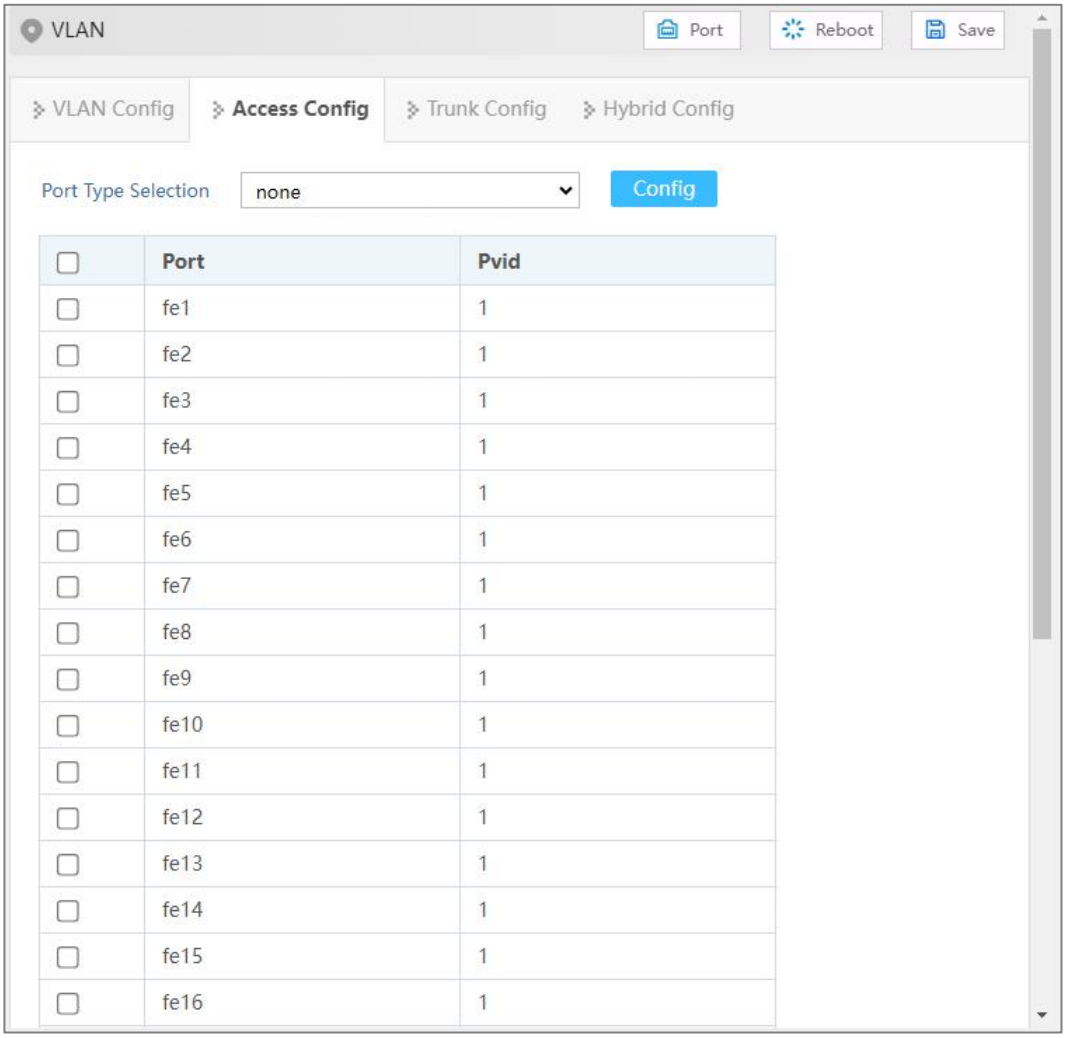
Configure the PVID (Port Default VLAN ID) of the Access interface, or modify it to Trunk interface.

Operation Path

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

Interface Description

Access config interface is as follows:



The main element configuration description of Access config 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.
Config	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,

Interface Element	Description
	but only allow the messages of one VLAN to transmit without tag (strip Tag) from this kind of interface. Commonly used in the connection between network devices.

5.1.3 Trunk Config

Function Description

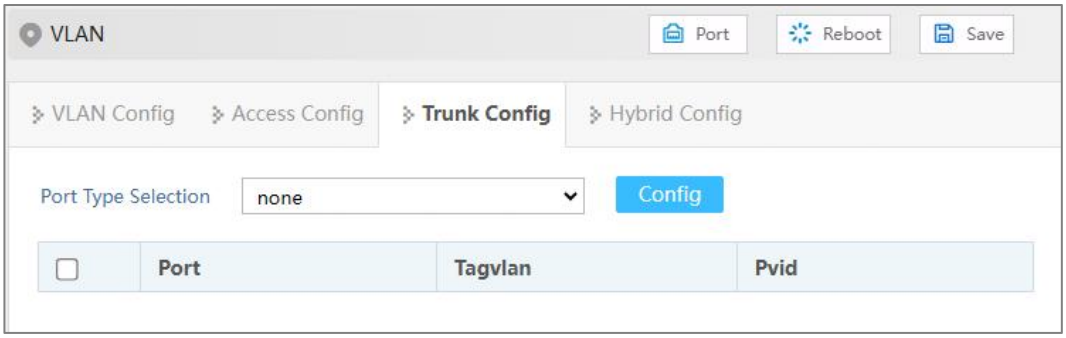
Configure the pvid value and tagvlan of Trunk port, or modify it to Access interface.

Operation Path

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

Interface Description

Trunk config interface is as follows:



The main element configuration description of Trunk config 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.
Config	Check the port and click “Config” to configure the VLAN and PVID of the port, as well as the processing of PVID when sending messages.

Process for Port Receiving Message

Interface Type	Process for Receiving Untagged Message	Process for Receiving Tagged 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, if not, discard the message.
Trunk		Receive this message when the VLAN ID is in the list of VLAN ID that allow to pass through the interface, if not, discard the message.

Process for Port Sending Message

Interface Type	The process of transmit frame
Access	Strip the PVID Tag of the message first, then transmit it.
Trunk	Sending the message when the VLAN ID is the VLAN ID allowed by the interface; In addition, if the VLAN ID is the same as the default VLAN ID, the Tag can be removed or reserved according to the configuration, and send the message.

5.1.4 Hybrid Config

Function Description

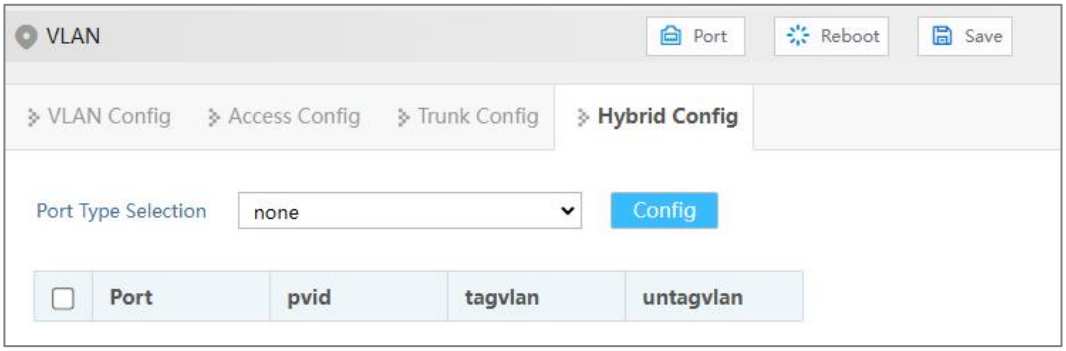
On the "Hybrid Configuration" page, user can configure Hybrid relative parameters.

Operation Path

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

Interface Description

Hybrid config interface is as follows:



The main element configuration description of Hybrid config interface.

Interface Element	Description
Port Type Selection	Filter the ports to be configured through the drop-down list.
Config	Check or filter the entries that need to be reconfigured, click configure to reset the parameters of PVID, tagvlan, and untagvlan.
pvid	VLAN ID number, value range is 1-4094.
untagvlan	The untagged value, an individual number or range ("-" represents range). For example: 9 or 10-15.
tagvlan	The tagged value, an individual number or range ("-" represents range). For example: 9 or 10-15.
Mode setting	Click "Mode setting" to set the type to access or trunk

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	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.
Hybrid		

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.

Interface type	The process of transmit frame
	• 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 Source 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.

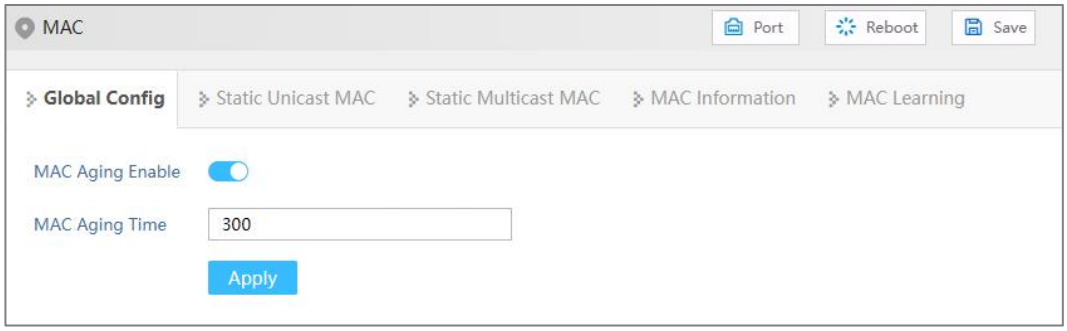
Each port in the switch is equipped with automatic address learning function, it stores the frame source address (source MAC address, switch port number) that port sends and receives in the address table. Ageing time is a parameter influencing the switch learning process; the default value is 300 seconds. 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

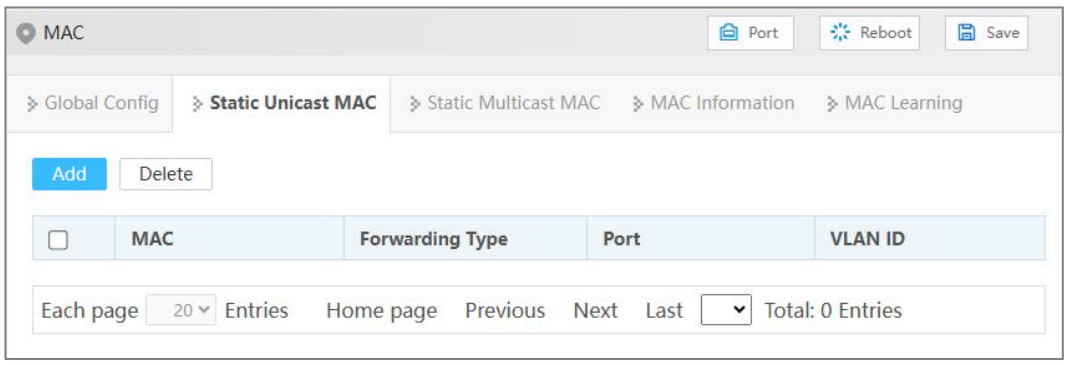
Source unicast MAC address binding and filtering will not age.

Operation Path

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

Interface Description

Static unicast MAC interface is as follows:



The main element configuration description of static MAC interface:

Interface Element	Description

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

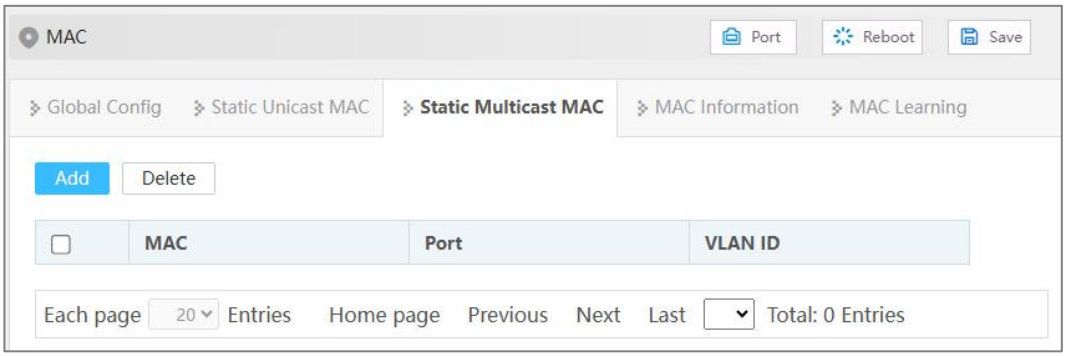
Source multicast MAC address binding will not age.

Operation Path

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

Interface Description

Static multicast MAC interface is 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

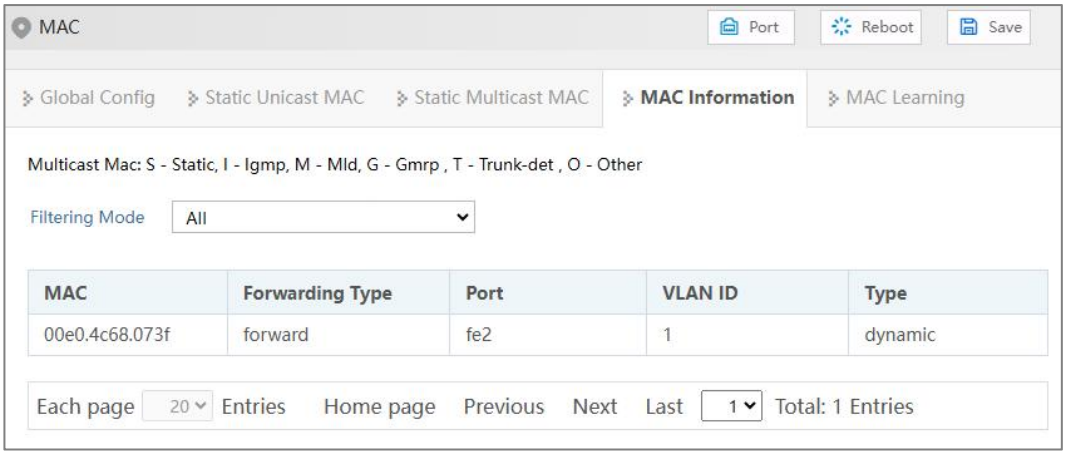
Check the MAC address table information.

Operation Path

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

Interface Description

MAC Information interface is as follows:



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

Interface Element	Description
	• 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

5.2.5 MAC Learning

Function Description

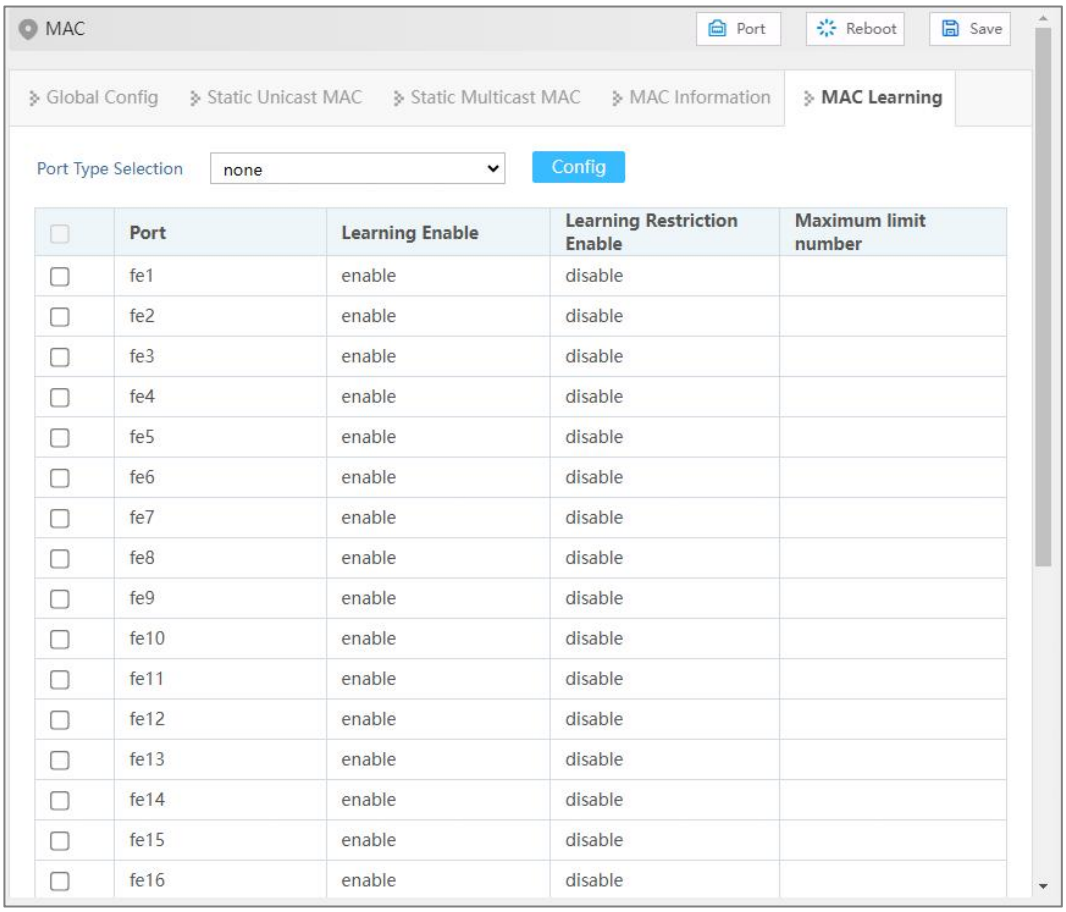
The main function of MAC learning is to limit the number of MAC learning on the port. When the MAC address table of the switch is full, it is impossible to learn new MAC addresses. At this time, if a large number of forged messages with different source MAC addresses are sent to the switch, it will exhaust the resources of the MAC address table of the switch and lead to the failure to learn normal MAC addresses. Therefore, limiting the number of MAC learning of the switch can prevent this from happening and improve the security of the switch and the network.

Operation Path

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

Interface Description

The MAC learning interface is as follows:



The main element configuration description of MAC learning interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Learning Enable	"Learning Enable" means that the switch turns on or off the learning function of MAC address. When MAC learning is enabled, the switch will learn and record the MAC addresses received from each port to establish a MAC address table for forwarding packets. When MAC learning is disabled, the switch will stop learning new MAC addresses and will only use the learned MAC addresses for forwarding. The operation of the 'learning enable switch' is as follows: • Disable: disable the learning restriction; • Enable: enable the learning restriction.
Learning Restriction Enable	"Learning Restriction Enable" refers to the function of the switch to turn on or off the learning restriction of a VLAN and the number of MAC addresses learned on a port. When learning restriction is enabled, the switch will limit the number of MAC addresses learned on a certain port, and MAC

Interface Element	Description
	addresses exceeding the limit may be discarded or ignored. When learning restriction is disabled, the switch does not limit the number of MAC addresses learned on a port. The operation of the 'learning limits enable switch' is as follows: • Disable: disable the learning restriction; • Enable: enable the learning restriction. Note: The "learning enable switch" and "learning restriction switch" can be turned on or off simultaneously, but the "learning restriction switch" only has actual impact when the "learning enable switch" is turned on.
Maximum limit number	The maximum number of restrictions means that "Learning Restriction Enable" restricts the number of MAC addresses learned on a port.

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 Config

Function Description

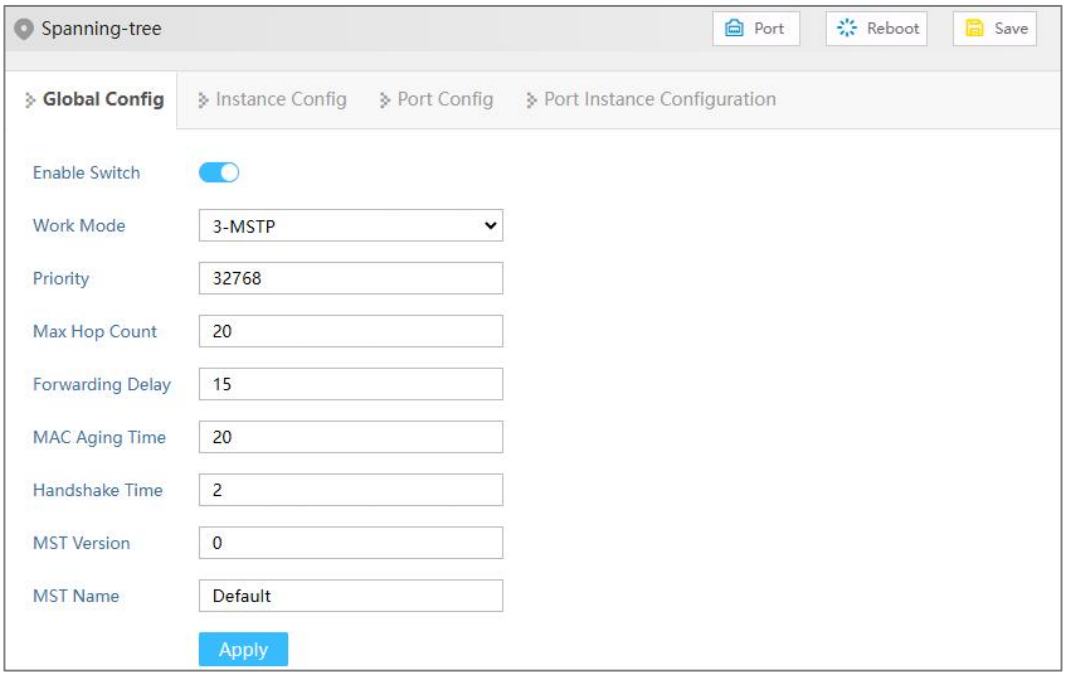
Configure the relevant parameters of spanning tree.

