12/20-Port Series
Layer 3 Industrial Ethernet Switch for Rail Transit
User Manual

Document Version: 04

Issue Date: 09/23/2021

Preface

Layer 3 Ethernet Switch User Manual has introduced this switch:

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

Note

The reference model for the screenshot in this manual is 12 Gigabit PoE + 4 Gigabit + 2 110VDC. In addition to the differences in the supported power supply and port type, the interface functions and operation of other models in this series are similar.

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Text Format Convention

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

Symbols

Format	Description

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

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.

Revision Record

Version No.	Date	Revision note
01	2020-10-23	Product release
02	2020-12-28	Document format changes
03	2021-03-16	Data optimization
04	2021-09-23	Upgrade

Contents

Part One: Operation

1 Login to the Web Interface

1.1 WEB Browsing System Requirement

While using managed industrial Ethernet switches, the system should meet the following conditions.

Hardware and Software	System requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	256 color or above
Browser	Internet Explorer 6.0 or above
Operating system	Windows XP/7/8/10

1.2 Setting IP Address of PC

The switch default management as follows:

IP Settings	Default Value
IP Address	192.168.1.254
Subnet mask	255.255.255.0

While configuring the switch via Web:

- Before remote configuration, please make sure the route between computer and

switch is reachable.

- Before local configuration, please make sure the IP address of the computer is on the same subnet to the one of switch.

Note:
When the switch is first configured. If it is configured locally, make sure the current computer network segment is 1.

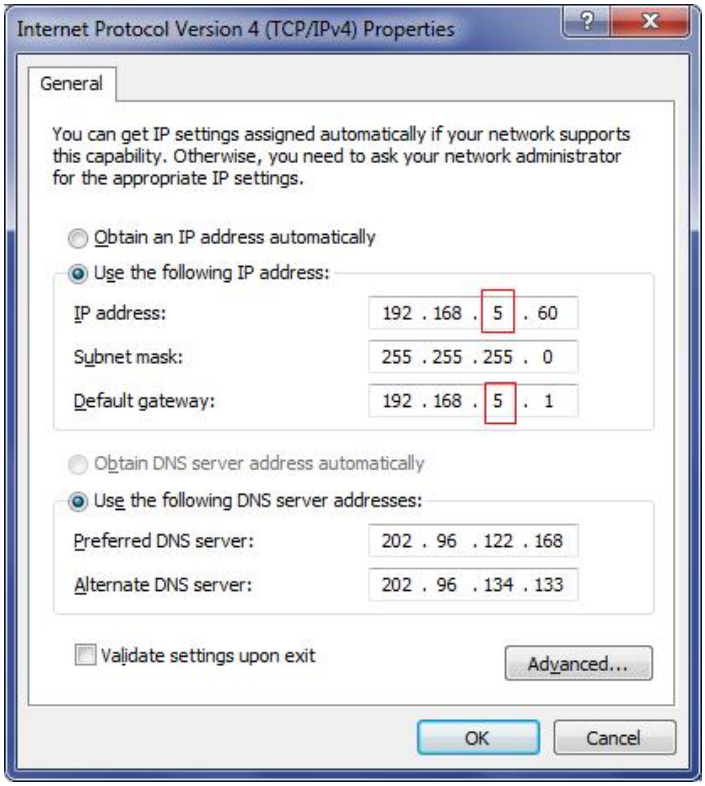
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follow:

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

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



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

Step 4 End.

1.3 Log in the Web Configuration Interface

Operation Steps

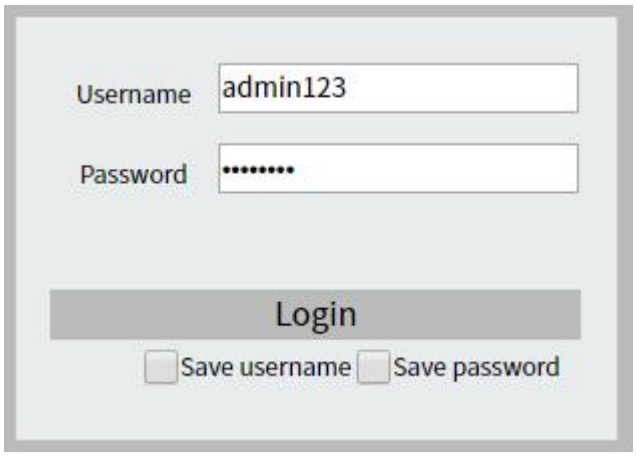
Login in the web configuration interface as follow:

Step 1 Run the computer browser.

Step 2 On the address bar of browser, enter in the IP address of the switch "http://192.168.1.254".

Step 3 Click the “Enter” key.

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



Note:

- The default username and password are “admin123”; please strictly distinguish capital and small letter while entering.
- Default user account has the administrator privileges.

Step 5 Click "Login".

Step 6 End.

After login in successfully, user can configure relative parameters and information according to demands.

Note:

After logging in to the device, you can modify the IP address of the switch for ease of use.

2 System Information

Function Description

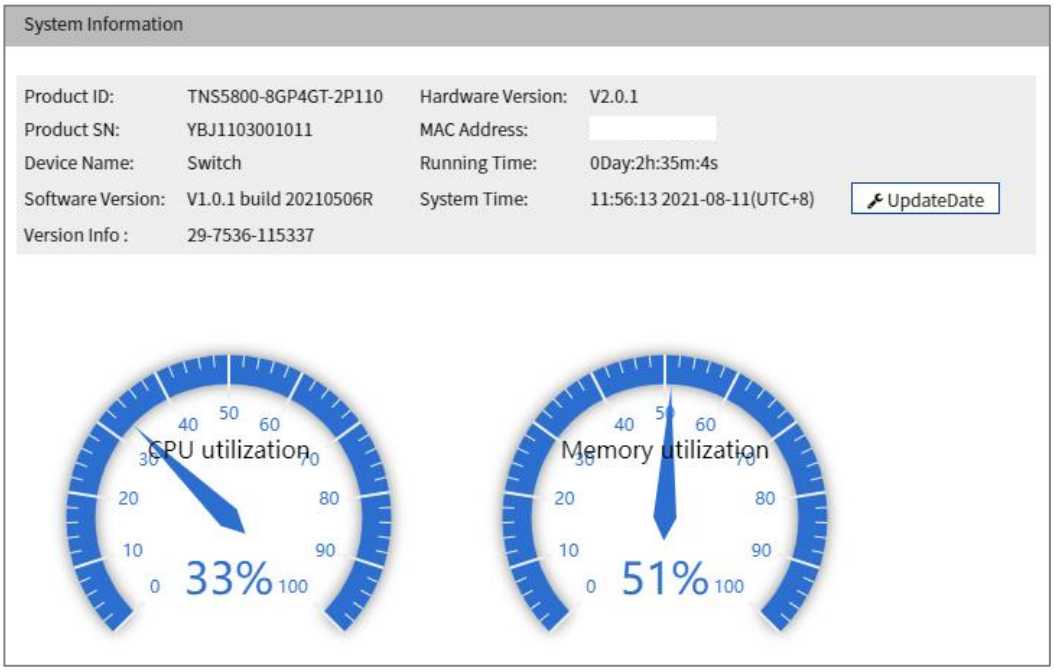
On the "System Information" page, you can view product information such as product model, hardware version, software version and MAC address.

Operation Path

Open: “System Information”.

Interface Description

System information interface as follows:



The main element configuration description of state information interface:

Interface Element	Description
Product ID.	Model of the device.
Product SN.	Product SN

Interface Element	Description
Device Name	Network identity used by the device.
Software Version	Software version information currently in use.
Version Info	The version information of current device, such as ID-Version-Time.
Hardware Version	Current hardware version information, pay attention to the hardware version limits in software version.
MAC Address;	Hardware address of device factory configuration.
Running Time	Running time of the current device.
System Time	Current system time information. Users can specify the time zone and server in “NTP Configuration”.
Update Date	Click the “Update Date” button to synchronize the local host time to the device.
CPU Utilization	CPU usage of the current device. Note: When the CPU utilization rate and memory utilization rate are lower than 90%, the system is running normally.
Memory Utilization	Memory usage of the current device. Note: When the CPU utilization rate and memory utilization rate are lower than 90%, the system is running normally.