Operation Path

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

Interface Description

Global config interface is as follows:



The main element configuration description of global config interface:

Interface Element	Description
Enable Switch	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

Interface Element	Description
	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 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 Config

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 an 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).

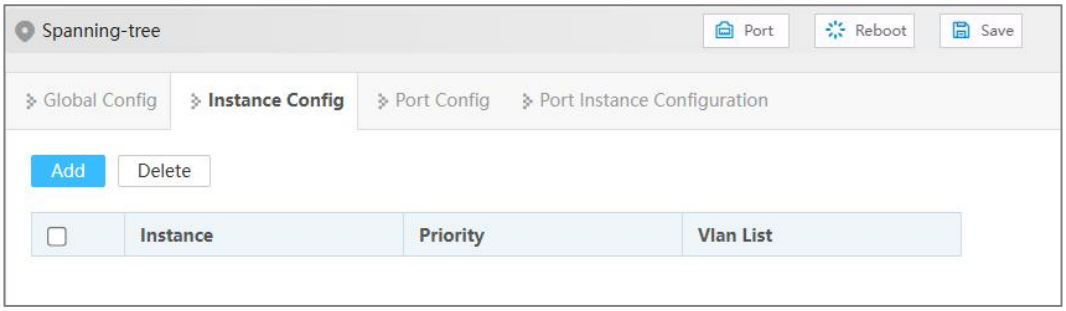
VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI.

Operation Path

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

Interface Description

Instance config interface is 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 Config

Function Description

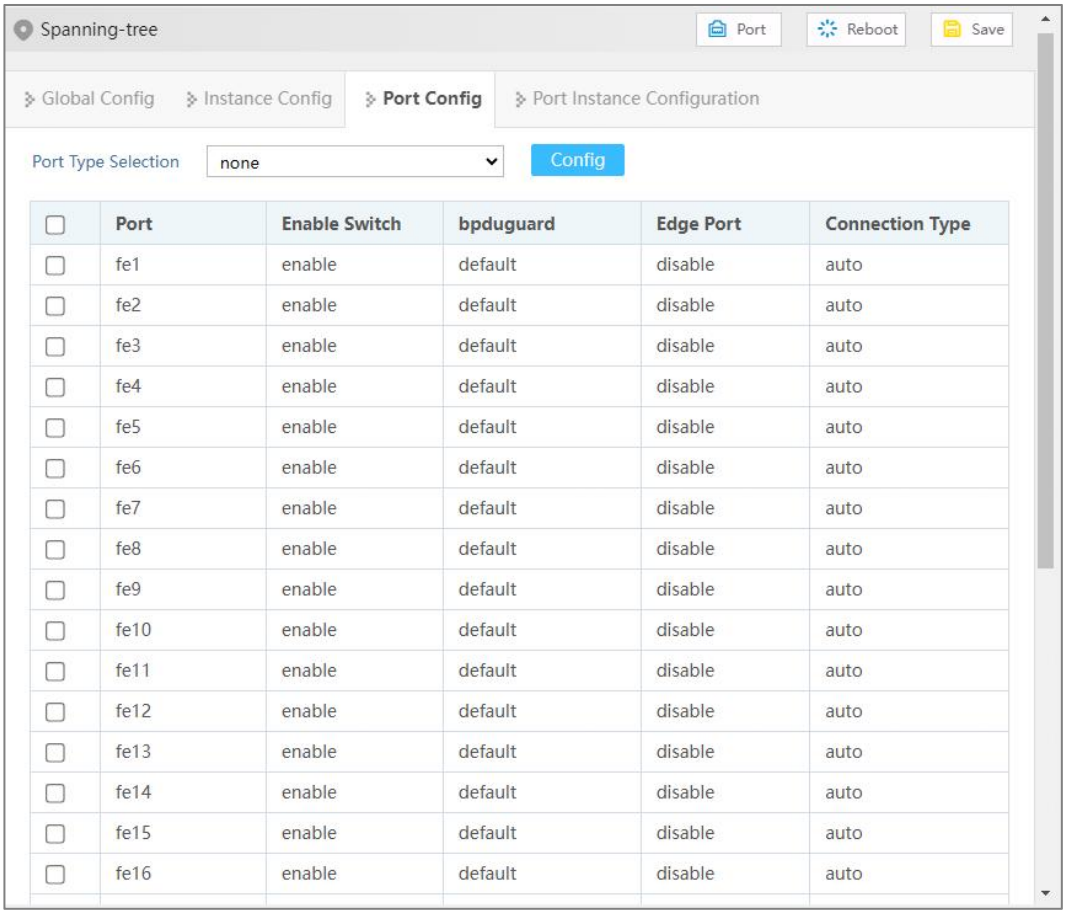
Enable port to participate in spanning-tree and configure port type, link type and BPDU protection function.

Operation Path

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

Interface Description

Check port config interface is as below:



The main element configuration description of port config interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Enable Switch	The enable status of ports participating in spanning tree can be shown as follows: • Enable • Disable
bpduguard	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

Interface Element	Description
	• Enable • 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
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 Port Instance Configuration

Function Description

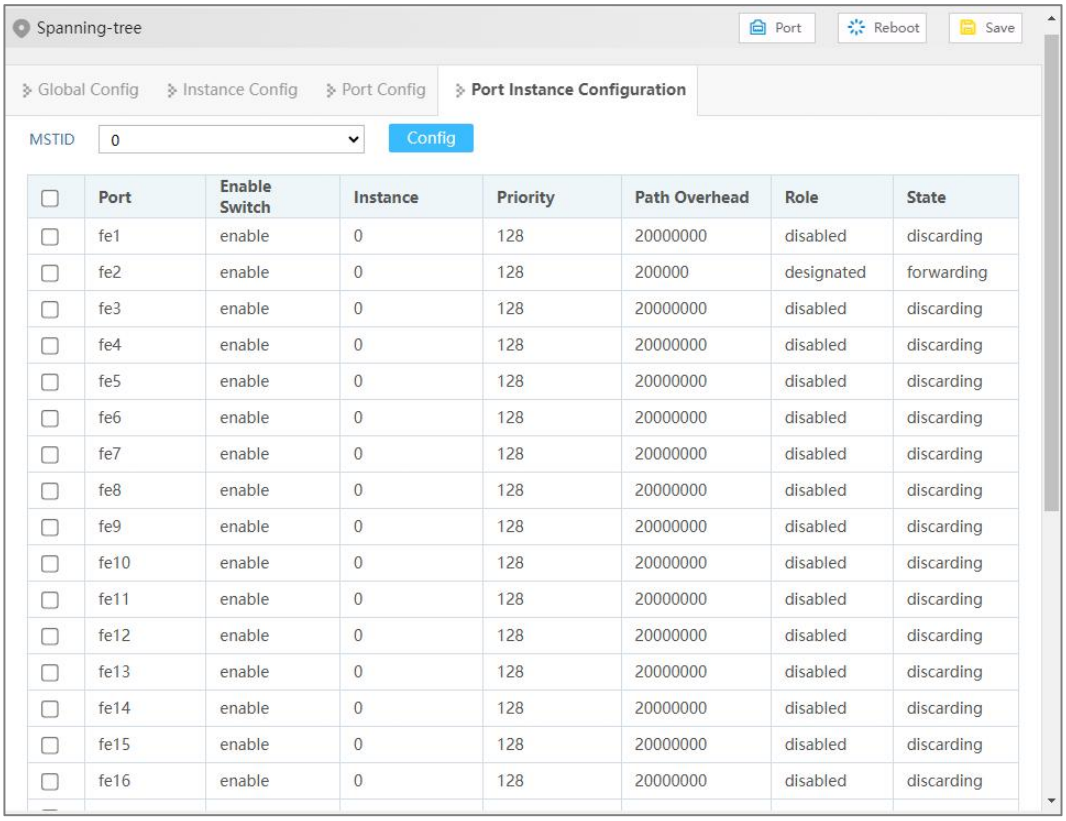
Configure port priority and cost

Operation Path

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

Interface Description

Port instance configuration interface is as follows:



Port	Enable Switch	Instance	Priority	Path Overhead	Role	State
fe1	enable	0	128	20000000	disabled	discarding
fe2	enable	0	128	200000	designated	forwarding
fe3	enable	0	128	20000000	disabled	discarding
fe4	enable	0	128	20000000	disabled	discarding
fe5	enable	0	128	20000000	disabled	discarding
fe6	enable	0	128	20000000	disabled	discarding
fe7	enable	0	128	20000000	disabled	discarding
fe8	enable	0	128	20000000	disabled	discarding
fe9	enable	0	128	20000000	disabled	discarding
fe10	enable	0	128	20000000	disabled	discarding
fe11	enable	0	128	20000000	disabled	discarding
fe12	enable	0	128	20000000	disabled	discarding
fe13	enable	0	128	20000000	disabled	discarding
fe14	enable	0	128	20000000	disabled	discarding
fe15	enable	0	128	20000000	disabled	discarding
fe16	enable	0	128	20000000	disabled	discarding

The main element configuration description of port instance configuration interface:

Interface Element	Description
MSTID	Choose multiple Spanning-tree ID number.
Port	The corresponding port name of the device Ethernet port.
Enable Switch	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 of the port, 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

Interface Element	Description
	• 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.

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.

5.4.1 Global Configuration

Function Description

Configure Ring private protocol ring network.

Operation Path

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

Interface Description

Ring interface is as follows:

The main element configuration description of Ring interface.

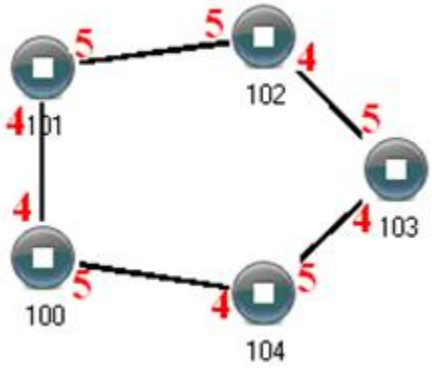
Interface Element	Description
Enable switch	Enable switch, which can enable the Ring network function after being enabled.
Ring Group	Support ring group 1-12, it can create multiple ring networks at the same time.
Ring ID	When multiple switches form a ring, the current ring ID would be network ID. Different 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	The network port 1 on the switch device used to form the ring network. 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 device used to form the ring network. Note:

Interface Element	Description
	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 State	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, which is a query packet sent by the CPU to adjacent devices through the ring port to confirm whether the connection is normal. Value range is 0-300.
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 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

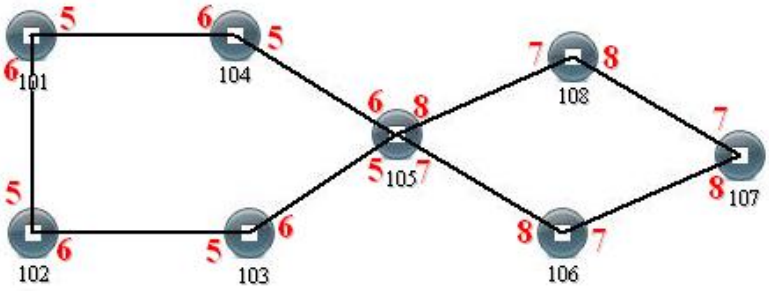
Enable Single, enable ring group 1 (other ring group is OK), Set the device port 4 and port 5 to ring port, and set other switches to the same configuration as the switch

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 is 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;

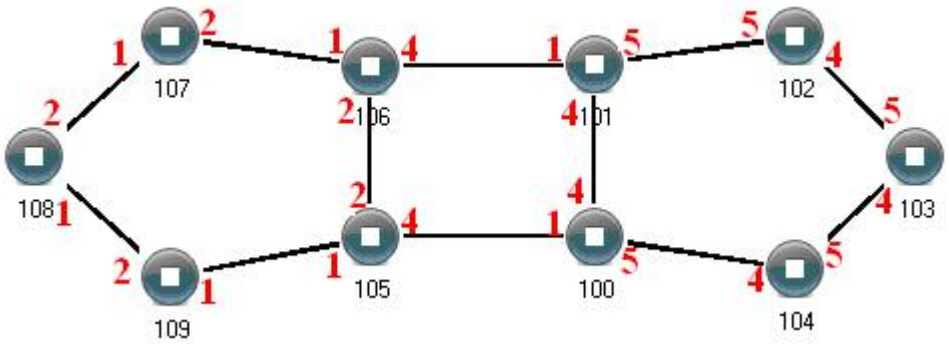
Step 4 Adopt network cable to connect the ring group 2;

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 is 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.

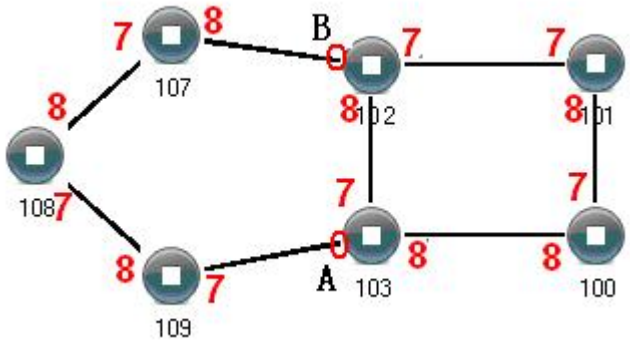
Step 4 Set the ring port of NO. 107, 108 and 109 device ring group 1 to port 1 and port 2, network identification to 1, ring type to Single; Set the ring port of NO. 102, 103 and 104 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single.

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. 105109 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 is 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.

5.4.2 Ring Information

Function Description

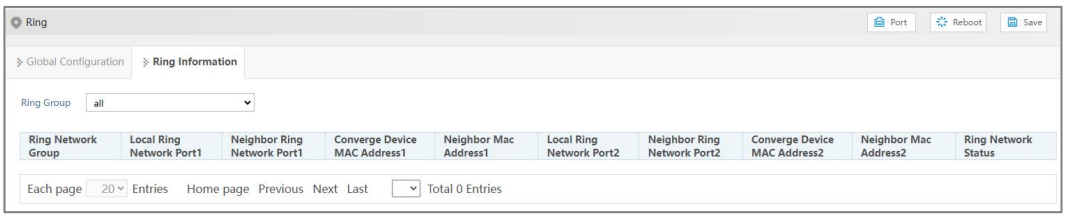
This function is provided by the system, and you can view it through the "Ring Information" page.

Operation Path

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

Interface Description

Ring Information interface is as follows:



The main element configuration description of Ring information interface:

Interface Element	Description
Ring group	Support the display of ring network group 1-12.
Local Ring Network Port 1	The network port 1 on the switch device used to form the ring network. 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.
Neighbor Ring Network Port 1	The port number of the neighbor ring network port 1, for example: 3.
Convergence Device MAC Address 1	The MAC address 1 of the convergence device is the MAC address 1 of the ring network device, for example, 00:22:6f:01:d0:a2.
Neighbor MAC Address 1	The MAC address 1 of the neighbor device of the ring network group, for example: 00:22:6f:01:cc:a2.
Local Ring Network Port 2	The network port 2 on the switch device used to form the ring network. 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.

Interface Element	Description
Neighbor Ring Network Port 2	The port number of the neighbor ring network port 2, for example: 5.
Convergence Device MAC Address 2	The MAC address 2 of the convergence device is the MAC address 2 of the ring network device, for example, 00:22:6f:01:d0:a2.
Neighbor MAC Address 2	The MAC address 2 of the neighbor device of the ring network group, for example: 00:22:6f:01:cc:a2.
Ring Network Status	Ring network status display: ● stable: indicates that the current ring network group is in a stable state; ● open: indicates that the current ring network group is in an open state.

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

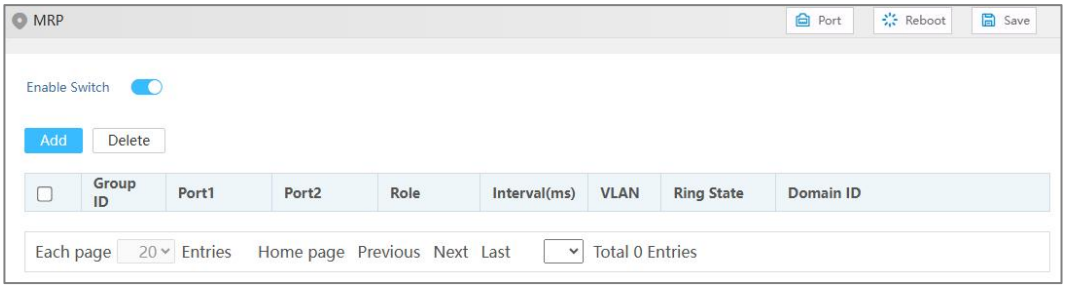
Configure MRP ring network.

Operation Path

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

Interface Description

MRP interface is as below:



The main element configuration descriptions of MRP interface:

Interface Element	Description
Enable Switch	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 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: • 200ms • 500ms
VLAN	VLAN ID used by MRP management message, its value range is 1-4094.
Ring 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 Config

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. To prevent this problem, the node where the RPL owner port resides starts the wait to restore (WTR) timer after receiving a 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 a RAPS (NR) message, the local port enters the Forwarding state.

- Hold Timer

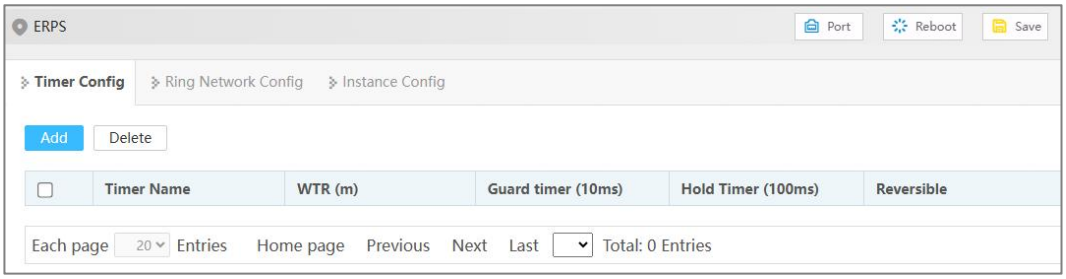
  On Layer 2 networks running ERPS, there may be different requirements for protection switching. For example, on a network where multi-layer services are provided, after a server fails, users may require a period of time to rectify the server fault so that clients do not detect the fault. Users can set 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 Config".

Interface Description

Timer config interface is 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 (m)	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 Config

Function Description

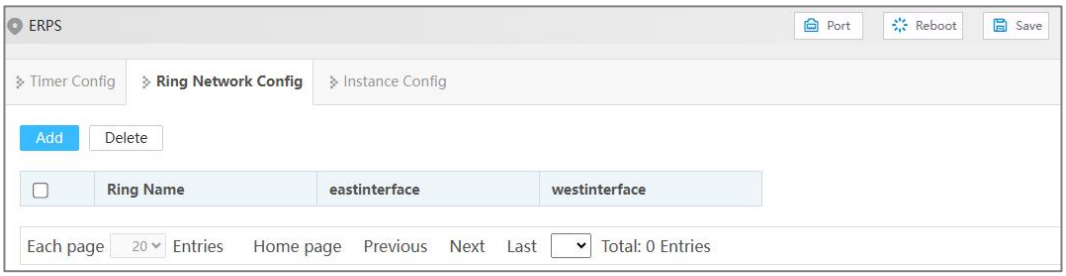
Configure ERPS ring port.

Operation Path

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

Interface Description

Ring network config interface is 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 Config

Function Description

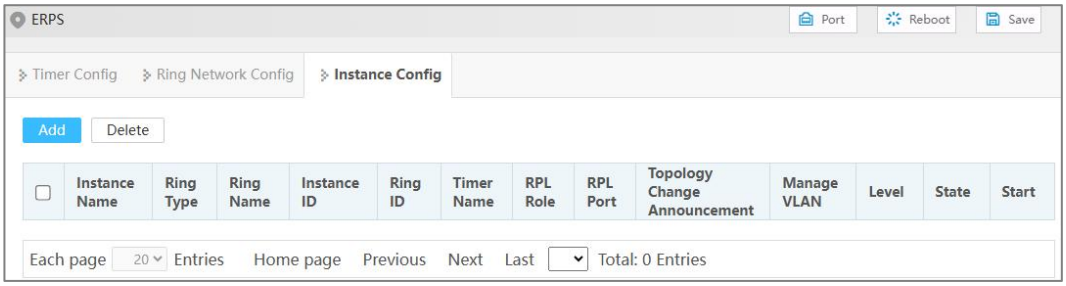
Configure ERPS ring network instance.

Operation Path

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

Interface Description

Instance config interface is as follows:



The main element configuration description of instance config 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 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.

Interface Element	Description
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 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.

Interface Element	Description
Enable	ERPS instance startup status: • start • stop

5.7 IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is an IPv4 layer 2 multicast Protocol. It maintains the egress interface information of Group broadcast by snooping for the multicast protocol messages sent between the layer 3 multicast device and the user host, so as to manage and control the forwarding of multicast data message in the data link layer.

5.7.1 Global Config

Function Description

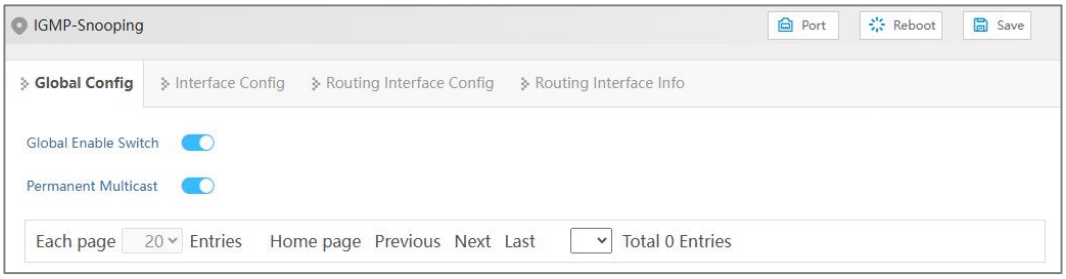
Enable/disable IGMP-Snooping and resident multicast.

Operation Path

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

Interface Description

Global config interface is as follows:



The main element configuration description of global config 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.

Interface Element	Description
Permanent Multicast	Do not age the received IGMP report member groups.

5.7.2 Interface Config

Function Description

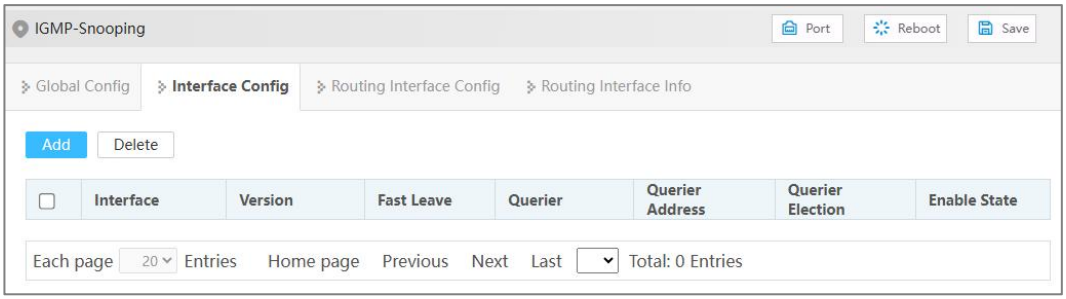
Configure parameters related to IGMP Snooping of VLANIF interface.

Operation Path

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

Interface Description

Interface config interface is as follows:



The main element configuration description of interface config 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

Interface Element	Description
	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 Query 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 Interface Config

Function Description

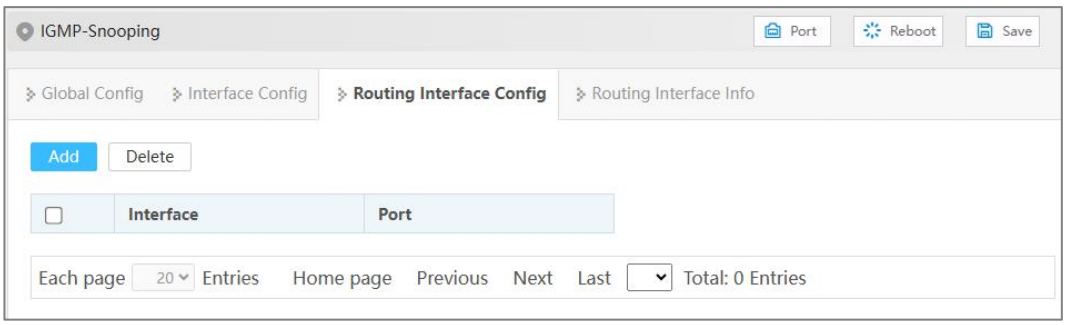
Configure multicast router ports.

Operation Path

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

Interface Description

Routing interface config interface is as below:



Main elements configuration description of routing interface config 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 Info

Function Description

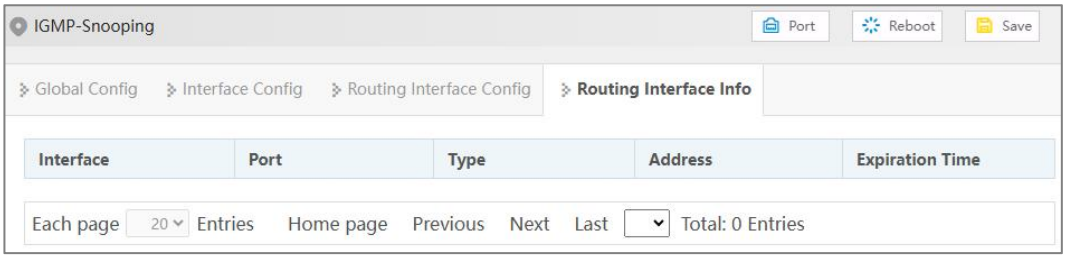
Check the router port information of IGMP Snooping in VLAN, including static router port and dynamic router port.

Operation Path

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

Interface Description

Routing interface info interface is as follows:



Configuration description of main elements of routing interface info 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 Config

Function Description

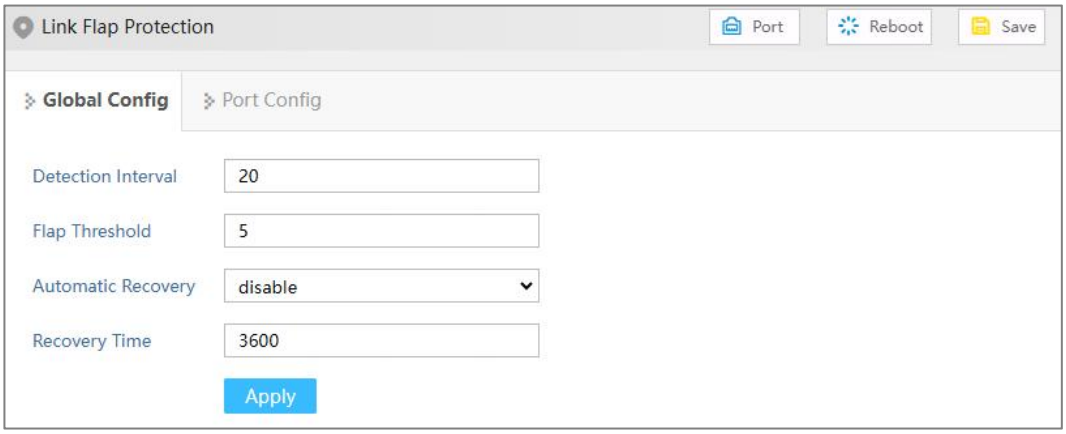
Configure relative parameters of link flapping protection.

Operation Path

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

Interface Description

Global config interface is as follows:



The main element configuration description of global config 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

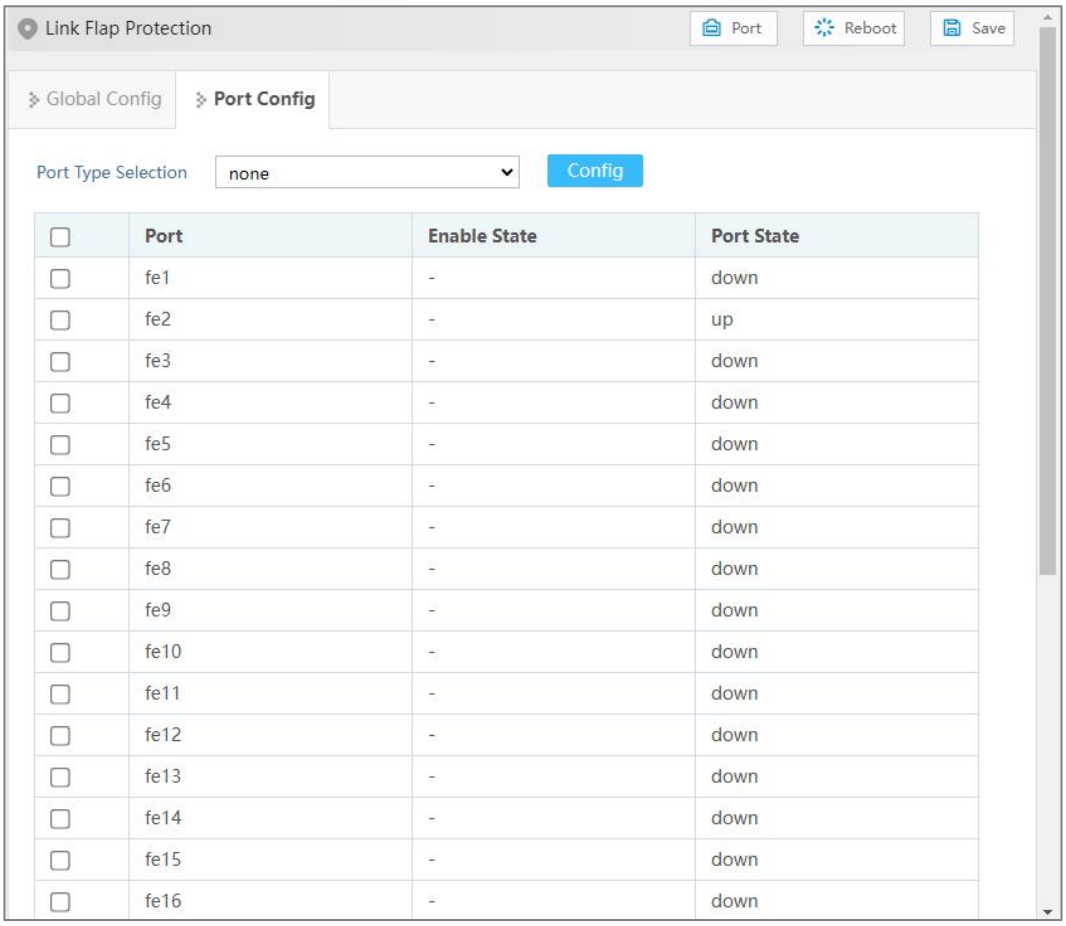
Enable link oscillation protection for this port.

Operation Path

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

Interface Description

Check port config interface as below:



The main element configuration description of port config 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 Loop 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

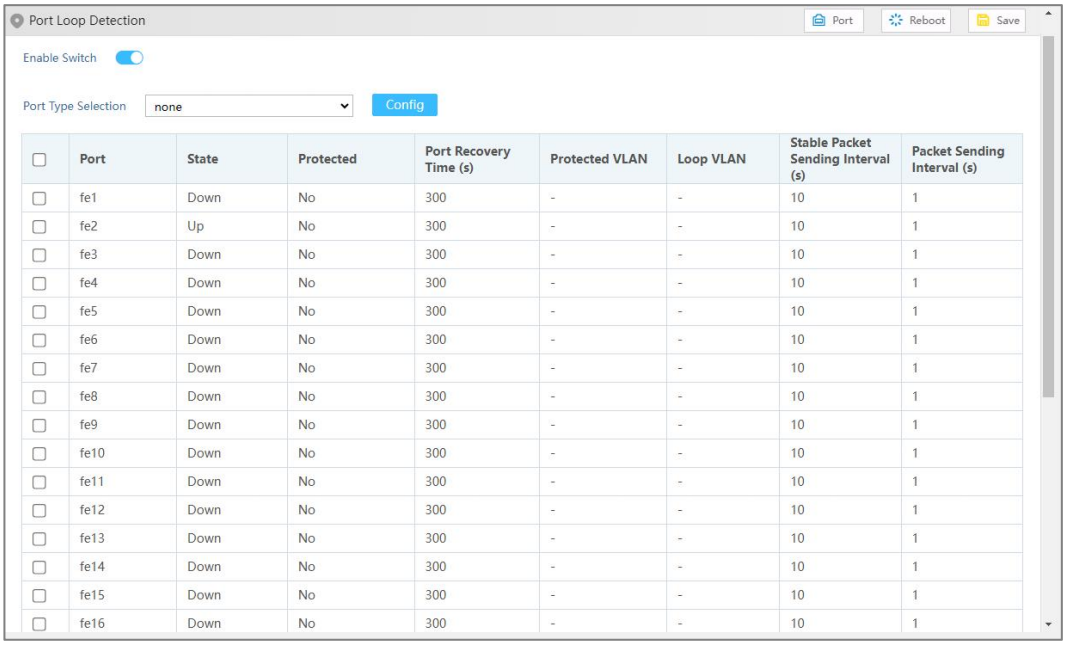
Enable port loop detection.

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 Switch	Global enable configuration of port loop detection.
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

Interface Element	Description
	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

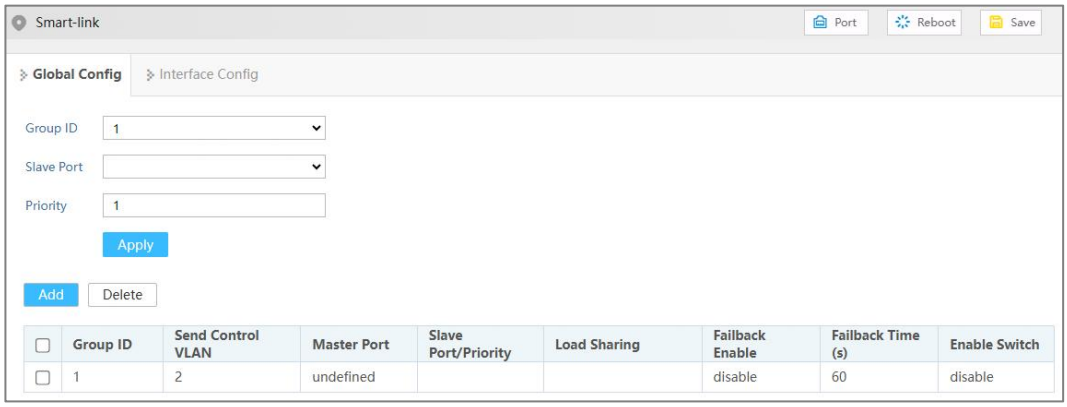
Configure Smart-link related parameters.

Operation Path

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

Interface Description

Global config interface is as follows:



The main element configuration description of global config 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/Priority	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 mapped in the specified load sharing instance, which can improve the utilization rate of the link.

Interface Element	Description
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
Failback Time (s)	Failback delay time, it can inhibit Smart Link switching caused by link flash, the value range is 30~1200 seconds.
Enable Switch	Smart Link function enable status can be displayed as follows: • Enable • Disable

5.10.2 Interface Config

Function Description

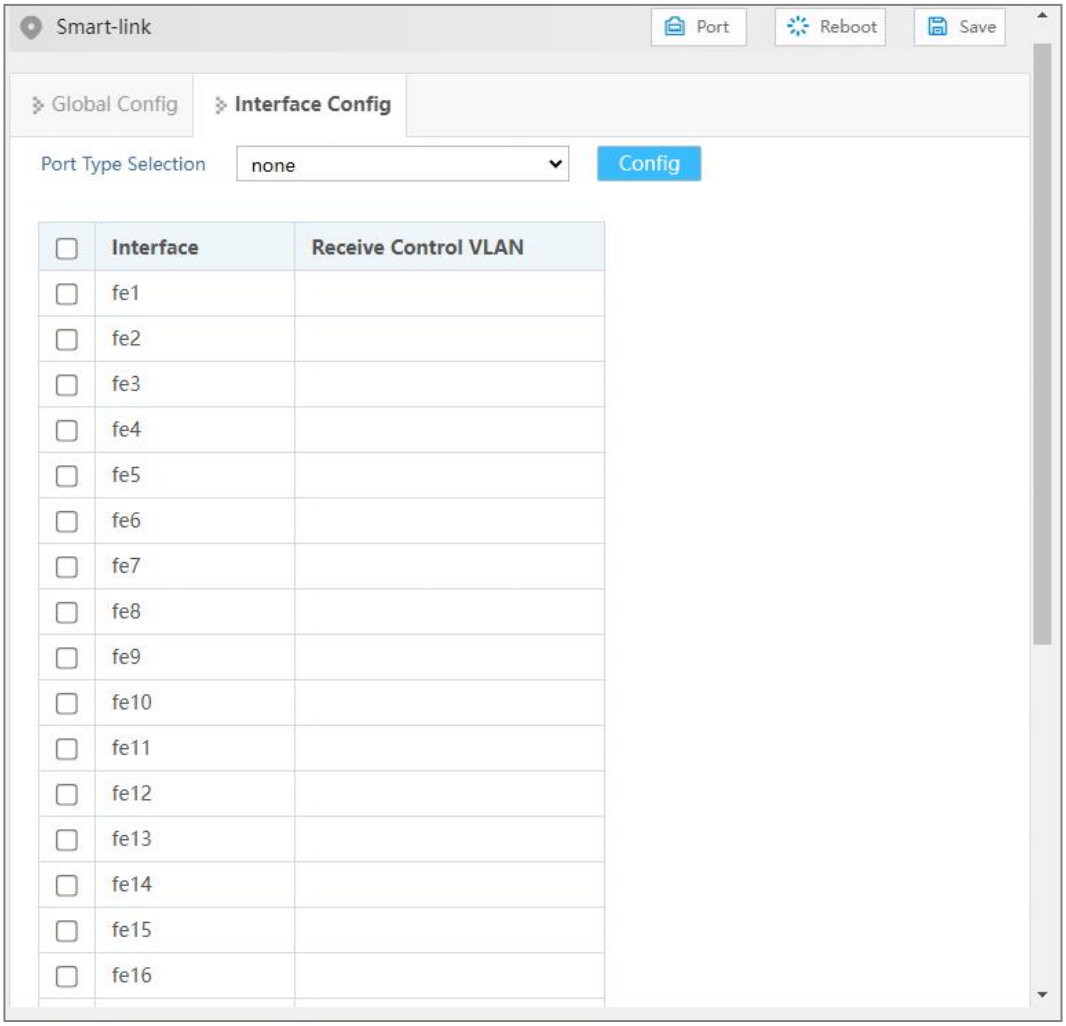
Configure Smart-link interface to receive control VLAN.

Operation Path

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

Interface Description

Interface config interface is as follows:



The main element configuration description of interface config 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

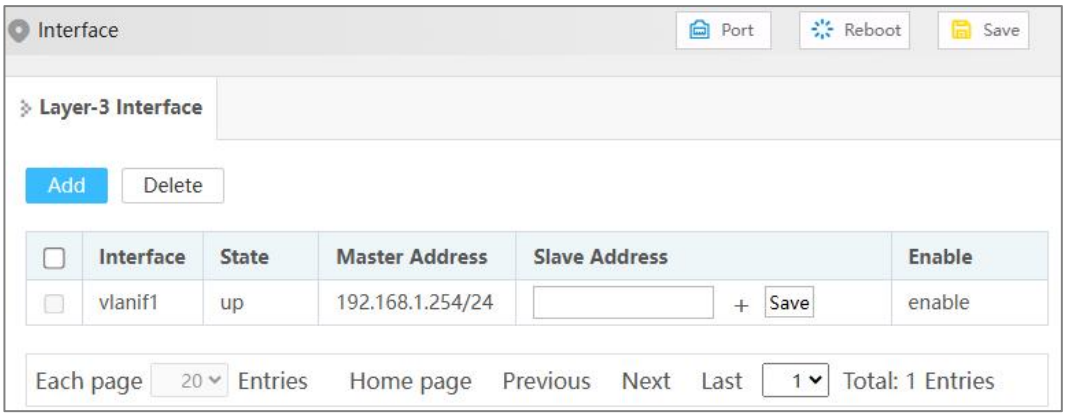
Create layer 3 VlANIF Interfaces and configure interface IP address.

Operation Path

Open in order: "IP Network Configuration > Interface > Layer-3 Interface".