3 System Configuration

3.1 IP Address Configuration

Function Description

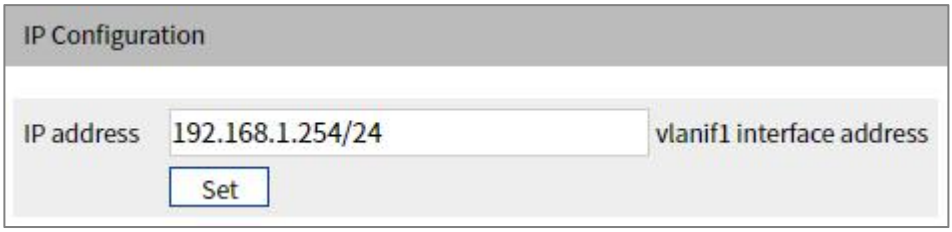
On the “IP Address Configuration” page, users can modify the vlanif1 interface address of the device. The format of IP address is: XXX.XXX.XXX.XXX/XX. For example, 192.168.1.254/24, 192.168.1.254 represents IP address, and 24 represents subnet mask 255.255.0.

Operation Path

Open in order: "System Configuration > IP Address Configuration".

Interface Description

IP address configuration interface is as follow:



The main elements configuration description of IP address configuration interface:

Interface Element	Description
IP Address	IP address and subnet mask of the device, such as 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 User Configuration

Function Description

On the page of "User Configuration", user can:

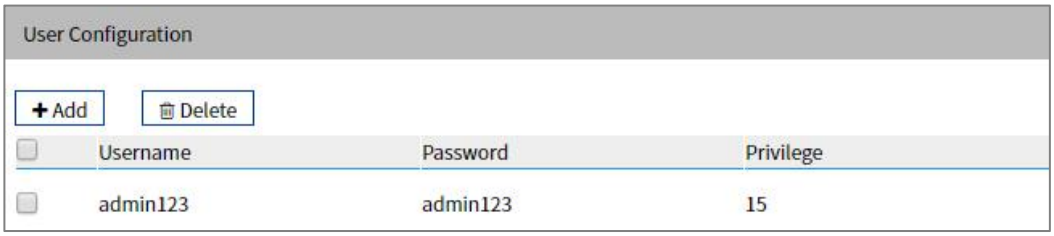
- Add users, and set their login password and user rights.
- Delete user.

Operation Path

Open in order: "System Configuration > User Configuration".

Interface Description

The User Configuration interface is as follows:



The main elements configuration description of user configuration interface:

Interface Element	Description
Username	Identification of the visitor. Note: The user name cannot be empty, and the length is less than 16 characters.
Password	Password used by the visitor. Note: Password cannot be empty and the length is less than 8 characters.
Privilege	User permissions are divided into 16 levels from 0 to 15, corresponding to 4 different types of permissions, and the corresponding relationship is as follows. • 0: visit level, user can only check system information, device IP address and log information, and cannot modify configuration. • 1: check level, user can check device configuration information without modifying it. • 2: configuration level, user can check and configure device information, but not manage devices. • 3-15: manage level, user has all privileges of the device, including downloading, uploading, rebooting, modifying device information and other other operations.

3.3 Network Diagnosis

Network diagnosis is used to detect the status of the network, including:

- Ping
- Traceroute
- Port Loopback

3.3.1 Ping

Function Description

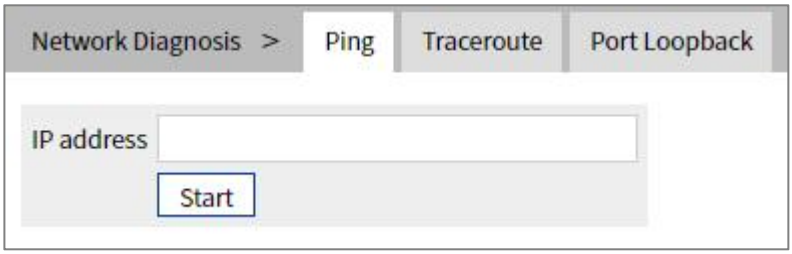
On the "Ping" page, users can use the Ping command to check whether the network is clear or the network connection speed. The Ping command uses the uniqueness of the IP addresses of the machines on the network to send a packet to the target IP address, and then asks the opposite end to return a packet with the same size to determine the connection status and delay value of the two network devices.

Operation Path

Open in order: "System Configuration > Diagnosis > Ping".

Interface Description

The interface of Ping is as follows:



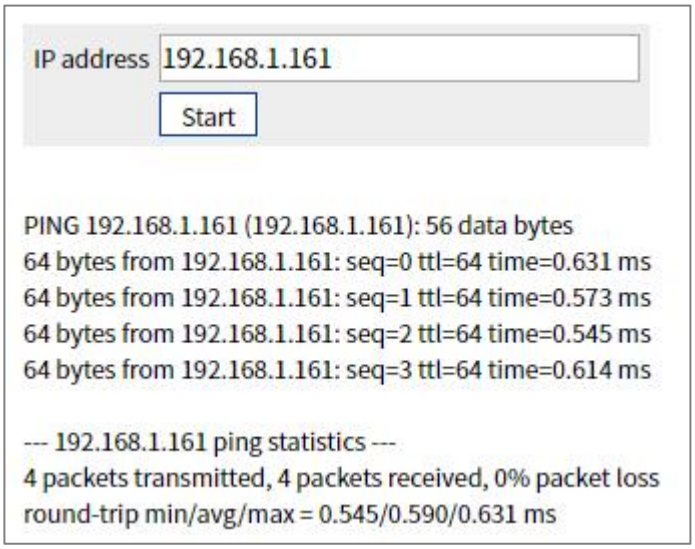
The main elements configuration description of Ping configuration interface:

Interface Element	Description
IP Address	The IP address of the detected device, that is, the destination address. The device can check the network intercommunity to other devices via the ping command.

Ping Configuration:

Step 1 Fill in the IP address that needs ping in the IP address text box;

Step 2 Click the "Start" button to check the ping results;



Step 3 End.

3.3.2 Traceroute

Function Description

On the "Traceroute" page, you can test the network situation between the switch and the target host, check whether the network connection is reachable, and help analyze where the network fails. Traceroute measures how long it takes by sending small packets to the destination device until they return. Each device on a path Traceroute returns a test result three times, up to the maximum number of hops, until the destination address returns a test result. Output results include the time of each test (ms), the name of the device (if there is no name, replace it with IP address), and IP address.

Operation Path

Open in order: "System Configuration > Diagnosis > Traceroute".

Interface Description

Traceroute interface as follows:

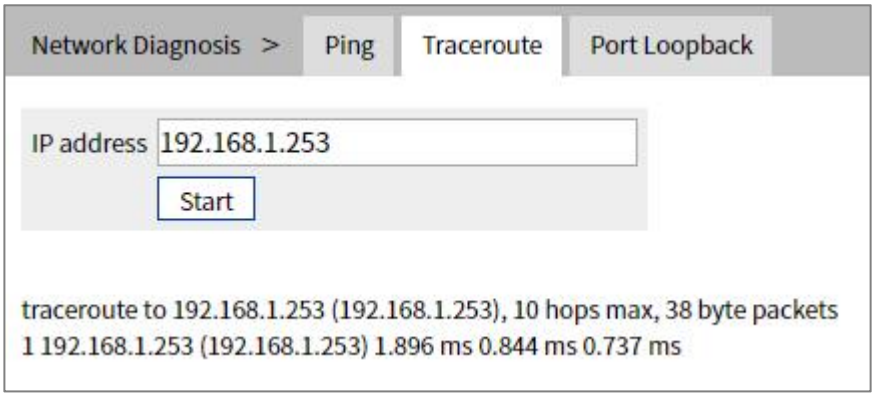
The main element configuration description of Traceroute interface:

Interface Element	Description
IP Address	IP address of the destination device, fill in the IP address of the opposite device that needs to be detected.

Traceroute Configuration:

Step 1 Fill in the destination IP address in the "IP address" text box;

Step 2 Click the "Start" button to check the results, as the picture below.