Interface Description

Layer-3 interface configuration interface is as follows:



The main element configuration description of Layer-3 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.
Enable	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 Info

Function Description

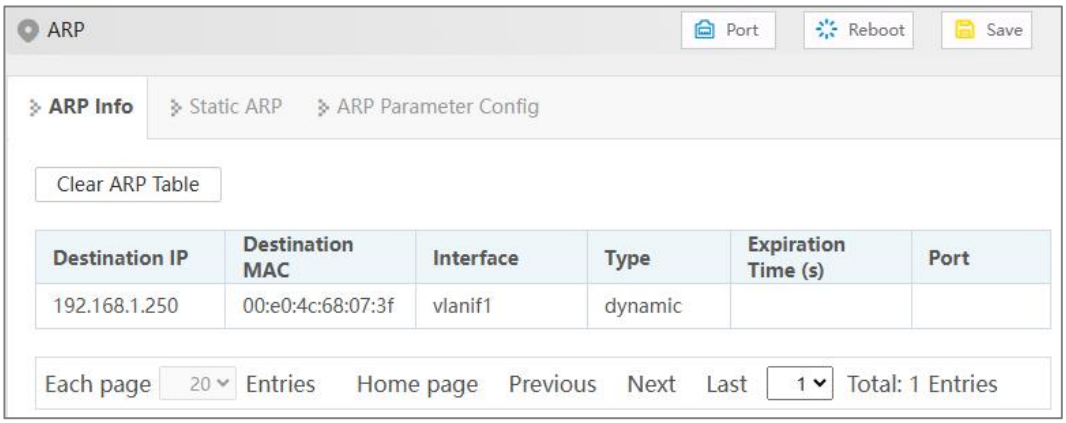
Check information such as IP address, MAC address and interface of the user via ARP table entries.

Operation Path

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

Interface Description

ARP Info interface is as follows:



The main element configuration description of ARP info 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

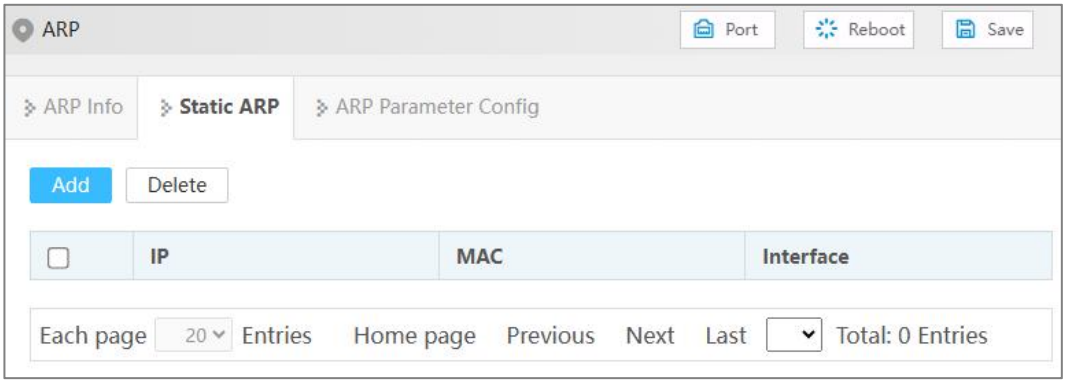
Configure static ARP entries, bind IP address and MAC address to avoid aging and prevent ARP attacks.

Operation Path

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

Interface Description

Static ARP interface is 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 Config

Function Description

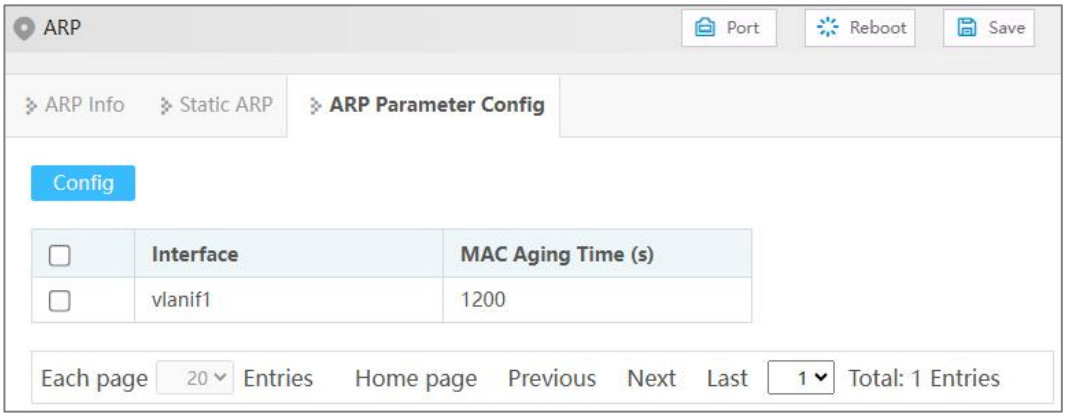
Configure the aging time of dynamic ARP.

Operation Path

Open in order: "IP Network Configuration > ARP > ARP Parameter Config".

Interface Description

ARP parameter config interface is as follows:



The main element configuration description of ARP parameter config interface:

Interface Element	Description

Interface Element	Description
Interface	Display VLANIF Interface name in ARP entry.
MAC Aging Time (s)	Configure aging time of dynamic ARP table entries, the value range is 1-1200 seconds.

7 Unicast Routing Table

7.1 IPv4

7.1.1 IPv4 Routing Table

Function Description

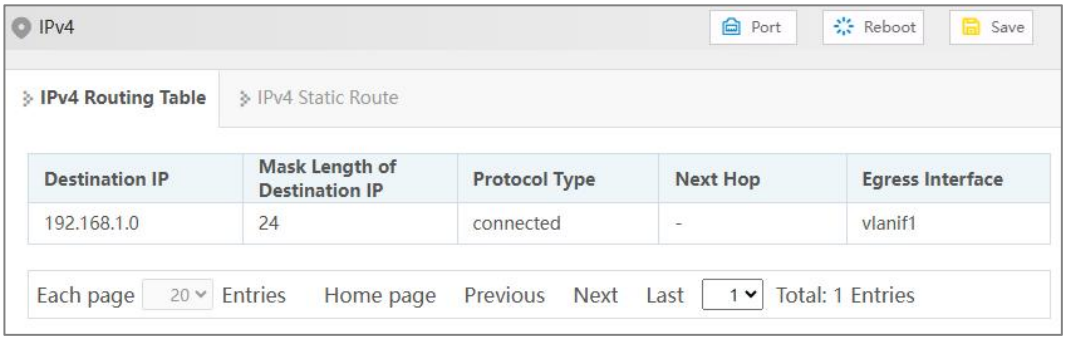
Check IPv4 routing table information.

Operation Path

Open in order: "Unicast Routing > IPv4 > IPv4 Routing Table".

Interface Description

The IPv4 routing table interface is as follows:



The main elements configuration description of IPv4 routing table 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.

Interface Element	Description
Egress Interface	Interface name.

7.1.2 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

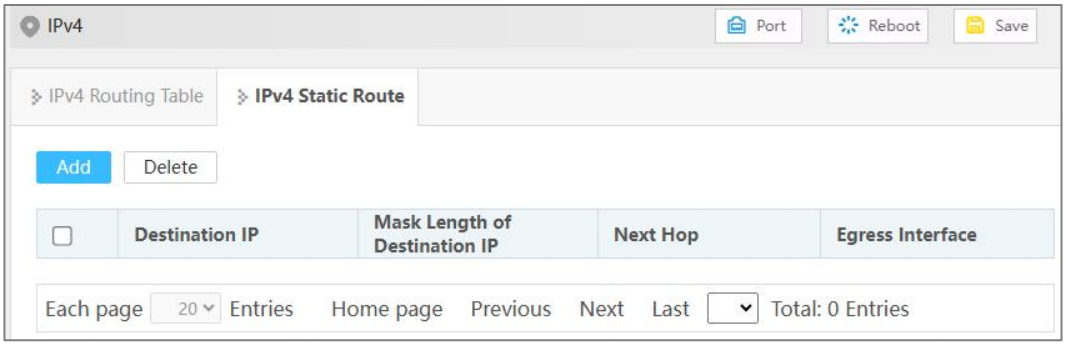
Configure IPv4 static routing.

Operation Path

Open in order: "Unicast Routing > IPv4 > IPv4 Static Route".

Interface Description

The IPv4 Static Route interface is 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.

8 Network Management

8.1 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.

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

8.1.2 View

Function Description

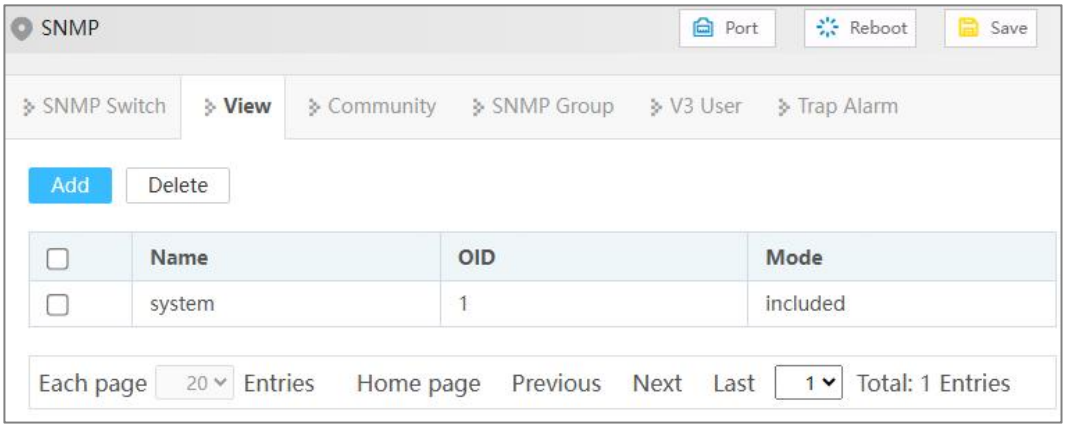
Add/delete SNMP view.

Operation Path

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

Interface Description

View interface is as below:



The main element configuration description of view interface:

Interface Element	Description
Name	SNMP view name definition, support 32 characters input.
OID	Node location information of MIB tree where the device resides.

Interface Element	Description
	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.

8.1.3 Community

Function Description

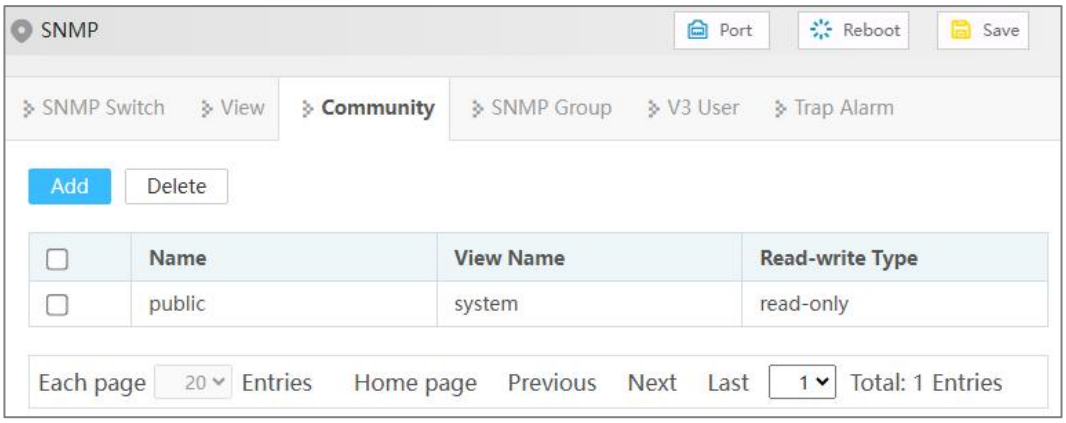
Add/delete SNMP community. Define MIB view that community name can access, set MIB object access privilege of community name as read-write privilege or read-only privilege.

Operation Path

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

Interface Description

Community interface is as below:



The main element configuration description of community interface:

Interface Element	Description
Name	Group name, including numbers or letters, with a length of no more than 32 characters.
View Name	SNMP view name.

Interface Element	Description
Read-write Type	View read-write permissions, options are as follows: • Read only • Read and write

8.1.4 SNMP Group

Function Description

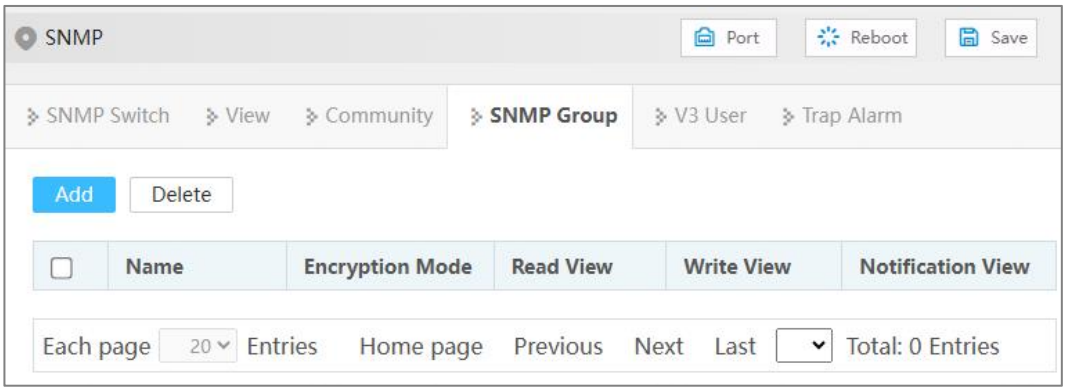
Configure a new SNMP group and set the secure mode and corresponding SNMP view of the SNMP group.

Operation Path

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

Interface Description

SNMP Group interface is 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 encrypted.
Read View	Specify the read view of the group.
Write View	Specify the write and read view of the group.

Interface Element	Description
Notification View	Specify the notification view of the group.

8.1.5 V3 User

Function Description

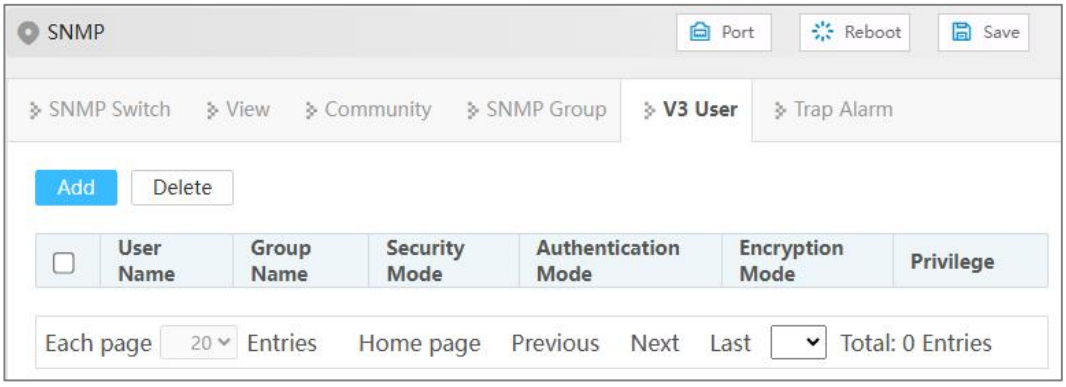
SNMPv3 adopts User-Based Security Model (USM) authentication mechanism. Network manager can configure authentication and encryption function. Authentication is used to verify the validity of the packet sender and prevent unauthorized users from accessing it. Encryption encrypts the transmission packet 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 User".

Interface Description

V3 user interface is as follows:



The main element configuration description of V3 user interface:

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

Interface Element	Description
	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.
Privilege	User protocol type, the options are as follows: • ro: Read only permission, allowing users to get the values of SNMP objects, but not allowing users to set these values. Users can get device status and information through this permission, but cannot set it; • rw: Read and write permission, allowing users to get and set the values of SNMP objects. Users can read the status and information of the device and have the right to make changes, including setting parameters, enabling or disabling functions, etc.

8.1.6 Trap Alarm

Function Description

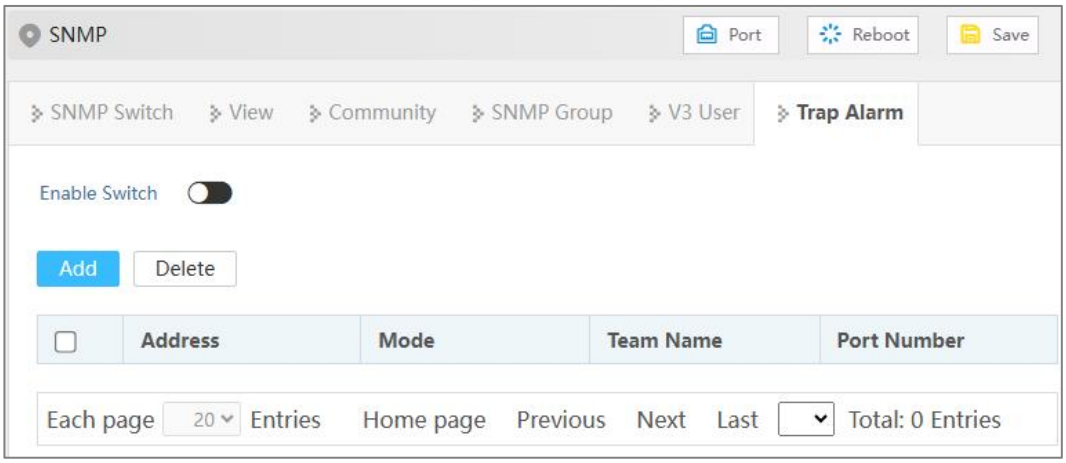
Base on TCP/IP protocol, SNMP usually adopts UDP port 161 (SNMP) and 162 (SNMP-traps), SNMP protocol agent exists in the network device and adopts information specific to the device (MIBs) as the device interface; these network devices can be monitored or controlled via Agent. When a trap event occurs, 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 is as follows:



The main element configuration description of Trap alarm interface:

Interface Element	Description
Enable Switch	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	The number of the port that sends the alarm.

8.2 RMON

RMON (Remote Network Monitoring) mainly achieves statistics and alarm functions, which are used for remote monitoring and management of management device to managed devices. Statistical function refers to that managed device can periodically or continuously keep track of all the traffic information on the network segment connected to the port, for example, the total number of packets received on a network segment in a period of time, or the total number of received super long packets. Alarm function refers to that the managed device can monitor the value of the specified MIB variable. When the value reaches the alarm threshold (such as the port rate reaches the specified value or the proportion of broadcast message reaches the specified value), it can automatically log and send Trap messages to the managed device.

8.2.1 Event

Function Description

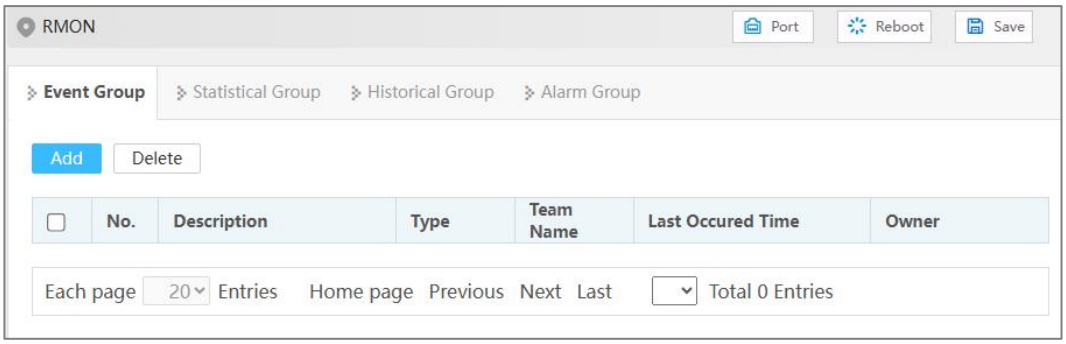
On the "Event" page, user can add, delete or check the configuration information of event.

Operation Path

Open in order: “Network Management > RMON > Event Group”.

Interface Description

Event group interface is as below:



The main element configuration description of event group interface:

Interface Element	Description
No.	Triggered event serial number when monitoring MIB object exceeds threshold value. Note: This serial number corresponds to the rising event index and falling event index set in RMON alarm configuration information.
Description	Some description information for describing the event.
Type	Event dealing method, options as below: • log: Record the event in the log table when the event is triggered; • trap: Send Trap information to management station for informing the occurring of event when the event is triggered; • Log, trap: Record the event in the log table and produce a trap information when the event is triggered.
Team Name	Community name of the network management station receiving the alarm information.
Last Occurred Time	The time of the last incident occurred.
Owner	The creator of the table entry.

Interface Element	Description
Operation	Check the entry and click the "Delete" button to delete it.

8.2.2 Statistical Group

Function Description

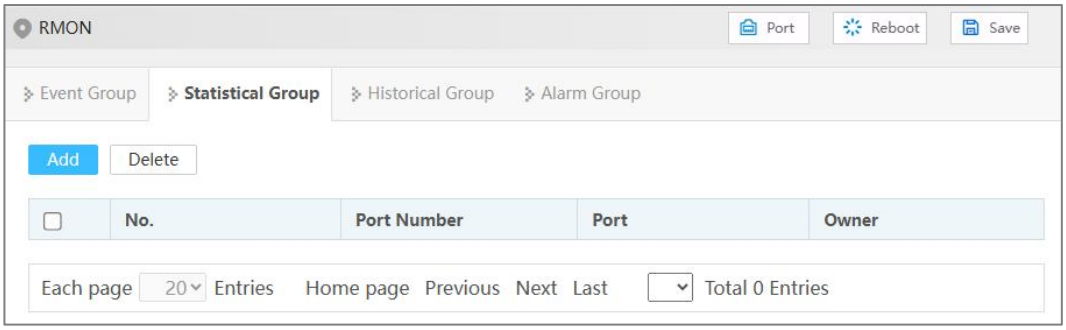
On the "Statistical" page, user can add, delete or check the configuration information of statistical.

Operation Path

Open in order: “Network Management > RMON > Statistical Group”.

Interface Description

Statistical group interface is as below:



The main element configuration description of statistical group interface:

Interface Element	Description
No.	Serial number is used to identify a special application interface, when the serial number is same to the application interface serial number set before, previous configuration will be replaced.
Port Number	The counted port serial number.
Port	The name of the port being counted.
Owner	The creator of the table entry.
Operation	Check the entry and click the "Delete" button to delete it.

8.2.3 Historical Group

Function Description

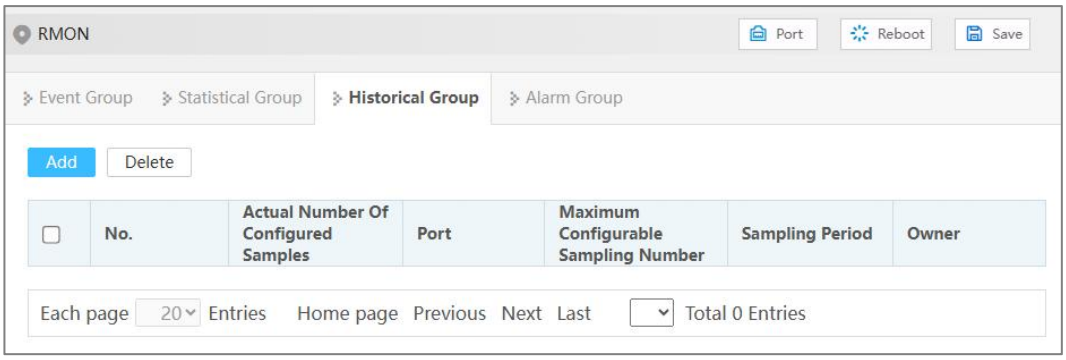
On the "History" page, user can add, delete or check the configuration information of history.

Operation Path

Open in order: “Network Management > RMON > Historical Group”.

Interface Description

Historical group interface is as below:



The main element configuration description of historical group interface:

Interface Element	Description
No.	Serial number is used to identify a special application interface, when the serial number is same to the application interface serial number set before, previous configuration will be replaced.
Actual Number Of Configured Samples	Set the historical statistics capacity corresponding to the history group, ranging from 1-65535.
Port	The recorded port name.
Maximum Configurable Sampling Number	Maximum capacity of historical statistics table supported by device.
Sampling Period	The interval time of gaining statistics data each two times.
Owner	The creator of the table entry.
Operation	Check the entry and click the "Delete" button to delete it.

8.2.4 Alarm

Function Description

On the "Alarm" page, user can add, delete the alarm or check the alarm configuration information. Alarm type adopts absolute to directly monitor MIB object value; Alarm type adopts delta to monitor changes in MIB object values between two samples;

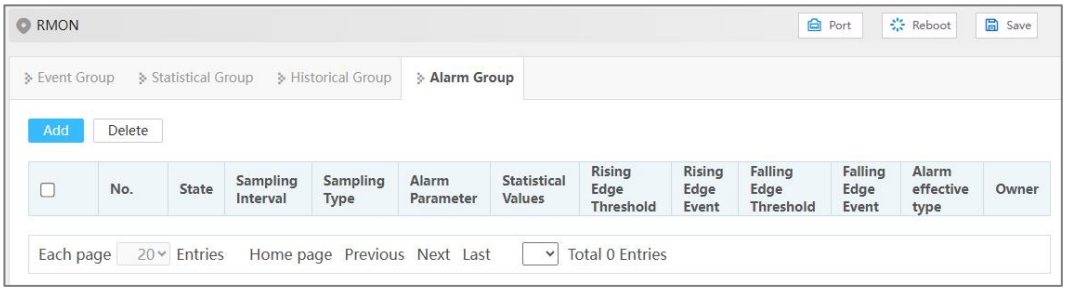
- When monitoring MIB object reaches or surpasses the rising threshold value, it will trigger corresponding event of rising event index;
- When monitoring MIB object reaches or surpasses declining threshold value, it will trigger corresponding event of declining event index;

Operation Path

Open in order: "Network Management > RMON > Alarm Group".

Interface Description

Alarm group interface is as below:



The main element configuration description of alarm group interface:

Interface Element	Description
No.	Triggered event serial number when monitoring MIB object exceeds threshold value. Note: This serial number corresponds to the rising event index and falling event index set in RMON alarm configuration information.
State	The status of alarm list items, which is not configurable when configuring alarm list items and is VALID by default.
Sampling Interval	Sampling time interval value, value range is 1-4294967295, unit: second.
Sampling Type	Two sampling methods, options are as follows: • Absolute: When alarm variable value reaches alarm threshold value, an alarm is triggered; If the second sampling is same to last sampling alarm type, alarm isn't triggered again; • Delta: When alarm variable value reaches alarm

Interface Element	Description
	threshold value during each sampling, an alarm is triggered.
Alarm Parameter	The monitored MIB node supports string format instead of oid format.
Statistical Values	That is, the defined statistical group.
Rising Edge Threshold	Alarm variable value, upper limit alarm, threshold value is between 1-12147483647. Note: In the rising process of alarm variable value, when the variable value surpasses rising threshold, an alarm occurs at least one time.
Rising Edge Event	Event index, when alarm variable value reaches or surpasses the rising event threshold value, it will activate corresponding event in event group, value range is 1-65535.
Falling Edge Threshold	Alarm variable value, lower limit alarm, threshold value is between 1-12147483647. Note: In the falling process of alarm variable value, when the variable value reaches falling threshold, an alarm occurs at least one time.
Falling Edge Event	Event index, when alarm variable value reaches or is less than the falling threshold value, it will activate corresponding event in event group, value range is 1-65535.
Alarm effective type	There are three alarm effect types. The options are as follows: • Rising edge effective • Falling edge effective • Both the rising and falling edges are effective
Owner	The creator of the table entry.
Operation	Check the entry and click the "Delete" button to delete it.

8.3 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.

8.3.1 Global Config

Function Description

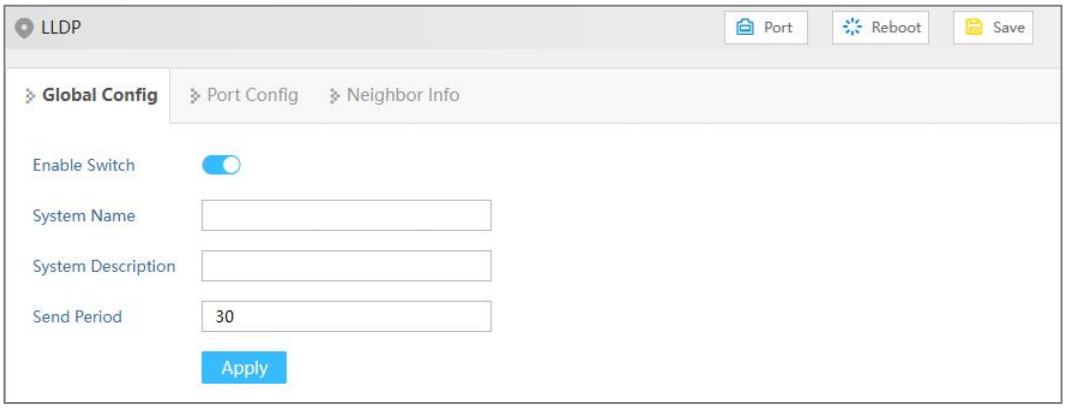
Configure LLDP global parameter.

Operation Path

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

Interface Description

Global config interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Enable Switch	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.

8.3.2 Port Config

Function Description

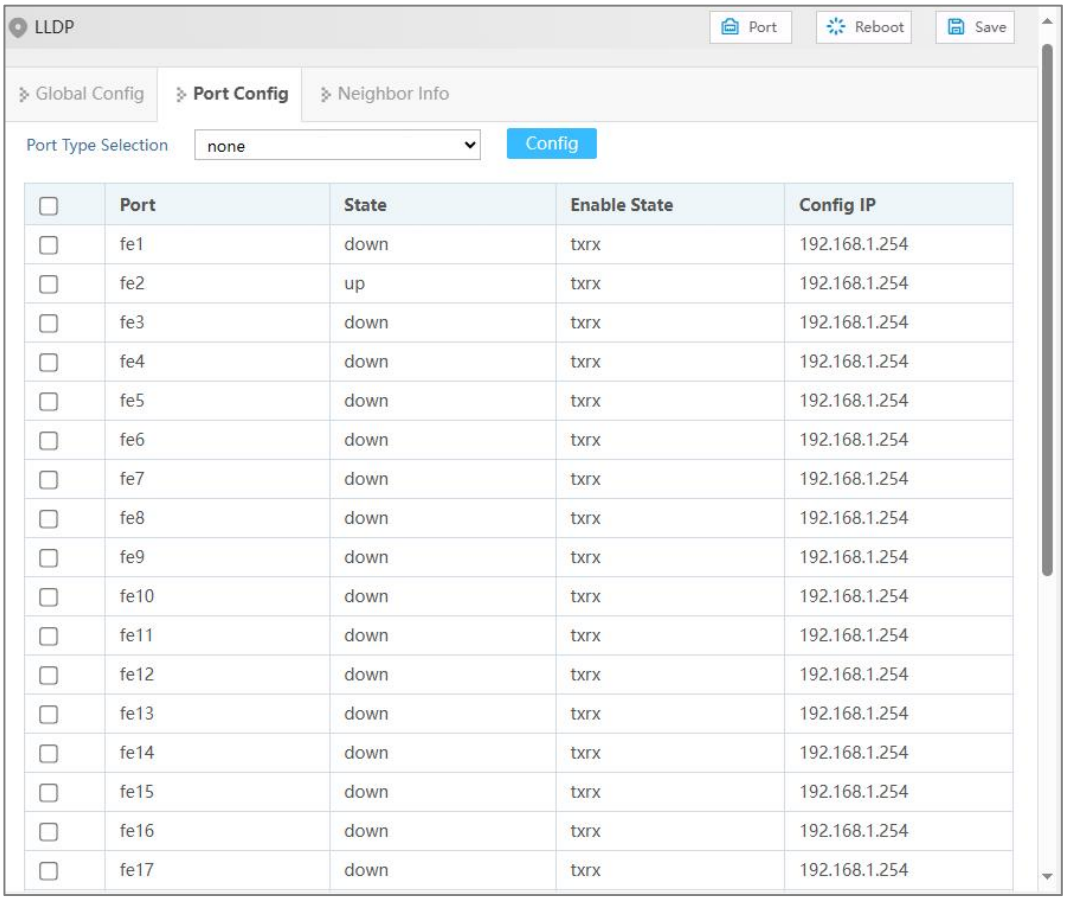
Configure the sending and receiving mode and management address of the port.

Operation Path

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

Interface Description

Check port config interface is as below:



The main element configuration description of port config 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

Interface Element	Description
	receiving LLDP message. • rxonly: working mode Rx, only receiving and not sending LLDP message. • txrx: working mode is TxRx, both sending and receiving LLDP message. • disable: the working mode is Disable, neither receiving nor sending LLDP message. Note: By default, the working mode of LLDP is TxRx when global LLDP is enabled.
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 o in the VLAN where the port resides. If the VLAN is not configured with a main IP address, it will be 0.0.0.0.

8.3.3 Neighbor Info

Function Description

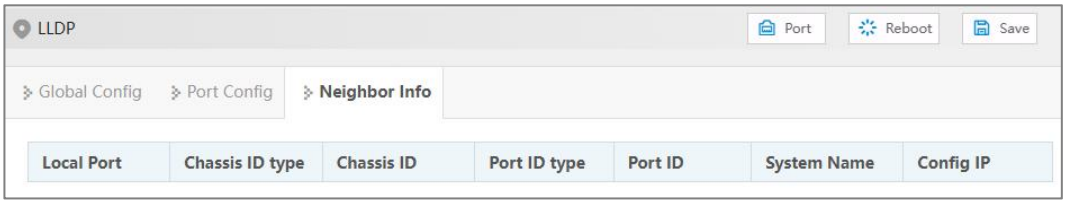
View neighbor-related information.

Operation Path

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

Interface Description

Neighbor info interface is as follows:



Main elements configuration description of neighbor info interface:

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

8.4 DHCP-Server

DHCP (Dynamic Host Configuration Protocol) is usually applied to large LAN environment. Its main functions are centralized management and IP address distribution, which enables the host in the network to acquire IP address, Gateway address, DNS server address dynamically and improve the usage of addresses.

8.4.1 DHCP Switch

Function Description

On the "DHCP Switch" page, user can enable/disable DHCP.

Operation Path

Open in order: "Network Management > DHCP-Server> DHCP Switch".

Interface Description

DHCP switch configuration interface is as follows:

The main element configuration description of DHCP switch configuration interface.

Interface Element	Description
Enable Switch	After enabling the switch, set the device as a DHCP server by setting static allocation address table, the device can

Interface Element	Description
	distribute IP address to devices connected to it.

8.4.2 Address Pool Configuration

After user defines DHCP range and exclusion range, surplus addresses constitute an address pool; addresses in the address pool can be dynamically distributed to hosts in network. Address pool is valid only for the method of automated IP acquisition; manual IP configuration can ignore this option only if conforming to the rules.

DHCP server chooses and distributes IP address and other relative parameters for client from address pool.

DHCP server adopts tree structure: Tree root is the address pool of natural network segment. Branch is the subnet address pool of the network segment. Leaf node is the manually binding client address. The order of address pool at the same level is decided by the configuration order. This kind of tree structure has realized the inheritance of configuration, that is, subnet configuration inherits the configuration of natural network segment, and client configuration inherits the subnet configuration. Therefore, as for some common parameters (such as DNS server address), user only needs to configure in the natural network segment or subnet. Specific inheritance situation as follows:

1. When the parent-child relationship is established, sub address pool will inherit the existing configuration of parent address pool.
2. After the parent-child relationship is established, parent address pool is configured, sub-address pool will inherit or not, two situations as follows:
   - If the child address pool doesn't include the configuration, it will inherit the configuration of parent address pool;
   - If the child address pool has included the configuration, it won't inherit the configuration of parent address pool.

Function Description

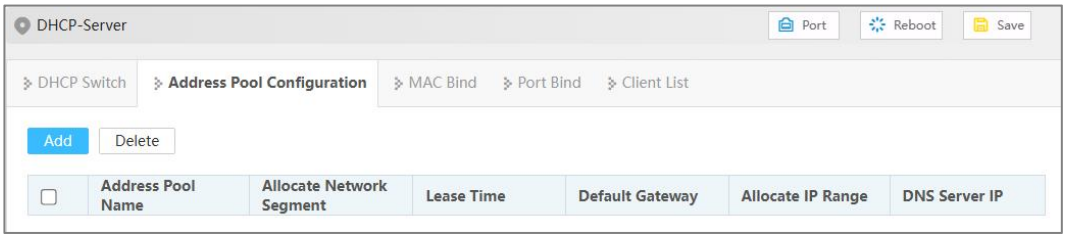
On the "DHCP Pool Configuration" page, user can add, delete the address pool and look over the configuration information of address pool.

Operation Path

Open in order: "Network Management > DHCP > Address Pool Configuration".

Interface Description

Address pool configuration interface is as follows:



The main element configuration description of Address pool configuration interface:

Interface Element	Description
Address Pool Name	The name of address pool, up to 32 characters.
Allocate Network Segment	Address pool distributes the IP address network segment of client, for example: 192.168.0.1/24.
Lease Time	IP address utilization valid time of client, format: day, hour, minute, range is 0-30 day, 0-24h and 0-60m, which are separated by space. Note: When the time of ip address obtained by dhcp client reaches the lease time, it needs to renew it otherwise the ip address would be invalid and dhcp client needs to request ip address again.
Default Gateway	Default client gateway address, example: 192.168.1.0/24
Allocate IP Range	The lowest address and the highest address in the DHCP address pool. The address that belongs to the range could be distributed effectively.
DNS Server IP	IP address of NDS server, for example: 192.168.1.1.
Operation	Click “Edit” button to modify the information of address pool. Click “Delete” under “operation” to delete the corresponding address pool entry directly.
Add	Click “Add” button to add the information of address pool.
Delete	Check address pool entry, click “Delete” button to delete address pool information.

8.4.3 MAC Bind

Function Description

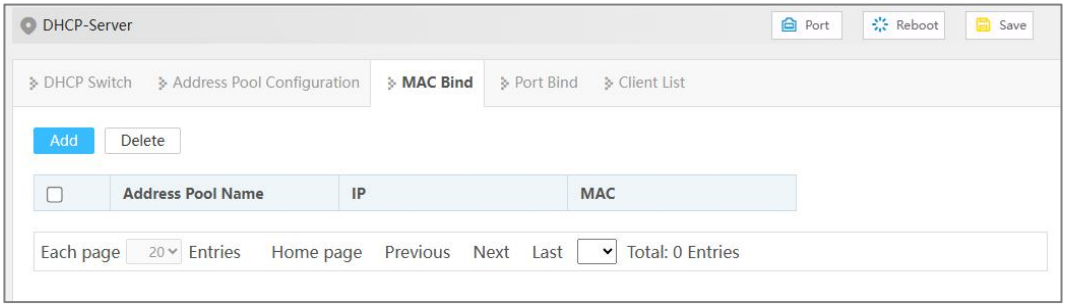
On the “MAC Bind” page, users can bind the IP address assigned by the address pool to the MAC address of the device.

Operation Path

Open in order: "Network Management > DHCP-Server > MAC Bind".

Interface Description

The MAC Bind interface is as follows:



The main element configuration description of MAC binding interface:

Interface Element	Description
Add	Click the "Add" button to add a static binding between the IP address assigned by the address pool and the MAC address of the device.
Delete	After checking the entry, click the "Delete" button to delete the binding of the corresponding IP address and MAC address.
Address Pool Name	Corresponding list name of DHCP address pool.
IP	IP addresses distributed by DHCP address pool, and IP addresses obtained by this MAC address.
MAC	The MAC address information of this device.
Operation	Click "Delete" under "operation" to delete this MAC binding.

8.4.4 Port Bind

Function Description

On the “Port binding” page, users can bind the relationship of IP addresses assigned by ports. Device A enables DHCP Server function and sets 2 static distribution

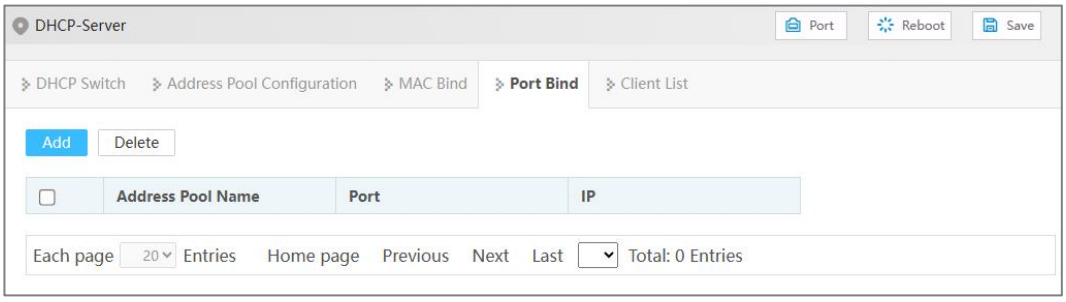
address tables: 192.168.1.19 corresponding port is 1; 192.168.1.20 corresponding port is 2. After device B enables IP address automated acquisition function, if device A is connected to device B via port 1, device B can automatically gain IP address 192.168.1.19; If device A is connected to device B via port 2, device B can automatically gain IP address 192.168.1.20.