Note:

"* * *" means that no response message is received within a certain period of time after the Nth hop. The number of device node hops in the path can be up to 10 hops.

Step 3 End.

3.3.3 Port Loopback

Function Description

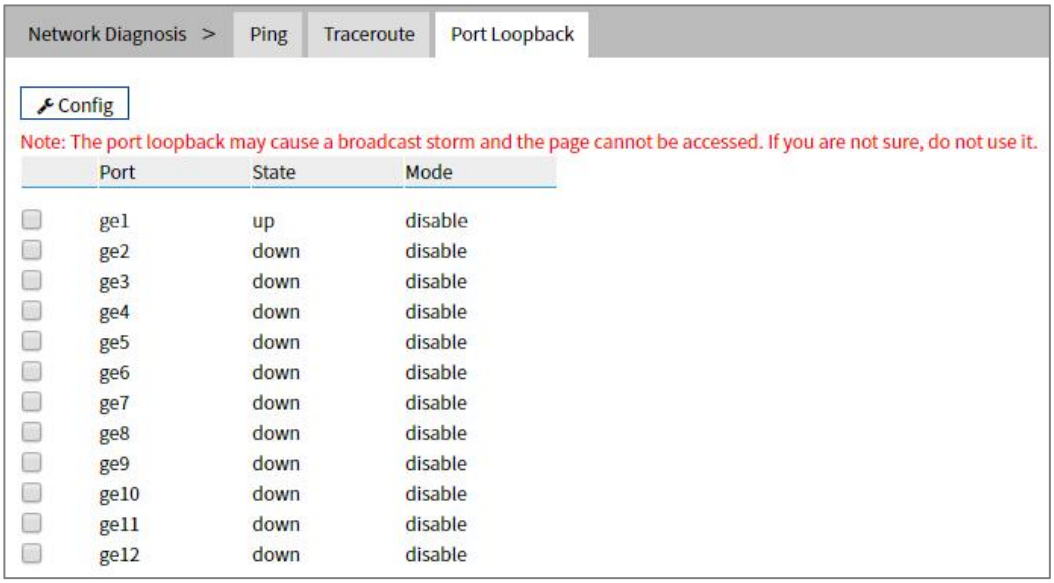
On "Port Loopback" page, user can measure the loopback situation of the switch port PHY or MAC for the convenience of troubleshooting. Port loopback is a common method for the maintenance and troubleshooting of communication port line. Connect the sending end of tested device or line to its receiving end, then the tested device can judge whether the line or port exists breakpoint by receiving the signal sent by it. The test instrument hanged on the loopback route can also test the transmission quality of the loopback route.

Operation Path

Open in order: "System Configuration > Diagnosis > Port Loopback".

Interface Description

Port loopback interface as follows:



The main element configuration description of port loopback interface:

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
Port	The corresponding port name of the device Ethernet port.
State	Display the connection status of the current port. • up: connected; • down: disconnected.
Mode	Port loopback method, options as follows: • Disable: the port loopback function of this port is disabled; • MAC: Data is looped back after transmitted to the MAC layer of Ethernet; • PHY: Data is looped back after transmitted to the physical layer of Ethernet.

3.4 Login Mode Configuration

Function Description

On the "Login Mode Configuration" page, Telnet service and SSH service of the device can be enabled or disabled. Telnet service and SSH service can both control the WEB or CLI interface access of devices. Their difference lies in:

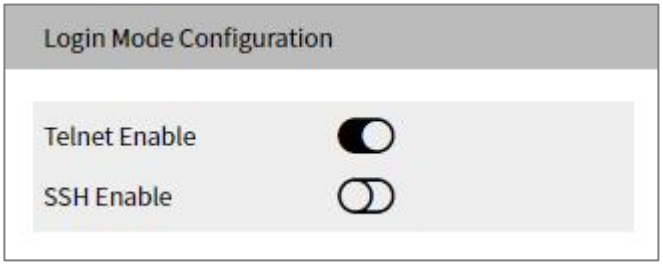
- Telnet transmission process adopts TCP protocol for plaintext transmission.
- SSH (Secure Shell) protocol provides secure remote login and encrypts transmission data, ensuring the safe transmission of data.

Operation Path

Open in order: "System Configuration > Login Mode Configuration ".

Interface Description

Login mode configuration interface as follow:



Main elements configuration description of login mode configuration interface:

Interface Element	Description
Telnet Enable	TELNET service enable switch button, which is enabled by default. It has the following status: • : represents enable; • : represents disable.
SSH Enable	SSH service enable switch button, which is disabled by default. It has the following status: • : represents enable; • : represents disable.

4 Port Configuration

4.1 Port Settings

Function Description

On the “Port Settings” page, you can implement the following functions:

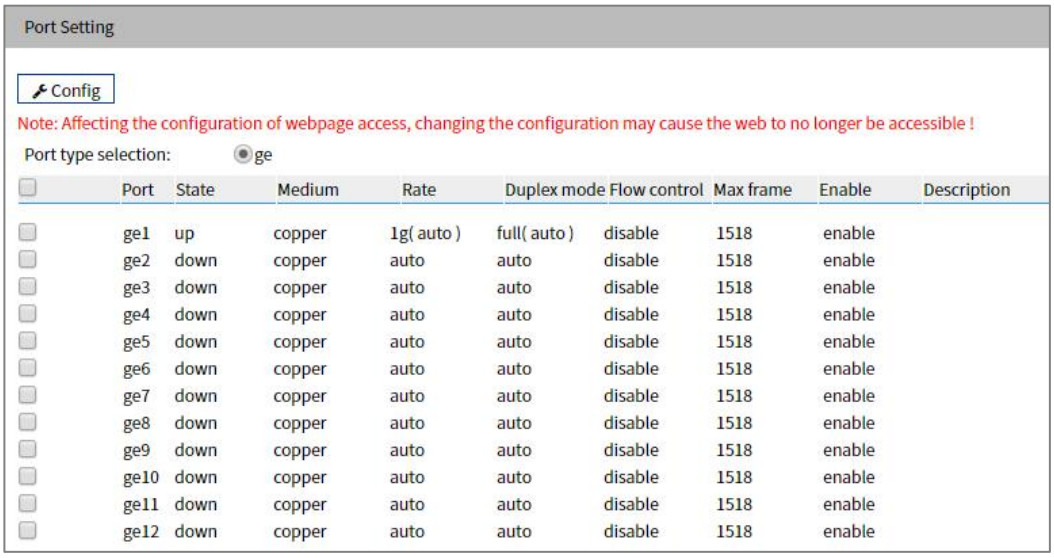
- Set parameters such as rate mode, duplex mode, flow control, maximum frame length and interface switch;
- View port status.

Operation Path

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

Interface Description

Port setting interface as follows:



Port	State	Medium	Rate	Duplex mode	Flow control	Max frame	Enable	Description
ge1	up	copper	1g(auto)	full(auto)	disable	1518	enable	
ge2	down	copper	auto	auto	disable	1518	enable	
ge3	down	copper	auto	auto	disable	1518	enable	
ge4	down	copper	auto	auto	disable	1518	enable	
ge5	down	copper	auto	auto	disable	1518	enable	
ge6	down	copper	auto	auto	disable	1518	enable	
ge7	down	copper	auto	auto	disable	1518	enable	
ge8	down	copper	auto	auto	disable	1518	enable	
ge9	down	copper	auto	auto	disable	1518	enable	
ge10	down	copper	auto	auto	disable	1518	enable	
ge11	down	copper	auto	auto	disable	1518	enable	
ge12	down	copper	auto	auto	disable	1518	enable	

Main elements configuration description of port settings interface:

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
Port type selection	Select the port type, and check the ports of the same type in batches: • 100M port (Fe); • Gigabit port (ge); • 10Gigabit port (xe); • Static aggregation port (sa); • Dynamic Aggregation Port (po). Note: The port type shall be determined by the port supported by the device, and the aggregation port shall be reflected after configuration.
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: • 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. Note: The selected maximum rate is different for different bandwidth ports.
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 • tx: enable the port to send data flow control; • rx: enable flow control of port data receiving; • both: enable flow control of both port data sending and receiving.
Max-Frame	The maximum data frame length that passes Ethernet port, the default value is 1518 and the supported input range is

Interface Element	Description (check the checkbox of the port, click “config” to configure it.)
	64~16360.
Enable	Enable or disable Ethernet port. Options are as follows: • enable • disable Notice: If the port "disable" is selected, the port will not be used.
Description	Port information description, supporting 24 valid characters.