Operation Path

Open in order: "Network Management > DHCP-Server > Port Bind".

Interface Description

Port binding interface is as follows:



The main element configuration description of port bind interface:

Interface Element	Description
Add	Click "Add" button to add a static binding between IP address allocated by address pool and layer 2 port.
Delete	After checking the entry, click the "Delete" button to delete the binding between the corresponding IP address and the layer 2 port.
Address Pool Name	Corresponding list name of address pool.
IP	IP address distributed by DHCP address pool, the IP addresses that client gains in the port.
Port	The corresponding port name of the device Ethernet port.
Operation	Click “Delete” under “Operation” to delete this port binding.

8.4.5 Client List

Function Description

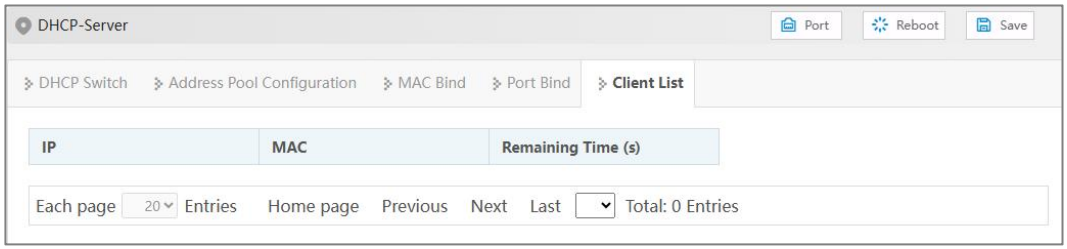
On the "Client List" page, user can look over the information of DHCP client.

Operation Path

Open in order: "Network Management > DHCP-Server > Client List".

Interface Description

Client list interface is as follows:



The main element configuration description of client list interface:

Interface Element	Description
IP	IP address of DHCP client device.
MAC	MAC address of DHCP client device.
Remaining Time (s)	Valid remaining time of DHCP client.

8.5 Modbus TCP

Function Description

Modbus TCP monitoring function can be enabled. Client can read the switch system, port, ring network, frame statistics and other parameters information via Modbus TCP protocol, which are convenient for various integrated systems to monitor and manage the device.

Note

Please see the switch read-only register address information in the "Modbus TCP data sheet" of this section.

Operation Path

Open in order: "Network Management > Modbus TCP".

Interface Description

Interface screenshot of Modbus TCP:

The main element configuration descriptions of Modbus TCP:

Interface Element	Description
Modbus TCP	Modbus TCP monitoring enable switch, which is disabled by default. After enabling Modbus TCP monitoring function, client can read the switch device information via function code 4.

Modbus_TCP Data Sheet

Switch read-only register (support function code 4) address information and stored device information, as the table below:

Note

The following table address is hexadecimal format, please convert it into suitable format according to the demands of current debugging tool.

Information Type	Address (HEX)	Data Type	Description
System Information	0x0000	2 Words	Device ID (reserved)
	0x0002	16 Words	Name (ASCII display)
	0x0012	16 Words	Description (ASCII display)
	0x0022	3 Words	MAC Address (HEX display)
	0x0025	2 Words	IP address
	0x0027	16 Words	Contact Information
	0x0037	16 Words	Firmware Ver (ASCII display)
	0x0047	16 Words	Hardware Ver (ASCII display)
	0x0057	16 Words	Serial No.
	0x0067	1 Word	Power supply 1 status: 0x0000: OFF

Information Type	Address (HEX)	Data Type	Description
			0x0001: ON
	0x0068	1 Word	Power supply 2 status: 0x0000: OFF 0x0001: ON
Port Information	0x1000-0x101B	1 Word	Port connection status: 0x0000: Link down 0x0001: Link up 0x0002: Disable 0xFFFF: No port
	0x101D-0x1038	1 Word	Port operating mode: 0x0000: 10M-Half 0x0001: 10M-Full 0x0002: 100M-Half 0x0003: 100M-Full 0x0004: 1G-Half 0x0005: 1G-Full 0xFFFF: No port
	0x1039-0x1054	1 Word	Port flow control status: 0x0000: OFF 0x0001: ON 0xFFFF: No port
	0x1056-0x1071	1 Word	Port interface type: 0x0000: Copper port 0x0001: Fiber port 0x0002: Combo port 0xFFFF: No port
Frame Statistics	0x2000-0x2037	2 Word	Port 1-28 Tx Packets For example: sending packets quantity of port 1 is 0x44332211, namely: Word 1 is 0x4433; Word 2 is 0x2211.
	0x2039-0x2070	2 Word	Port 1-28 Rx Packets For example: Receiving packets quantity of port 1 is 0x44332211,

Information Type	Address (HEX)	Data Type	Description
			namely: Word 1 is 0x4433; Word 2 is 0x2211.
	0x2072-0x20A9	2 Word	Port 1-28 Tx Error Packets For example: sending error packets quantity of port 1 is 0x44332211, namely: Word 1 is 0x4433; Word 2 is 0x2211.
	0x20AB-0x20E2	2 Word	Port 1-28 Rx Error Packets. For example: receiving error packets quantity of port 1 is 0x44332211, namely: Word 1 is 0x4433; Word 2 is 0x2211.
Ring Information	0x3000	1 Word	Link redundancy algorithm category: 0x0000: None 0x0001: SW-Ring V1 0x0002: SW-Ring V2 0x0003: SW-Ring V3 0x0004: RSTP
	0x3001	1 Word	Group I Ring Type: 0x0000: Single Ring 0x0001: Coupling Ring 0x0002: Chain 0x0003: Dual_homing
	0x3002	1 Word	Group I Ring Port 1
	0x3003	1 Word	Group I Ring Port 2
	0x3004	1 Word	Group I Ring ID:
	0x3005	1 Word	Group I HelloTime
	0x3006	1 Word	Group I Enable
	0x3007	1 Word	Group I Master- slave device: 0x0000: master device 0x0001: slave device

Information Type	Address (HEX)	Data Type	Description
	0x3008	1 Word	Group II Ring Type: 0x0000: Single Ring 0x0001: Coupling Ring 0x0002: Chain 0x0003: Dual_homing
	0x3009	1 Word	Group II ring port1
	0x300A	1 Word	Group II ring port2
	0x300B	1 Word	Group II Ring ID
	0x300C	1 Word	Group II HelloTime
	0x300D	1 Word	Group II Enable
	0x300E	1 Word	Group II Master-slave device: 0x0000: master device 0x0001: slave device
	0x300F	1 Word	Group III Ring Type: 0x0000: Single Ring 0x0001: Coupling Ring 0x0002: Chain 0x0003:Dual_homing
	0x3010	1 Word	Group III ring port1
	0x3011	1 Word	Group III ring port2
	0x3012	1 Word	Group III Ring ID
	0x3013	1 Word	Group III HelloTime
	0x3014	1 Word	Group III Enable
	0x3015	1 Word	Group III Master-slave device: 0x0000: master device 0x0001: slave device
	0x3016	1 Word	Group IV Ring Type: 0x0000: Single Ring 0x0001: Coupling Ring 0x0002: Chain 0x0003: Dual_homing
	0x3017	1 Word	Group IV ring port1
	0x3018	1 Word	Group IV ring port2
	0x3019	1 Word	Group IV Ring ID

Information Type	Address (HEX)	Data Type	Description
	0x301A	1 Word	Group IV HelloTime
	0x301B	1 Word	Group IV Enable
	0x301C	1 Word	Group IV Master-slave device: 0x0000: master device 0x0001: slave device

Instance: MODBUS TCP Configuration

Acquire the switch device name information via DebugTool analogue client, the switch information as follows:

- Switch default IP address: 192.168.1.254;
- Address of switch register that stores the device name information: 0x002;
- Number of switch register that stores the device name information: 16 words;

Operation Steps

First, configure the switch Modbus TCP monitoring enable.

Step 1 Log into Web configuration interface.

Step 2 Select "Network Management > Remote Monitoring > Modbus TCP".

Step 3 Slide on the "Modbus TCP" enable switch, as shown in the figure below.

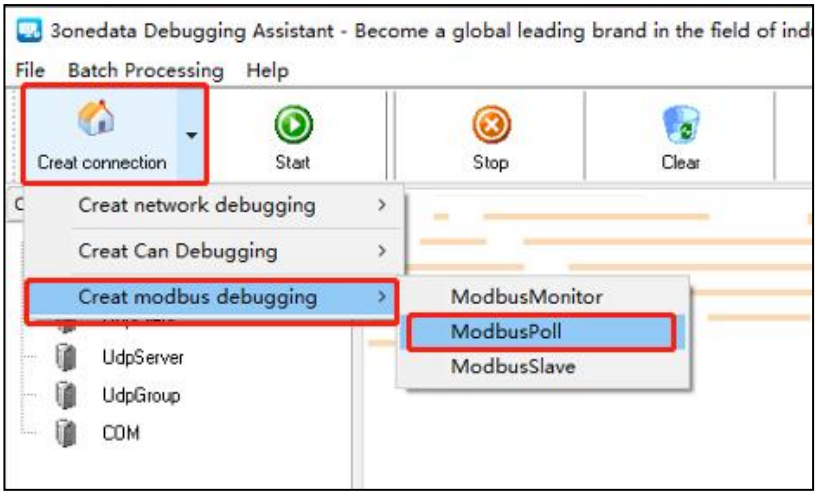
Step 4 End.

Then, run the debug tool software to acquire the device parameters.

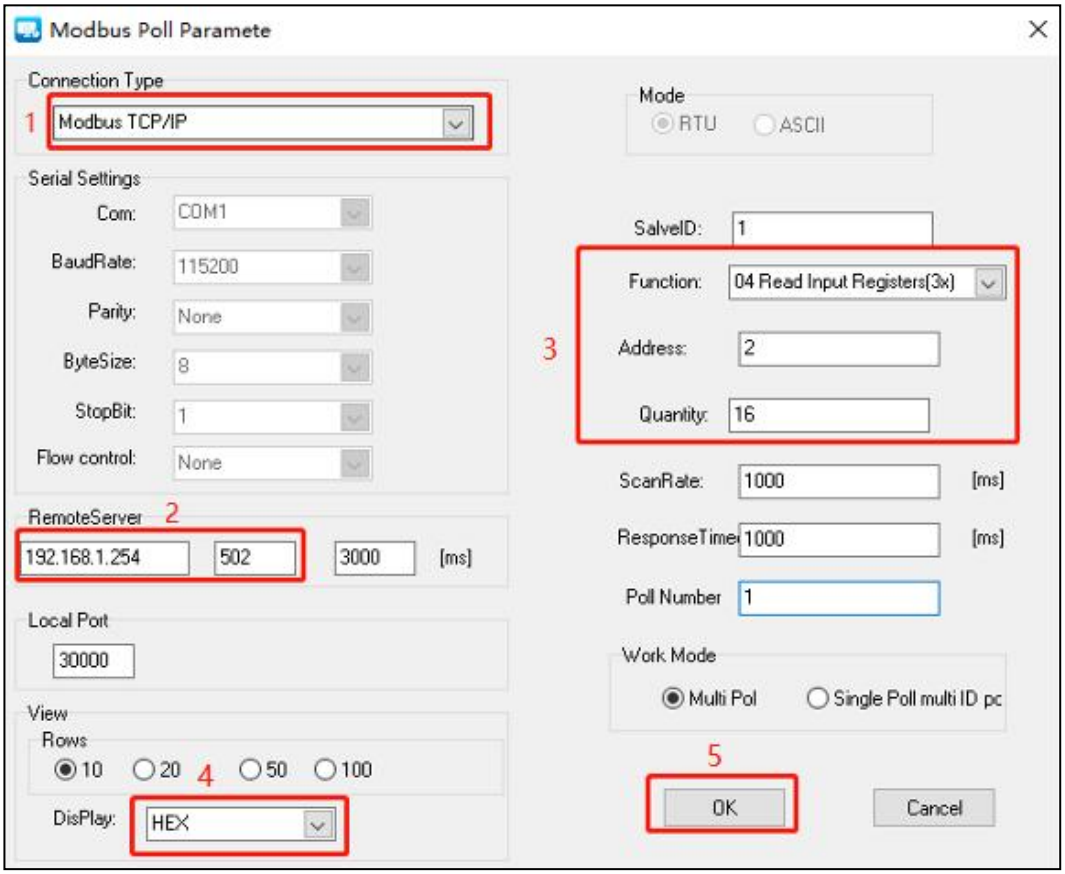
Step 5 Open "Debug Tool".

Step 6 Click the drop-down list of "Create connection".

Step 7 Select "Create Modbus debugging > ModbusPoll", as the picture below.



Step 8 Configuration window of ModbusPoll parameters pops up, the configuration as the picture below:



1 On the drop-down list of "Connection Type", select "Modbus TCP/IP";

1 Enter the switch IP address "192.168.1.254" and port number "502" on the column of "Remote Server";

2 Select "04 Read Input Registers (3x)" on the drop-down list of "Function";

3 Enter decimal device name register address "2" on the text box of "Address";

Notice:

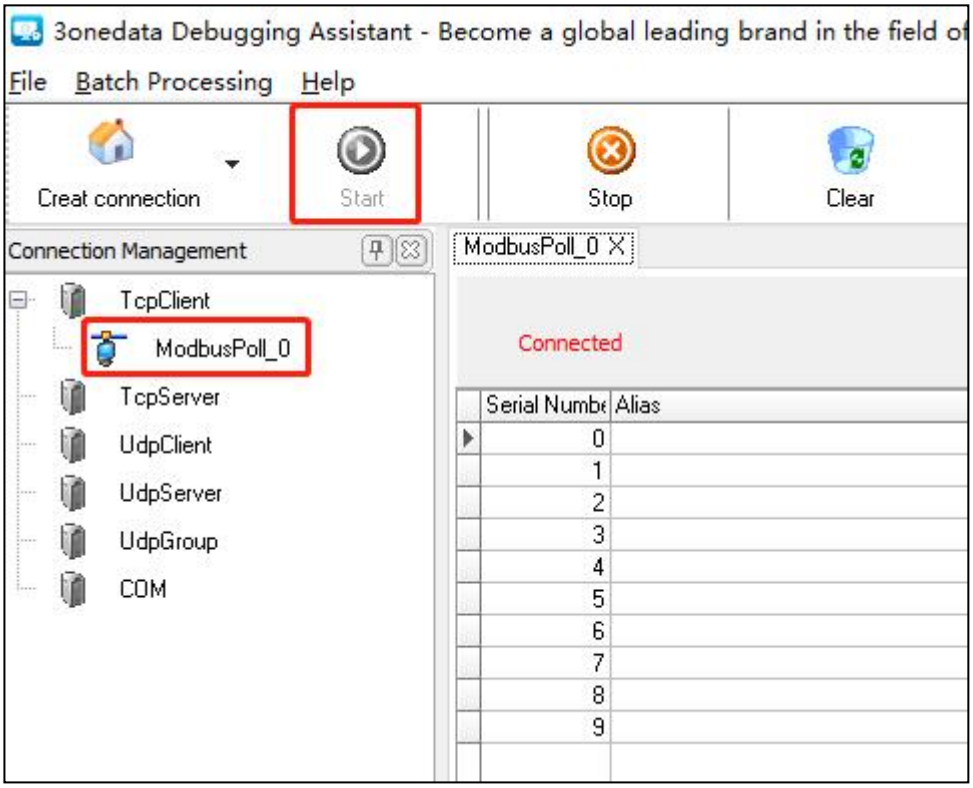
Here the start address is decimal format, so hexadecimal register address should be converted into decimal format.

4 Enter the register amount "16" on the text box of "Quantity";

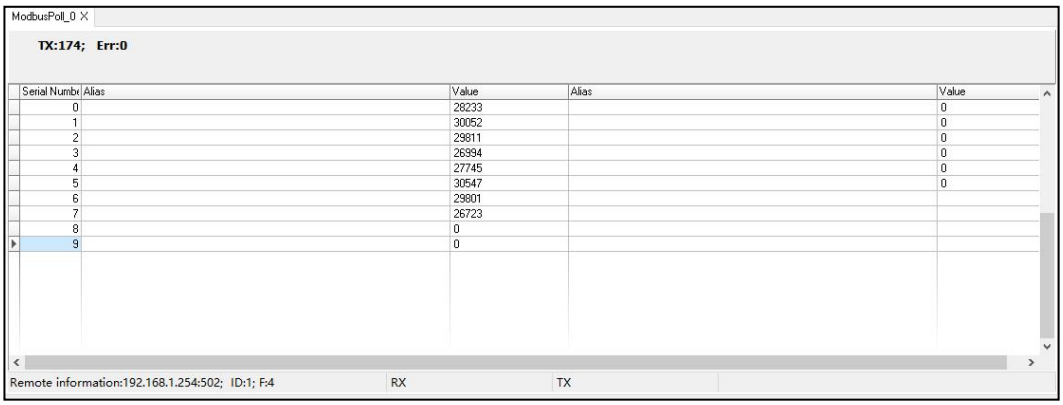
5 Select "HEX" on the drop-down list of "Display";

6 Click "OK".

Step 9 On the page of Debug Tool, select created ModbusPoll, and then click "Start";



Step 10 Check responsive data, and convert the hexadecimal value read by register into ASCII code, displayed as "Industrial Switch";



Step 11 End.

Note

- Switch can establish 4 Modbus TCP monitoring connections at the same time.
- Switch Port Information, Frame Statistics and Ring Network Information. It supports the sequential read of port parameters of multiple registers. For example, address range of the register that stores port connection status information is 0x1000-0x101B, each register data is 1 word; when the start address of register is 0x1000, the register number is 1, it will read port 1 status; If the register quantity is 10, it will read the status from Port 1 to Port 10; If the port doesn't exist, then the read data will be 0xFFFF.

9 System Maintenance

9.1 Network Diagnosis

9.1.1 Ping

Function Description

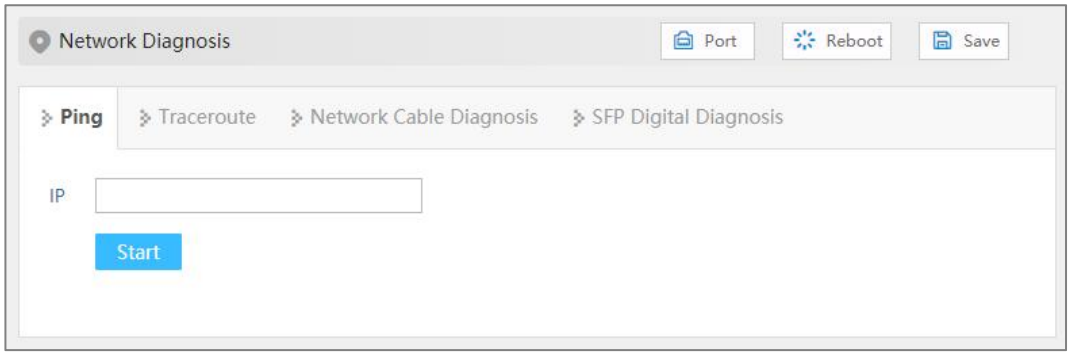
Ping is used to check whether the network is open or network connection speed. The Ping command uses the uniqueness of the IP address on the network to send a packet to the target IP address, and then asks to return a packet of the same size to determine whether the network is connected and what the delay is.

Operation Path

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

Interface Description

The Ping interface is as follows:



The main element configuration description of Ping interface:

Interface Element	Description
IP	The IPv4 or IPv6 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.

9.1.2 Traceroute

Function Description

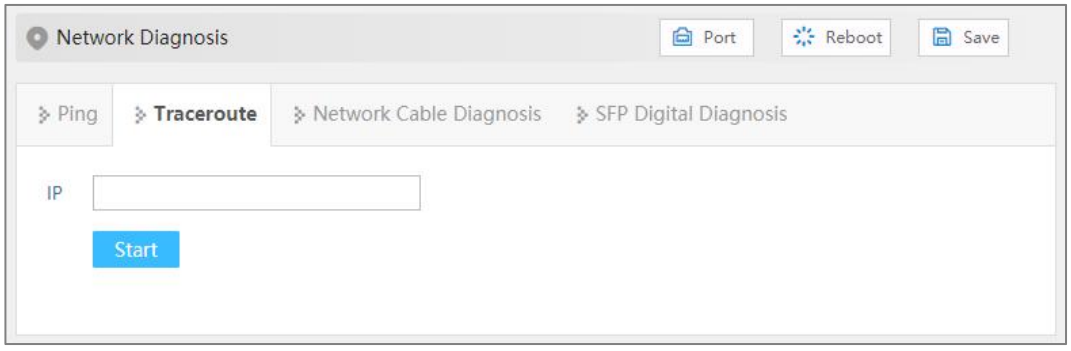
Test the network situation between the switch and the target host. Traceroute measures how long it takes by sending small packets to the destination device until they return. Each device on a path Traceroute returns three test results. Output result includes each test time (ms), device name (if exists)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

Operation Path

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

Interface Description

Traceroute interface is as follows:



The main element configuration description of Traceroute interface:

Interface Element	Description
IP	Destination device IPv4 or IPv6 address, fill in the opposite device IP address that needs test.