4.2 Storm Control

Function Description

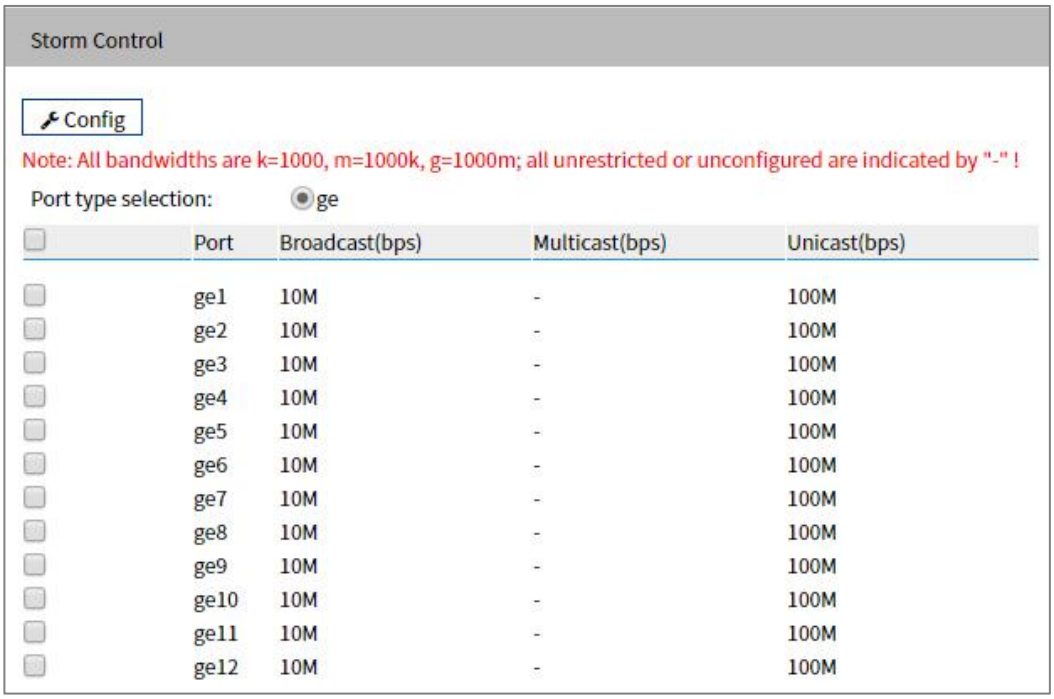
On the "Storm Control" page, user can set the maximum broadcast, multicast or unknown unicast packet flow the port allows. When the sum of each port broadcast, unknown multicast or unknown unicast flow achieves the value user sets, the system will discard the packets beyond the broadcast, unknown multicast 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 as follows:



Main elements configuration description of storm suppression interface:

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
Port type selection	Select the port type, and check the ports of the same type in batches: • 100M port (Fe); • Gigabit port (ge); • 10Gigabit port (xe); • Static aggregation port (sa); • Dynamic Aggregation Port (po). Note: The port type shall be determined by the port supported by the device, and the aggregation port shall be reflected after configuration.
Port	The corresponding port name of the device Ethernet port.
Broadcast (bps)	The port control for broadcast packet transmission speed, input value range: • 100M interface: 10-100,000Kbps or 1-100Mbps. • Gigabit interface: 100-1000000Kbps or 1-1000Mbps or 1-1Gbps. Note: Broadcast packet, namely, the data frame with the destination address of FF-FF-FF-FF-FF-FF.
Multicast (bps)	The port control for unknown multicast data packet transmission speed, input value range: • 100M interface: 10-100,000Kbps or 1-100Mbps.

Interface Element	Description (check the checkbox of the port, click “config” to configure it.)
	• Gigabit interface: 100-1000000Kbps or 1-1000Mbps or 1-1Gbps. 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)	The port control for unknown unicast data packet transmission speed, input value range: • 100M interface: 10-100,000Kbps or 1-100Mbps. • Gigabit interface: 100-1000000Kbps or 1-1000Mbps or 1-1Gbps. 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

- Supports 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.
- Different types of ports support different rates, and the port type is based on the actual port supported by the device.

4.3 Port Rate Limit

Function Description

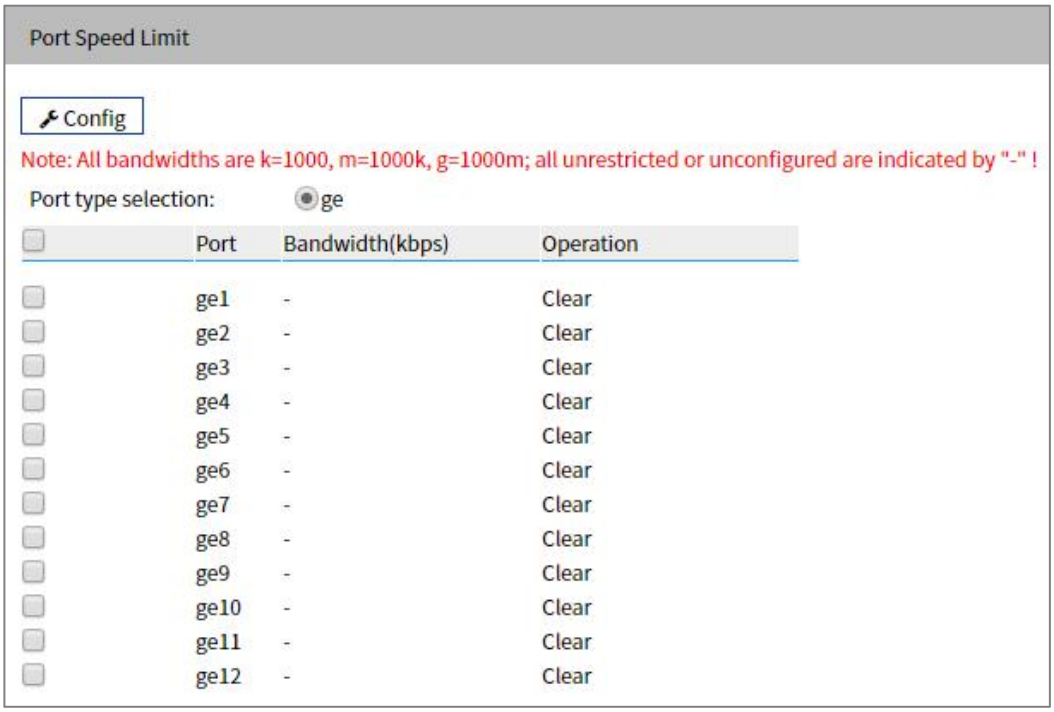
On the "Port rate-Limit" page, User can limit the communication flow of each port or cancel the port flow limit. The device provides port speed limit, including entrance and exit speed limit. User can select a fixed speed, the device will discard the packet or adopt flow control to limit the transmission speed or receiving speed of opposite device according to the flow control is enabled or not.

Operation Path

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

Interface Description

Port rate limit interface as follows:



The main element configuration description of port rate limit interface:

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
Port type selection	Select the port type, and check the ports of the same type in batches: • 100M port (Fe); • Gigabit port (ge); • 10Gigabit port (xe); • Static aggregation port (sa); • Dynamic Aggregation Port (po). Note: The port type shall be determined by the port supported by the device, and the aggregation port shall be reflected after configuration.
Port	The corresponding port name of the device Ethernet port.
Bandwidth (kbps)	The port control for all input and output data transmission speed, it has to be a multiple of 64Kbps, input value range: • 100M interface: 64-100,000Kbps or 1-100Mbps. • 10 Gigabit interface: 64-1000000Kbps or 1-1000Mbps or 1Gbps. Note: Supports unit of K/M/G when configure the rate. In WEB display, unit conversion will be conducted and the simplest values will be displayed according to the input value and the unit.
Operation	Click "delete" to delete port rate limit configuration, port rate

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
	restores to no limit by default.