9.1.3 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

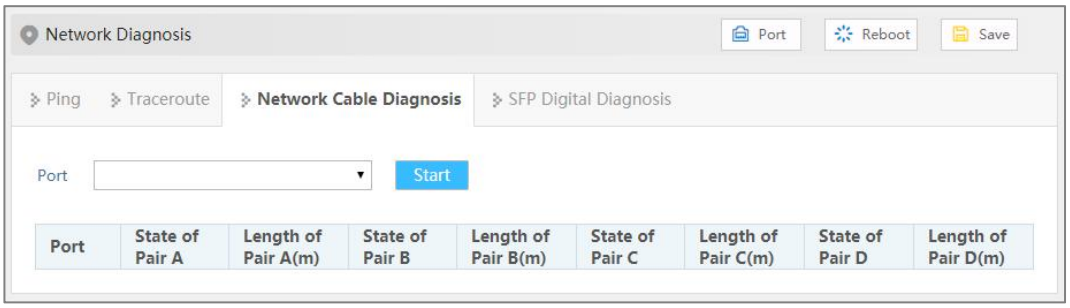
- The accuracy of detecting cable length is about 5 meters, and the test results are for reference only. The test results of different types or different manufacturers may be different.
- When testing, it will affect the normal use of the interface business in a short time, and may also cause the interface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

9.1.4 SFP Digital Diagnosis

Function Description

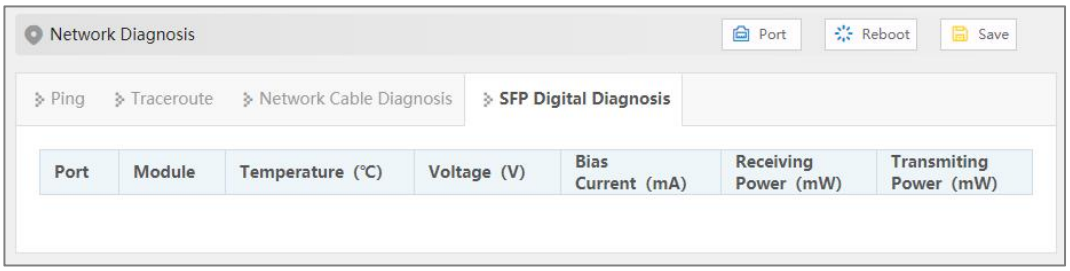
Monitor SFP parameters in real time. This function has greatly facilitated the troubleshooting process of optical fiber link and the cost of on-site debugging.

Operation Path

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

Interface Description

The SFP digital diagnosis 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.

9.2 Time

9.2.1 NTP Config

The full name of NTP protocol is 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

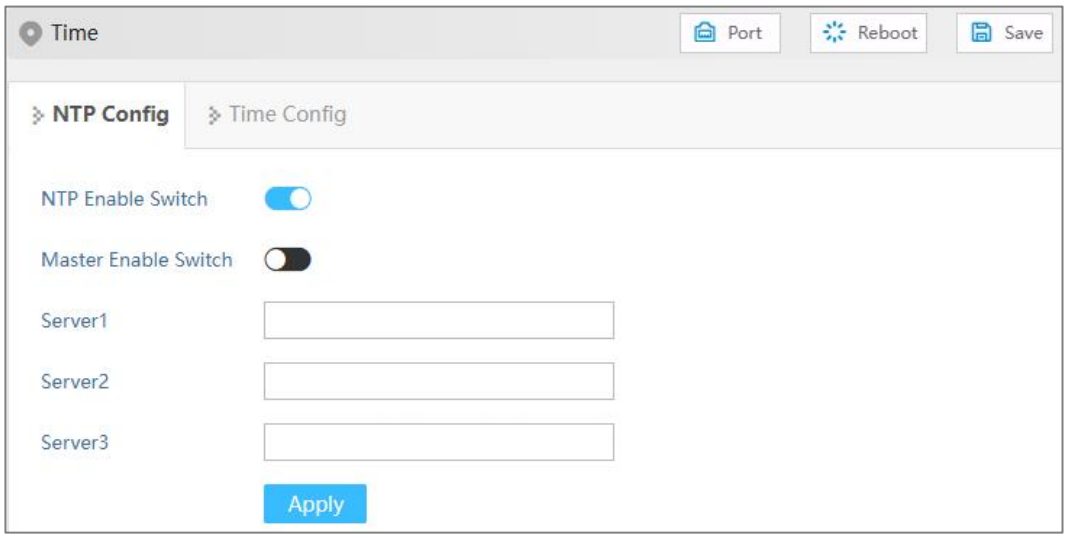
Configure the device time and NTP server information.

Operation Path

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

Interface Description

The NTP config interface is as follows:



Main element configuration description of NTP config interface:

Interface Element	Description
NTP Enable Switch	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.
Server	IP address of NTP server, for example: 192.168.1.1.

Interface Element	Description
	Note: As NTP client, the system will synchronize time with NTP server every 11 minutes.

9.2.2 Time Zone Configuration

Function Description

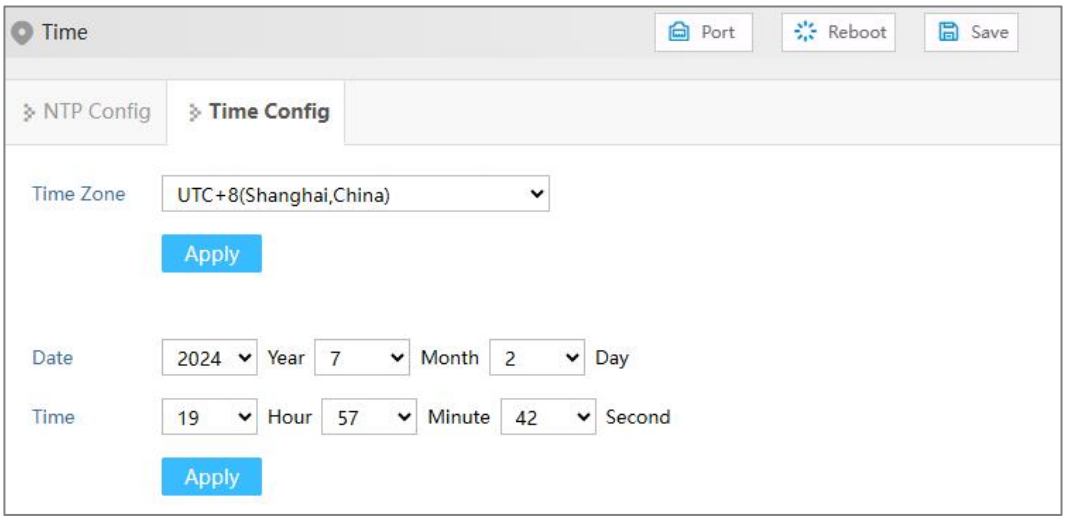
Configure the device time zone.

Operation Path

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

Interface Description

Time Zone Configuration interface is as follows:



Main elements configuration description of Time Config interface:

Interface Element	Description
Time Zone	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	Month/Day/Year
Time	Hour/Minute/Second

9.3 Alarm

9.3.1 Alarm Trigger

Function Description

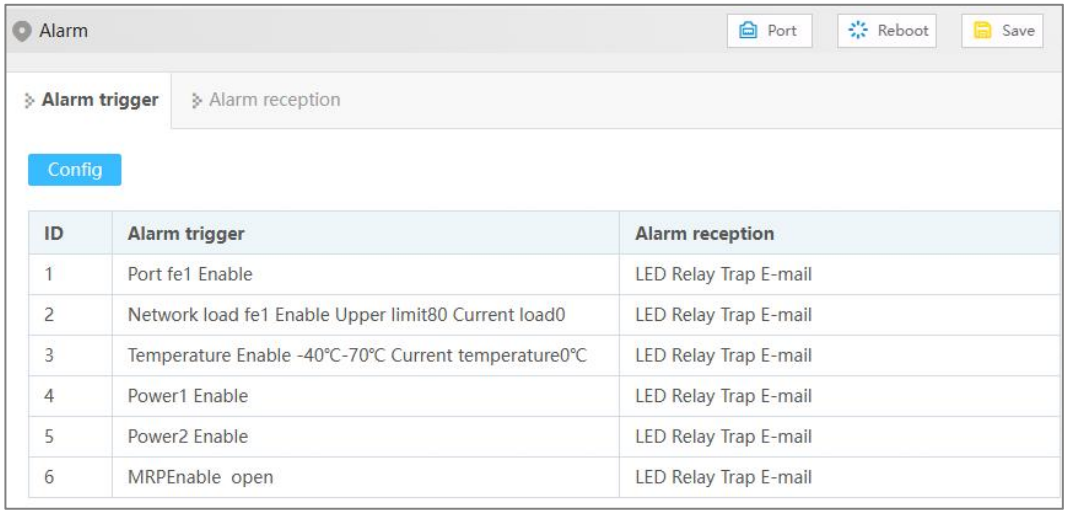
The device system provides multiple alarm trigger sources, including port status, abnormal temperature, power failure, MRP and excessive network load. When these trigger sources are activated, users can trigger the alarm by configuring LED indicator, relay, Trap message or email alarm mode, so as to respond and deal with potential problems in time.

Operation Path

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

Interface Description

The Alarm trigger interface is as follows:



The main element configuration description of Alarm trigger interface:

Interface Element	Description
ID	Alarm trigger entry.
Alarm trigger	Device alarm triggers include port, temperature, power supply, MRP and network load.
Alarm reception	Device alarm modes include LED, relay, Trap and E-mail.

9.3.1.1 Port Alarm

Function Description

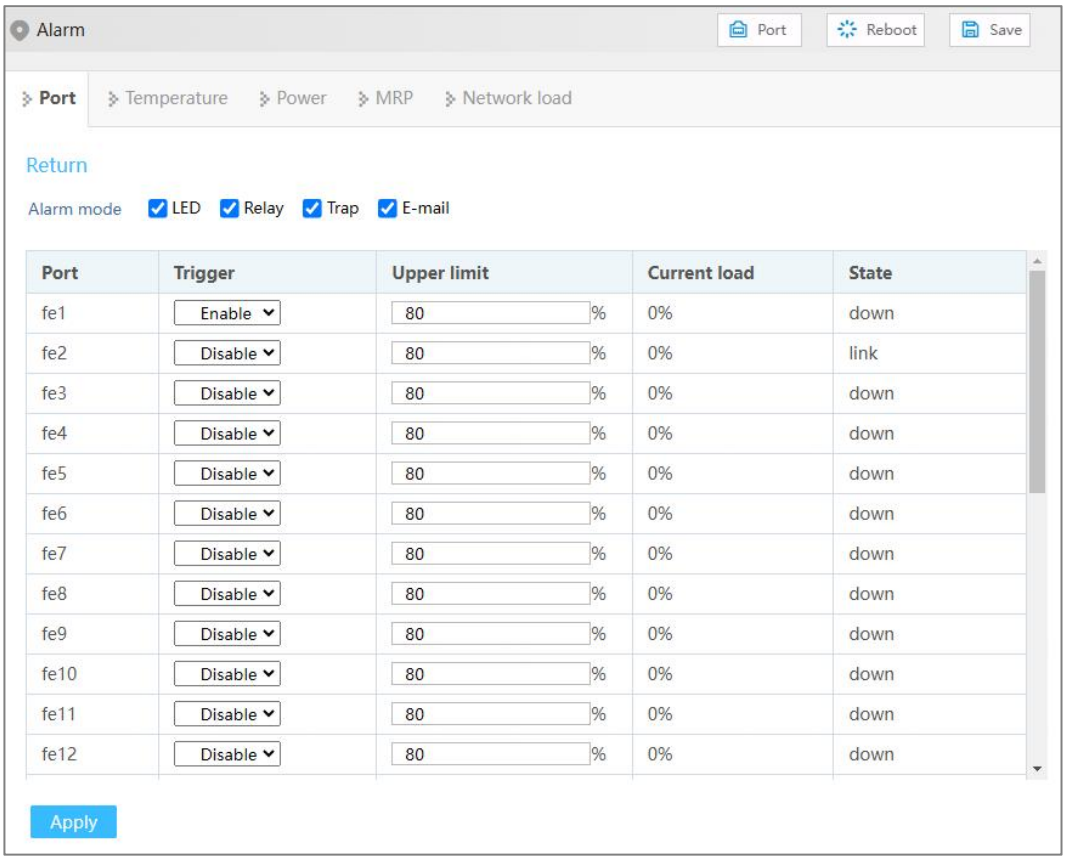
Configure the port alarm function. When the device port is in an abnormal state, the administrator can be informed in time, and the device state can be quickly repaired to avoid excessive loss.

Operation Path

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

Interface Description

Port alarm interface is as below:



The main element configuration description of port alarm configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
State	Port link status, display items as follows: • link • down
Trigger	Port alarm function status, options are as follows: • Enable

Interface Element	Description
	• Disable Note: After enabling port alarm, when port occurs abnormal status, such as disconnection, the device will output an alarm signal to hint the abnormal operation of device port via setting LED indicator, relay, Trap message or e-mail.
Alarm mode	Alarm mode of port alarm, with options: • LED • Relay • Trap • E-mail Note: If checked, the LED indicator, relay, Trap message or email alarm mode will be turned on to trigger the alarm.

9.3.1.2 Temperature Alarm

Function Description

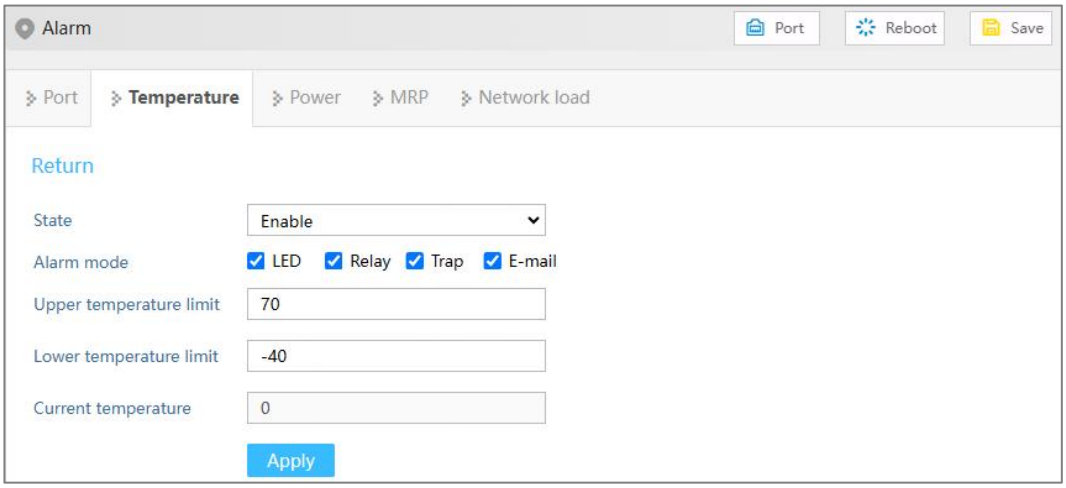
Configure the temperature alarm function. When the device temperature is in an abnormal state, the administrator can be informed in time, and the device can be quickly protected to avoid damage.

Operation Path

Open in order: "System Maintenance > Alarm > Alarm Trigger > Temperature".

Interface Description

The temperature alarm interface is as follows:



The main element configuration description of temperature alarm interface:

Interface Element	Description
State	Temperature alarm switch status, with options: • Enable • Disable Note: After the temperature alarm is enabled, when the temperature of the device is abnormal, such as when the temperature exceeds the set upper limit or lower limit, the device will output an alarm signal to remind the device that the temperature is abnormal by setting LED indicator, relay, Trap message or email.
Upper temperature limit	Set the upper limit temperature of the device, ranging from -40 to 120℃.
Lower temperature limit	Set the lower limit temperature of the device, ranging from -40 to 120℃.
Current temperature	Current temperature state of the device.
Alarm mode	Alarm mode of temperature alarm, with options: • LED • Relay • Trap • E-mail Note: If checked, the LED indicator, relay, Trap message or email alarm mode will be turned on to trigger the alarm.

9.3.1.3 Power Alarm

Function Description

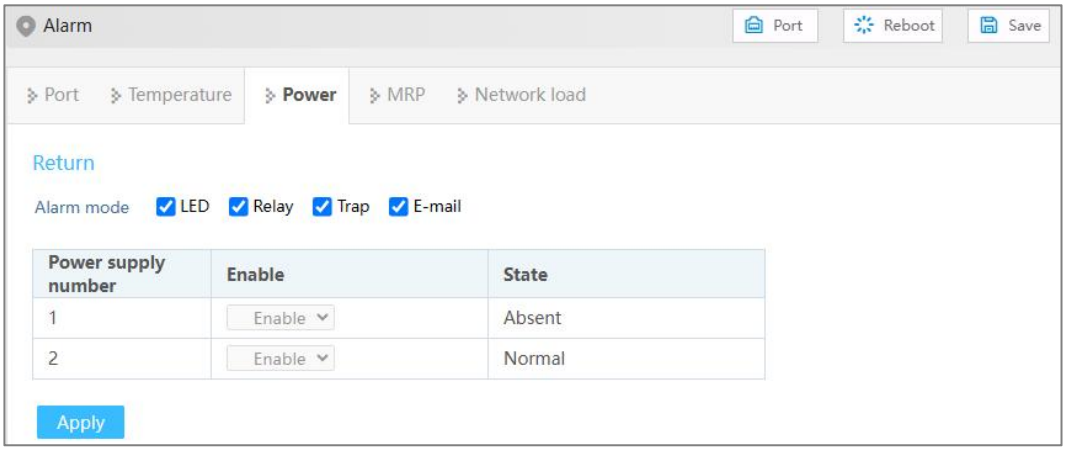
The device system provides this function, and you can set the power alarm function.

Operation Path

Open in order: "System Maintenance > Alarm > Alarm Trigger > Power ".

Interface Description

Power alarm interface is as below:



Main elements configuration description of power alarm interface:

Interface Element	Description
Power supply number	The corresponding name of this device's power supply.
Enable	The state of power supply alarm, with options: • Enable • Disable Note: The power alarm is applicable to dual power supplies. After it is enabled, when one of the power supplies is disconnected or fails, the device will output an alarm signal to hint the abnormal operation of device power via LED indicator, relay, Trap message or email.
State	Device power link status, display items as follows: • Normal • Absent
Alarm mode	Alarm mode of power alarm, with options: • LED • Relay • Trap • E-mail Note: If checked, the LED indicator, relay, Trap message or email alarm mode will be turned on to trigger the alarm.

9.3.1.4 MRP Alarm

Function Description

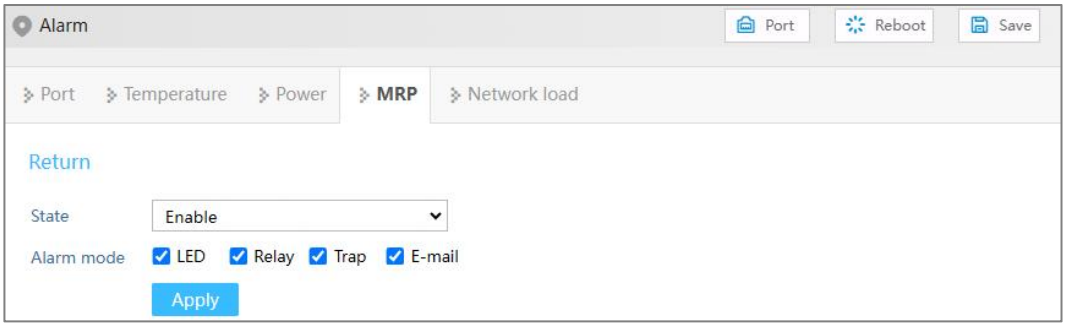
The device system provides this function, and you can set MRP alarm function.

Operation Path

Open in order: "System Maintenance > Alarm > Alarm Trigger > MRP".

Interface Description

The MRP alarm interface is as follows:



The main element configuration description of MRP interface:

Interface Element	Description
State	MRP alarm switch status, with options: • Enable • Disable Note: After enabling MRP alarm, when device ring network occurs abnormal status, such as disconnection, the device will output an alarm signal to hint the abnormal operation of device via setting LED indicator, relay, Trap message or e-mail.
Alarm mode	Alarm mode of MRP alarm, with options: • LED • Relay • Trap • E-mail Note: If checked, the LED indicator, relay, Trap message or email alarm mode will be turned on to trigger the alarm.