Note

- Flow control should be enabled when using port speed limit, otherwise the speed between devices would not be stable.
- 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 Port Mirroring

Function Description

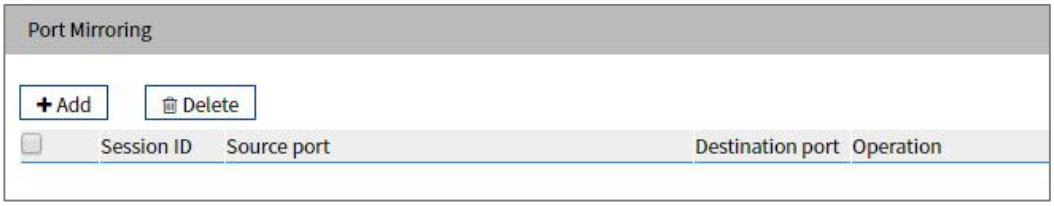
On the "Port mirroring" page, user can copy the data from the origin port to appointed port for data analysis and monitoring.

Operation Path

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

Interface Description

Port mirror interface as follows:



The main element configuration description of port mirror interface:

Interface Element	Description (check the checkbox of the port, and click "Add" button to configure it.
Session ID	Device mirror ID number, value is 1-4. Note: The device supports maximum 4-way mirror sessions.
Source port	Monitored ports, from which the device will collect input or output messages. There can be one or more mirror ports.
Destination port	Monitoring port, copying and analyzing messages from

Interface Element	Description (check the checkbox of the port, and click “Add” button to configure it.
	source port.
Operation	Click “Edit” under “Operation” to configure the direction type of source port data to be monitored in this session. Click “Delete” under “operation” to delete the corresponding port mirroring entry directly. Data direction options are as follows: • transmit:egress data, the message sent by the source port will be mirrored to the destination port; • receive: ingress data, the packet received by the source port will be mirrored to the destination port; • Both: all data, mirror the source port receiving and sending packets at the same time. Note: Directions can only be superimposed and cannot be deleted.
Add	Click "Add" to increase the port mirror entries.
Delete	Check the checkbox of port mirror entries, click “Delete” button to delete all mirror group entries

Note

- This function must be disabled during normal use, otherwise all port-based advanced management functions, such as RSTP and IGMP Snooping, cannot be used.
- Mirror function only deals with FCS normal packet; it cannot handle the wrong data frame

4.5 Link Aggregation

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. LACP priority is used to distinguish the priority of different interfaces being selected as active interfaces. The smaller the priority value, the higher the priority.

Function Description

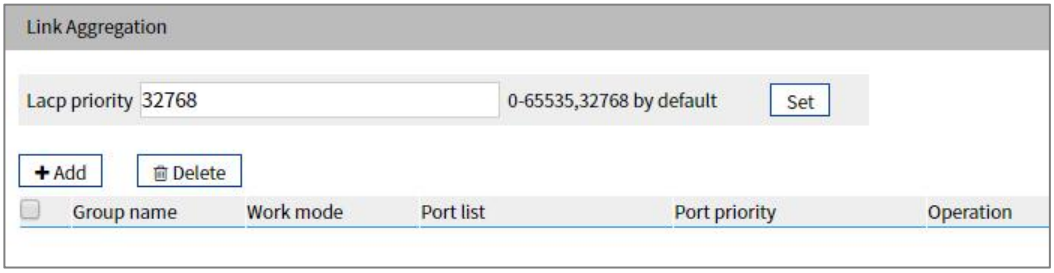
Under static aggregation mode, the member port in aggregation group disables LACP protocol, its port status is maintained manually.

Operation Path

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

Interface Description

Link Aggregation interface as below:



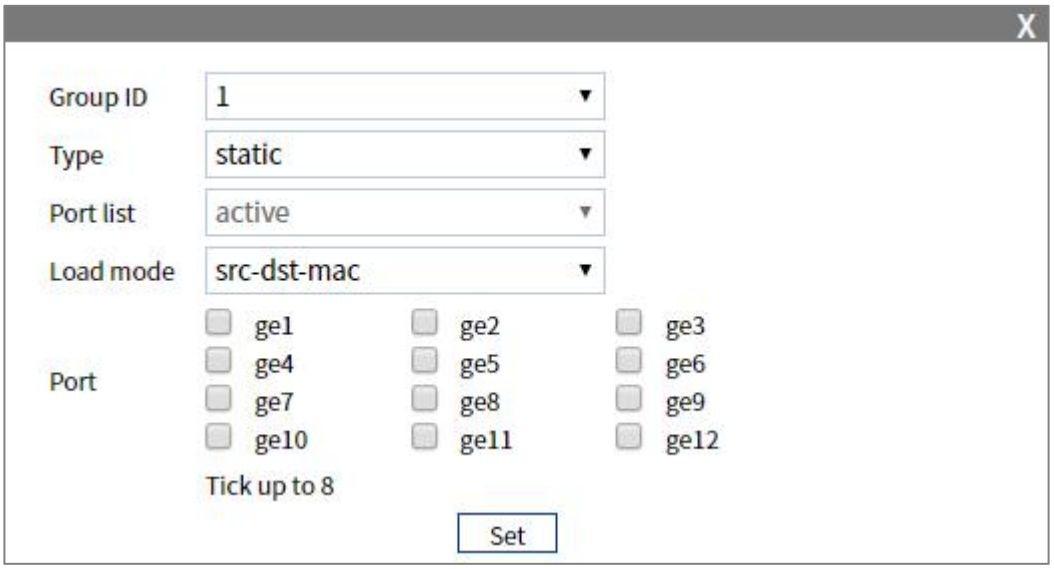
The main element configuration description of Link Aggregation interface:

Interface Element	Description
Lacp Priority	LACP priority setting, the setting range is 0-65535, and the default value is 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.
Group Name	The ID number of static aggregation link, support maximum 12 groups, each group can configure 8 ports to join aggregation.
Work Mode	There are 6 options for the configuration of trunk group load balance mode: • Dst-ip: Load balance mode based on destination IP; • Dst-mac: Load balance mode based on destination MAC; • Src-dst-ip: Load balance mode based on source and destination IP; • Src-dst-mac: Load balance mode based on source and destination MAC;

Interface Element	Description
	• Src-ip: Load balance mode based on source IP; • Src-mac: Load balance mode based on source MAC.
Port List	Port member in the link aggregation group.
Port Priority.	Port LACP priority, value range 0-65535, default value 32768. Used to distinguish the priority of different interfaces in the same aggregation link being selected as activity interfaces. Note: The lower the priority value of interface LACP is, the higher the priority is, and the interface with higher priority will be selected as the activity interface.
Operation	Click “Edit” under “Operation” to set the working mode for the specified dynamic aggregation group. Click “Delete” under “operation” to delete the corresponding link aggregation group directly.
Add	Click "Add" to add link aggregation entry.
Delete	Check the checkbox of link aggregation entry and click “Delete” button to delete link aggregation entry.

Interface Description: Add

The Link Aggregation-Add interface as follows:



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

Interface Element	Description
Group ID	The ID number of static aggregation link, support maximum 12 groups, each group can configure 8 ports to join aggregation.

Interface Element	Description
Type	Aggregation group mode: • Static: Static aggregation. • Dynamic: Dynamic aggregation.
Port List	The drop-down box of port member: • Active: the active interface, that is, the interface for forwarding data. • Passive: inactive interface, that is, interface that does not forward data. Note: When the type is Static, this function cannot be edited.
Load Mode	There are 6 options for the configuration of trunk group load balance mode: • Dst-ip: Load balance mode based on destination IP; • Dst-mac: Load balance mode based on destination MAC; • Src-dst-ip: Load balance mode based on source and destination IP; • Src-dst-mac: Load balance mode based on source and destination MAC; • Src-ip: Load balance mode based on source IP; • Src-mac: Load balance mode based on source MAC.
Port	Port member in the aggregation group.

4.6 Aggregation Protection

Function Description

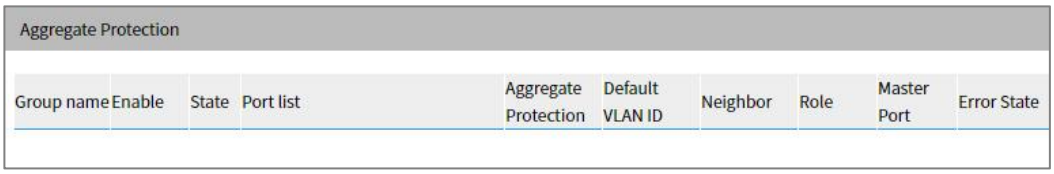
Aggregation protection provides protection against link failure when there are multiple links between two devices. In the aggregation protection mode, when a link between two nodes fails, both nodes only need to redistribute traffic to the remaining links.

Operation Path

Open in order: "Port Configuration > 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 List	Port member in the aggregation group.
Aggregation Protection	Aggregation protection switch, when aggregation protection is enabled: • Ports that can participate in data forwarding will be selected to participate in link aggregation, and the port status is active; • Ports that cannot participate in data forwarding will be unselected and the port status will be passive, so as to avoid data loss or ring formation caused by link failure.
Default VLAN ID	The VLAN where that aggregate group port reside.
Neighbor	MAC address of the opposite device of aggregation group. Note: If no device is connected to the opposite end, the MAC address is displayed as 0000.0000.0000.
Role	Elected roles in this device and the opposite device • Master: the one with a smaller MAC address is elected as master; • Slave: the one with a larger MAC address is elected as Slave;
Master Port	The second link port of the master device is the master port.
Error State	Error message prompt of aggregation protection: • Neighbor timed out; • Loop: forming a loop; • Link error (such as generating a large number of error frames).

4.7 Port Statistics

On the Port Statistics page, you can implement the following functions:

- Check the number of messages sent and received by each port and the number of message bytes; Number of discarded and erroneous messages.
- Check the classification statistics of the total number of messages sent and received by the designated port and the number of bytes of messages.

4.7.1 Port Statistics-Overview

Function Description

In the "Port Statistics - Overview" page, the following functions can be achieved:

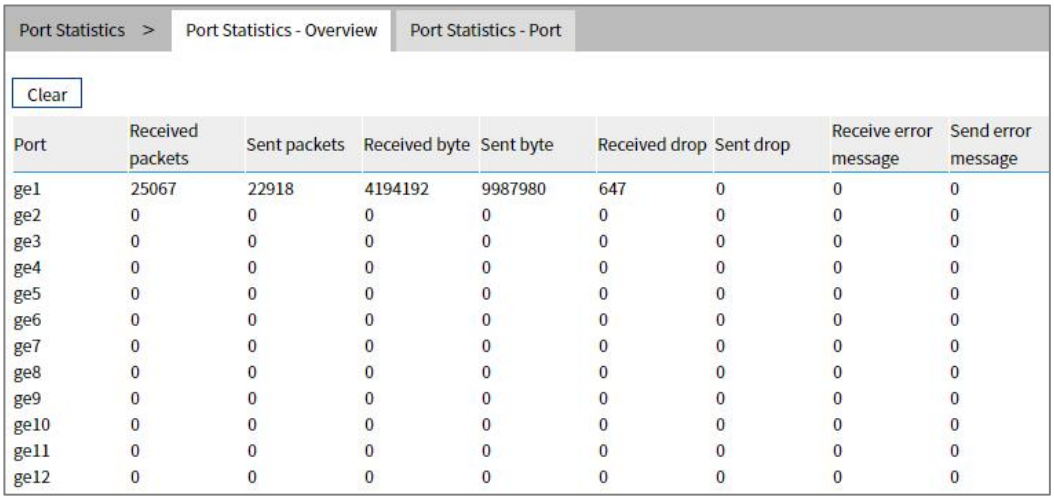
- Check the number of messages sent and received by each port and the number of message bytes; Number of discarded and erroneous messages.
- Click the “Clear” button to clear the overview information of the screen.

Operation Path

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

Interface Description

Port Statistics-Overview interface as follows:



Port	Received packets	Sent packets	Received byte	Sent byte	Received drop	Sent drop	Receive error message	Send error message
ge1	25067	22918	4194192	9987980	647	0	0	0
ge2	0	0	0	0	0	0	0	0
ge3	0	0	0	0	0	0	0	0
ge4	0	0	0	0	0	0	0	0
ge5	0	0	0	0	0	0	0	0
ge6	0	0	0	0	0	0	0	0
ge7	0	0	0	0	0	0	0	0
ge8	0	0	0	0	0	0	0	0
ge9	0	0	0	0	0	0	0	0
ge10	0	0	0	0	0	0	0	0
ge11	0	0	0	0	0	0	0	0
ge12	0	0	0	0	0	0	0	0

4.7.2 Port Statistics-Port

Function Description

On the Port Statistics-Port page, you can implement the following functions:

- Check the classification statistics of the total number of messages sent and

received by the designated port and the number of bytes of messages.

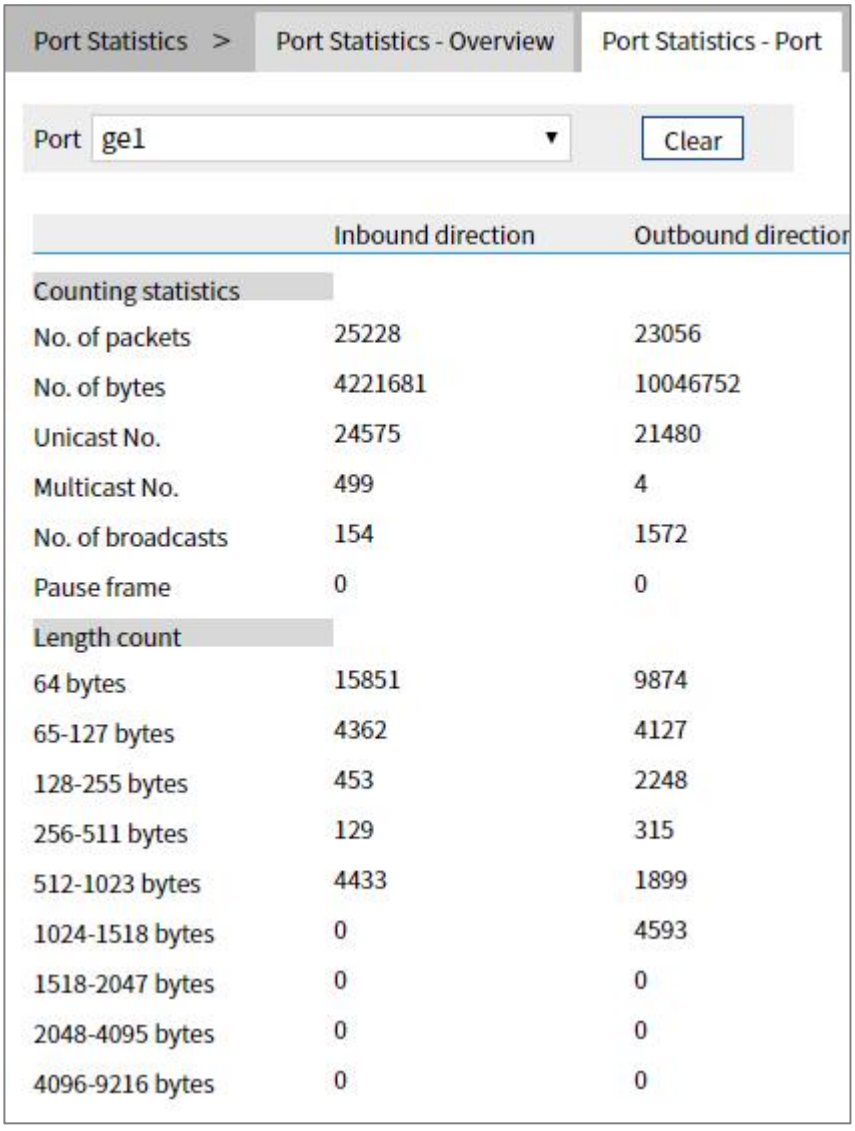
- Click the “Clear” button to clear the port information from the screen.