9.3.1.5 Network Load Alarm

Function Description

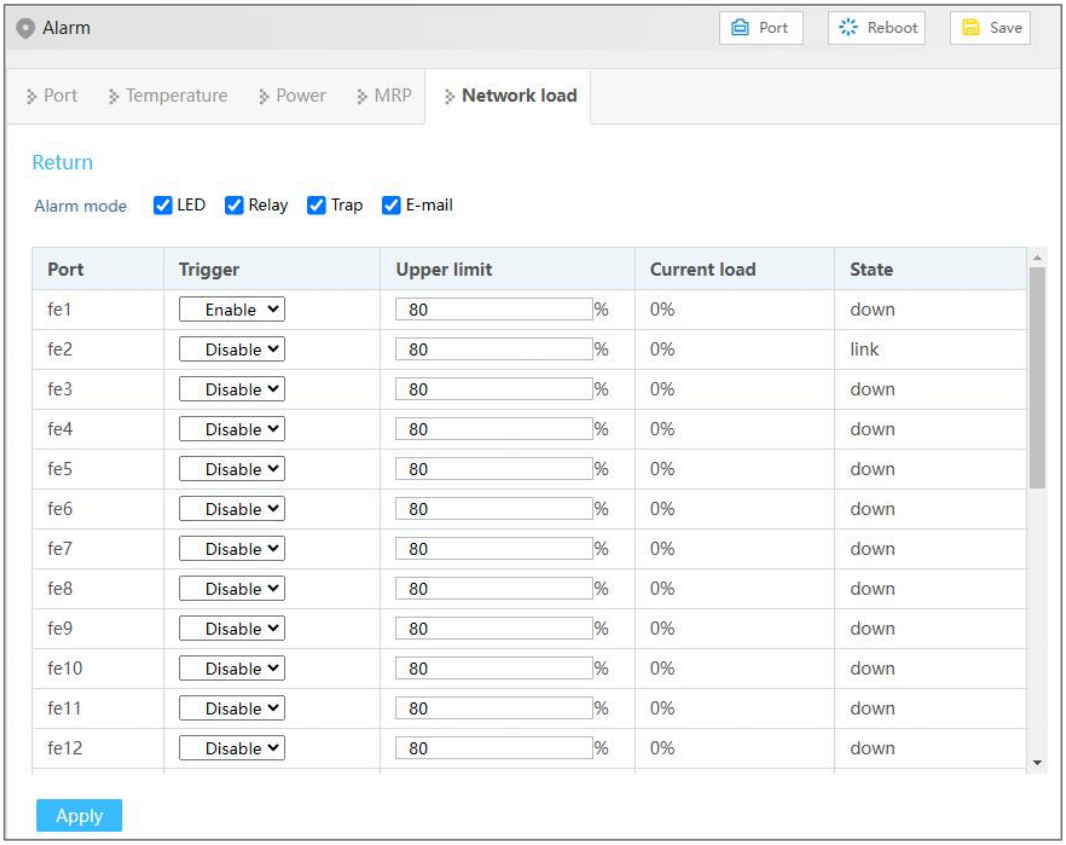
The device system provides this function, and you can set the network load alarm function.

Operation Path

Open in order: "System Maintenance > Alarm > Alarm Trigger > Network Load".

Interface Description

Network load alarm interface is as follows:



The main element configuration description of network load alarm interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Trigger	Network load alarm switch status, with options: • Enable • Disable Note: After enabling network load alarm, when the device's network load is abnormal, such as when the current network load of the device exceeds the upper limit value, the device will output an alarm signal, which will prompt the device to be abnormal by setting LED indicator, relay Trap messages, or email.
Upper limit	Set the upper limit of network load of device, ranging from 0 to 100.
Current load	If the current network load value of the device exceeds the upper limit value, an alarm will be triggered.
State	Port link status, display items as follows: • link • down
Alarm mode	Alarm mode of network load alarm, with options: • LED • Relay

Interface Element	Description
	• Trap • E-mail Note: If checked, the LED indicator, relay, Trap message or email alarm mode will be turned on to trigger the alarm.

9.3.2 Alarm Reception

Function Description

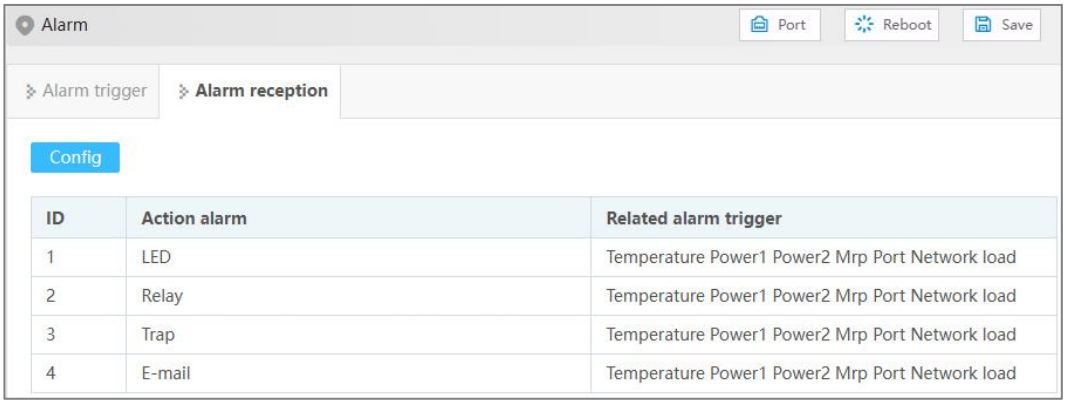
Users can check the configured LED indicator, relay, Trap or email alarm modes, so as to know the different alarm modes of the device in time.

Operation Path

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

Interface Description

Alarm reception interface is as below:



The main element configuration description of alarm reception interface:

Interface Element	Description
ID	Alarm mode entry.
Action alarm	Device alarm modes include LED, relay, Trap and mail.
Related alarm trigger	Device alarm triggers include port, temperature, power supply, MRP and network load.

9.3.2.1 Trap Setting

Function Description

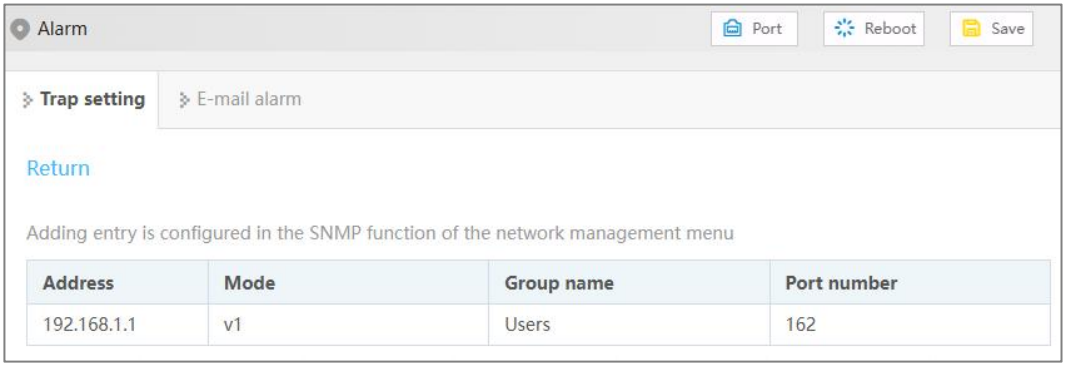
By setting the Trap message trap, the administrator can realize real-time monitoring and quick response to the device or system status, so as to find and deal with problems in time.

Operation Path

Open in order: "System Maintenance > Alarm > Alarm reception > Trap setting".

Interface Description

The Trap setting interface is as follows:



The main element configuration description of Trap setting interface:

Interface Element	Description
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
Group name	Group name.
Port number	The corresponding port name of the device Ethernet port.

9.3.2.2 E-mail Alarm

Function Description

On the "Email Alarm" page, user can configure the sender, recipient, mailbox server and other parameters. The system can inform the hot start, cold start, login failure, static IP modification and password modification of the device by email.

Operation Path

Open in order: "System Maintenance > Alarm > Alarm reception > E-mail Alarm".

Interface Description

The E-Mail alarm configuration interface is as follows:

Main elements configuration description of E-mail alarm configuration interface:

Interface Element	Description
Enabled state	Enable/disable E-mail alarm.
Mail server	Server address of used E-mail should be filled according to the account of used E-mail address. The host IP address or used host name that provides E-mail delivery service for the device.
Receiver address	Mailbox address used for receiving alarm mails.
Sender address	Mailbox address used for sending alarm mails.
Port No.	Port number of mailbox server.
TLS	TLS (Transport Layer Security) is a transport-layer security encryption protocol, which is used to provide data confidentiality and integrity in network communication. By using TLS protocol, the transmission process of mail will be encrypted to prevent sensitive information from being eavesdropped or tampered with during transmission. The operation of "TLS" is as follows: • Off: disable TLS encryption protocol; • On: enable TLS encryption protocol.
Authentication	Authentication refers to whether to verify the mailbox password. The operation of "Authentication" is as follows: • Off: disable the verification email password; • On: enable the verification email password.

Interface Element	Description
Email login address	User name for logging in to the mailbox server.
Email login password	Password of the user name for logging in to the mailbox server.

9.4 Configuration File Management

9.4.1 Current Configuration

Function Description

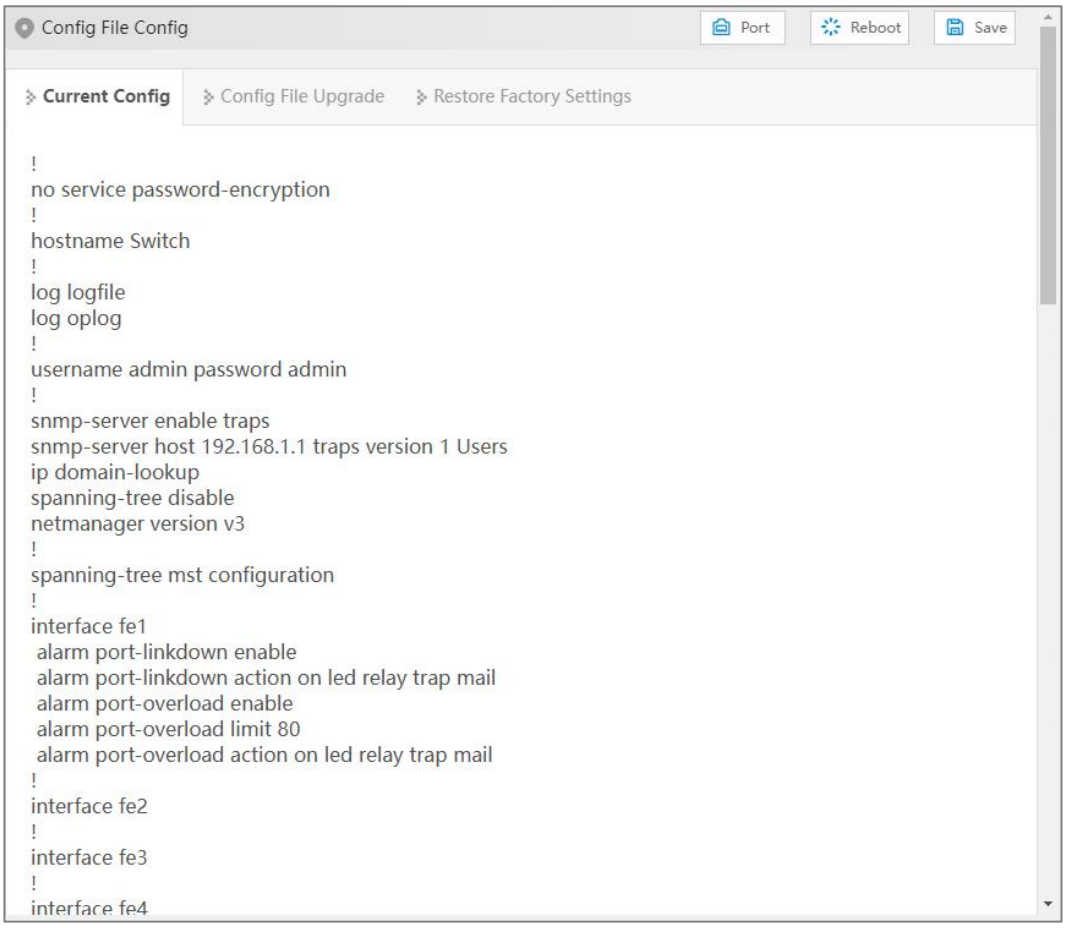
Check current configuration information.

Operation Path

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

Interface Description

The current configuration interface is as follows:



9.4.2 Config File Upgrade

Function Description

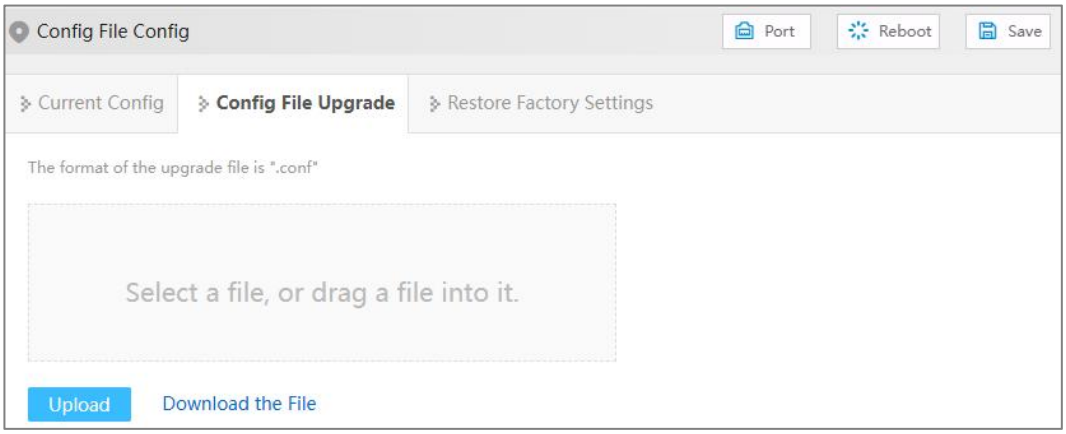
Upload and upload configuration file.

Operation Path

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

Interface Description

Config file upgrade interface is as follows:



The main element configuration description of config 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".

9.4.3 Restore Factory Settings

Function Description

Restore device to factory settings.

Operation Path

Open in order: "System management > Config File Upgrade > Restore Factory Settings".

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.

9.5 Upgrade

Function Description

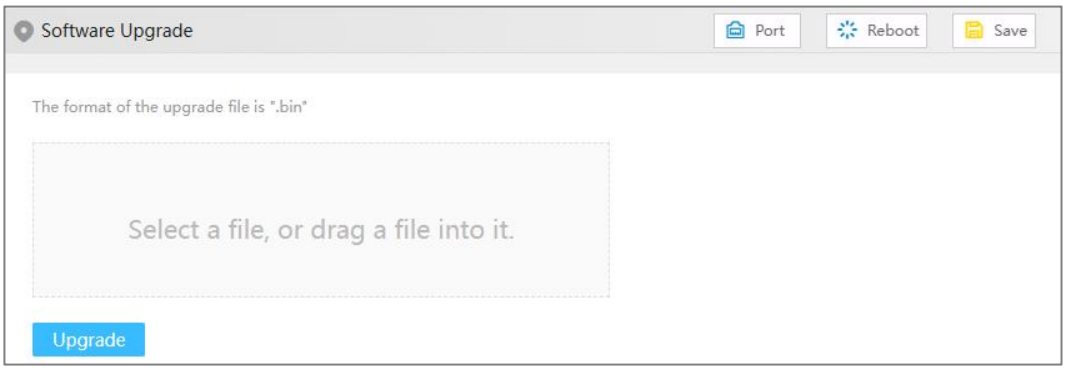
Update and upgrade the device program.

Operation Path

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

Interface Description

The software upgrade interface is as follows:



The main elements configuration description of software upgrade 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.

9.6 Log Information

9.6.1 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.

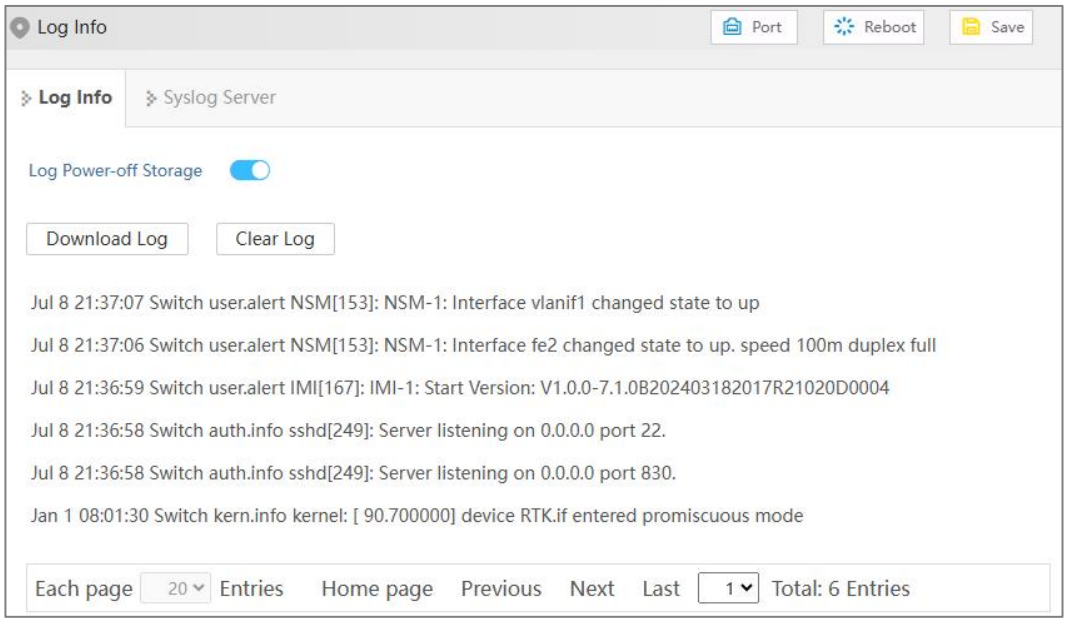
- User log: records user operations and system operation information.
- Security log: records information including account management, protocol, anti-attack and status.
- Diagnostic log: records information that assists in problem identification.

Operation Path

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

Interface Description

Log info interface is as follows:



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.

Interface Element	Description
Clear Log	Click the “Clear Log” button to clear the current log information record.

9.6.2 Syslog Server

Function Description

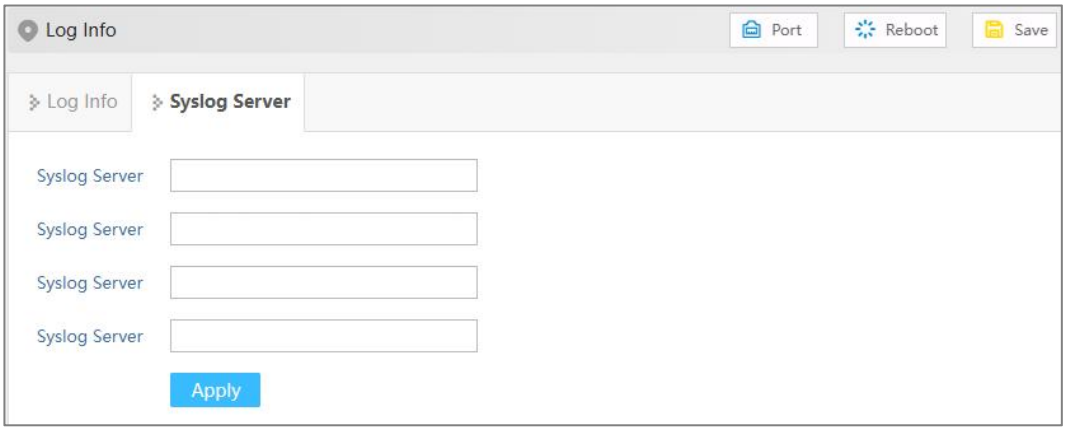
Configure the Syslog server IP address, and the system log information can be sent to the configured syslog server.

Operation Path

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

Interface Description

The Syslog server interface is 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 needs to be canceled, delete the input box and click Set.

10 FAQ

10.1 Login Problem

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

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

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

   IF you forget the login password, you can initialize the password by restoring factory settings. The specific method is to search by BlueEyes_Ⅱ software and use restore factory setting function, then the password will be initialized. The initial user name and password are "admin".

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

   Both configurations are the same, without conflict.

10.2 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.

10.3 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.