Operation Path

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

Interface Description

Port Statistics-Port interface as follows:



4.8 Port Isolation

Function Description

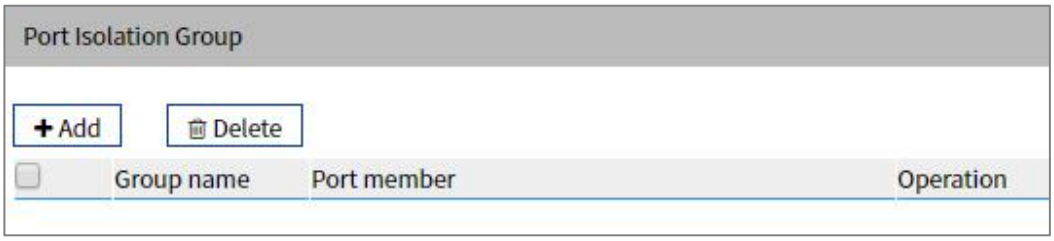
Port isolation is to isolate different interfaces of the same VLAN. Ports of the same VLAN that are not in the same isolation group cannot be accessed from each other. Port isolation has provided safer and more flexible networking scheme for users.

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
VLAN name	The Group ID of the device's port isolation group. Its value range is 1-8.
Port Member	The port of the isolation group that this device joins
Operation	Click "Delete" button to delete the corresponding port isolation group.
Add	Click "add" button to add the group name of isolation group and isolation port.
Delete	Check the radio box of port isolation group, and click "delete" button to delete port isolation group.

4.9 PoE Management

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

PoE power supply system includes:

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

4.9.1 Global Configuration

Function Description

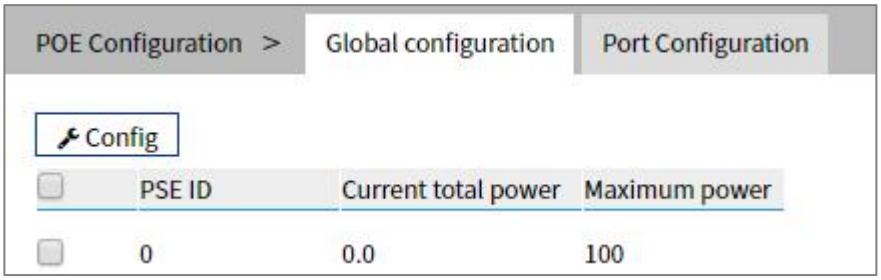
On the "Global Config" page, user can configure the maximum PoE output power of the device.

Operation Path

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

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

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

4.9.2 Port Configuration

Function Description

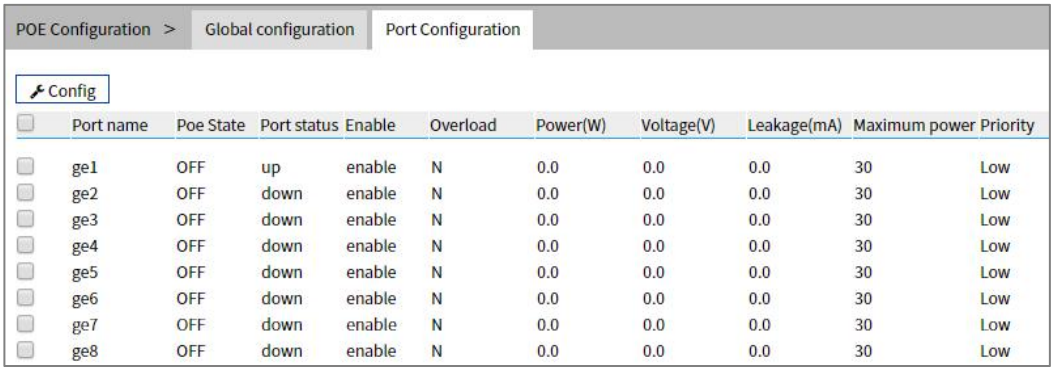
On the “Port Configuration” page, user can configure the device's PoE port enablement, maximum output power, power supply priority etc.

Operation Path

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

Interface Description

Check port configuration interface as below:



Port name	Poe State	Port status	Enable	Overload	Power(W)	Voltage(V)	Leakage(mA)	Maximum power	Priority
ge1	OFF	up	enable	N	0.0	0.0	0.0	30	Low
ge2	OFF	down	enable	N	0.0	0.0	0.0	30	Low
ge3	OFF	down	enable	N	0.0	0.0	0.0	30	Low
ge4	OFF	down	enable	N	0.0	0.0	0.0	30	Low
ge5	OFF	down	enable	N	0.0	0.0	0.0	30	Low
ge6	OFF	down	enable	N	0.0	0.0	0.0	30	Low
ge7	OFF	down	enable	N	0.0	0.0	0.0	30	Low
ge8	OFF	down	enable	N	0.0	0.0	0.0	30	Low

The main element configuration description of port configuration interface:

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
Port Name	The corresponding port name of the device PoE Ethernet port.
PoE State	The port PoE work state of current device, display state as follows: • ON: PoE port supplies power to PD; • OFF: PoE port is not powered or PD is not connected.
Port Status	Ethernet port connection status, display status as follows: • down: represent the port is disconnected; • up: represent the port is connected.
Enable	Port enable check box, check the check box to enable the PoE port; not check this check box, the PoE port would be disabled.
Overload	The overload status of current device's PoE port, display items as follows: • Y: The current PoE port output power is greater than the maximum power. • N: The current PoE port output power is smaller than or equal to the maximum power.
Power (W)	The output power display of current device's PoE port, its unit is W.
Voltage (V)	The output voltage display of current device's PoE port, its unit is V.
Leakage (mA)	The current display of current device's PoE port, its unit is mA.
Maximum Power	The maximum power value configuration of PoE output of current device, and the value range is 0-30, and the unit is W.
Priority	The priority configuration of PoE port power supply. Priority is

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

4.10 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.

4.10.1 Global Configuration

Function Description

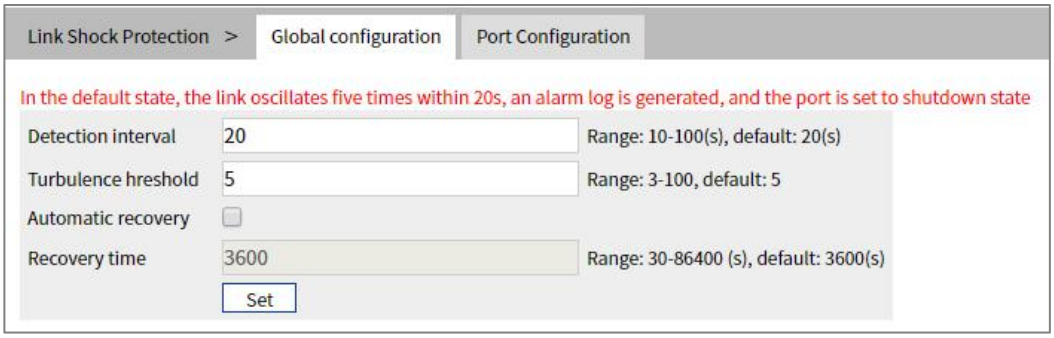
On the "Global Config" page, user can configure relative parameters of link flapping protection.

Operation Path

Open in order: "Port Configuration > Link Shock Protection > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Detection interval	The value range of link detection interval is 10-100s, and the default value is 20s.
Turbulence threshold	The threshold value of oscillation times for link detection, when the oscillation times exceed the threshold value within a certain detection time, an alarm log will be generated, and the port will be set to shutdown state. The range is from 3 to 100, default value is 5.
Automatic recovery	Automatic recovery radio box. After being checked, 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.

4.10.2 Port Configuration

Function Description

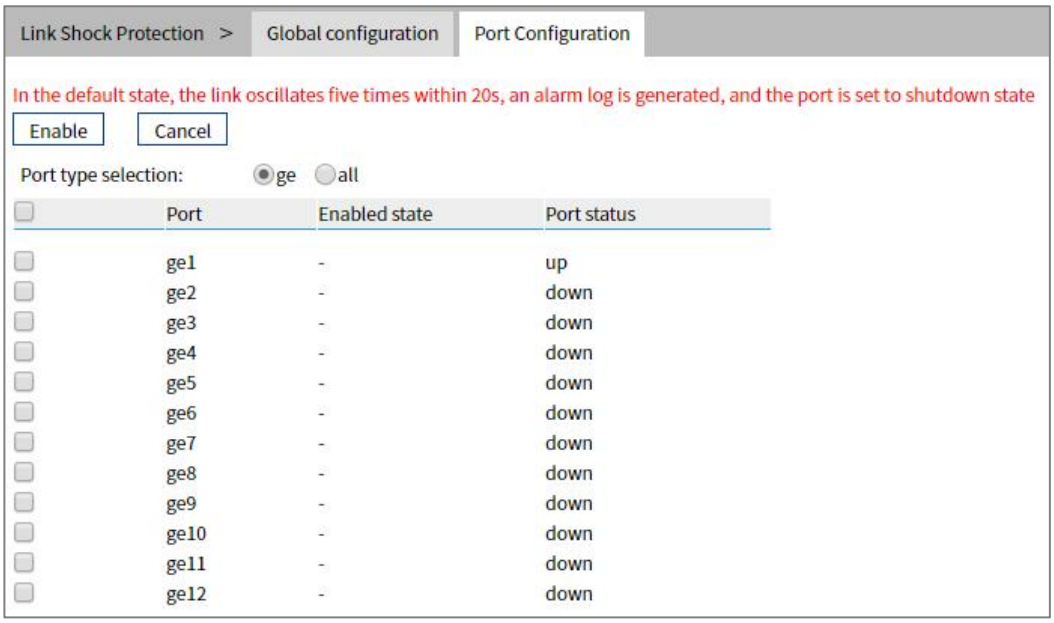
On the "Port Config" page, user can enable port link flapping protection.

Operation Path

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

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Enable	Select the port and click Enable to enable the link flapping protection function of the port.
Cancel	Select the port and click Disable to disable the link flapping protection function of the port.
Port type selection	Click to select ports of the same type in batches, and the options are fe, ge, xe and all, where all is all selected. Note: The port type shall be determined by the port supported by the device, and the aggregation port shall be reflected after configuration.
Radiobox	Tick to enable link oscillation protection for this port.
Port	The corresponding port number of this device's Ethernet port.
Enabled state	Whether the port is enabled for link flapping protection. • ON: means enabled; • - : means not enabled.
Port status	Ethernet port connection status, display status as follows: • down: port is disconnected; • up: port is connected.

5 Layer 2 Configuration

5.1 MAC Configuration

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.

5.1.1 MAC Settings

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).

Function Description

On the page of "MAC Settings", user can:

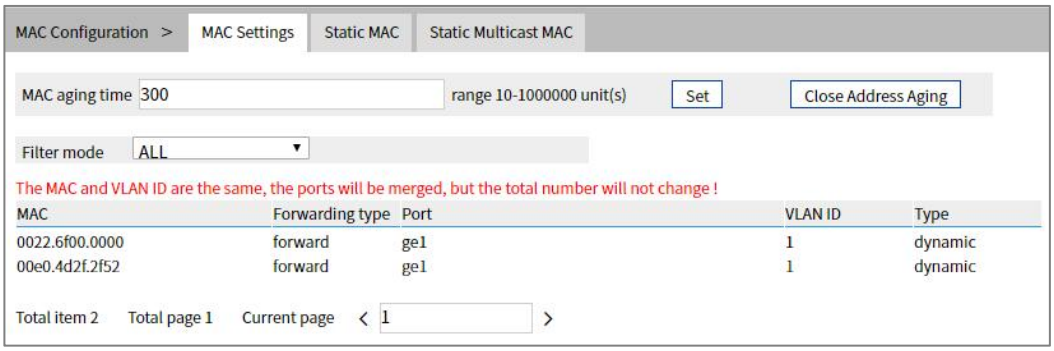
- Enable or disable the aging time of dynamic MAC addresses;
- Filters view static/dynamic unicast/multicast information.

Operation Path

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

Interface Description

MAC configuration interface as follows:



The main element configuration description of MAC setting interface:

Interface Element	Description
MAC Aging Time	MAC address aging-time, unit is second, default value is 300, and range is 10-1000000. Note: When "Close Address Aging" is selected, the MAC address will no longer age and become a static address.
Filter Mode	Drop-down list of MAC mode to filter the display of the MAC address list of the specified type. The options are as follows: • All; • Dynamic Unicast • Dynamic Multicast • Static Multicast • Static Unicast
MAC	The dynamic MAC addresses that the device have learned or the static MAC address information that user has configured.
Forwarding Type	MAC forwarding type, as shown below: • Discard • Forward
Port	Corresponding port number of the MAC address.
VLAN ID	VLAN ID number the data MAC address sending belongs to.
Type	The type of MAC address, it displays as follows: • Dynamic: dynamic MAC address; • Static: static MAC address.

5.1.2 Static MAC

Function Description

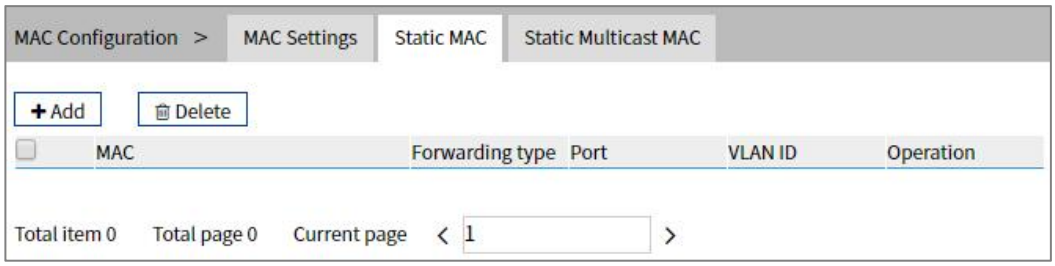
On the static MAC page, you can bind unicast MAC addresses manually. The unicast address after binding is static MAC, which will not age.

Operation Path

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

Interface Description

Static MAC interface as follows:



The main element configuration description of static MAC interface:

Interface Element	Description
MAC	Fill in the unicast MAC address that needs to bind the interface, such as 0001.0001.0001.
Forwarding Type	The forward type of MAC, discard or transmit, it displays as follows: • 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.
Operation	Click “Delete” under “operation” to delete the corresponding MAC entry directly.
Add	Click “Add” button to add static MAC entry.
Delete	Check the radio box of MAC entries and click “delete” button to delete MAC entries

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.

5.1.3 Static Multicast MAC

Function Description

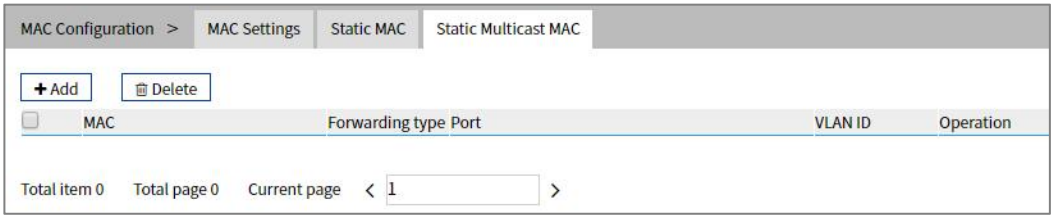
On the static multicast MAC page, you can bind multicast MAC addresses. The bound multicast address is static multicast MAC, which will not age.

Operation Path

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

Interface Description

Static multicast MAC interface as follows:



The main element configuration description of static multicast MAC interface:

Interface Element	Description
MAC	Fill in the multicast MAC address that needs to bind the interface, such as 0100.0001.0001.
Forwarding Type	The forward type of MAC, discard or transmit, it displays as follows: • 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.
Operation	Click “Delete” under “operation” to delete the corresponding MAC entry directly.
Add	Click “Add” button to add static MAC entry.

Interface Element	Description
Delete	Check the radio box of MAC entries and click “delete” button to delete MAC entries

5.2 VLAN Configuration

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.

5.2.1 VLAN Configuration

Function Description

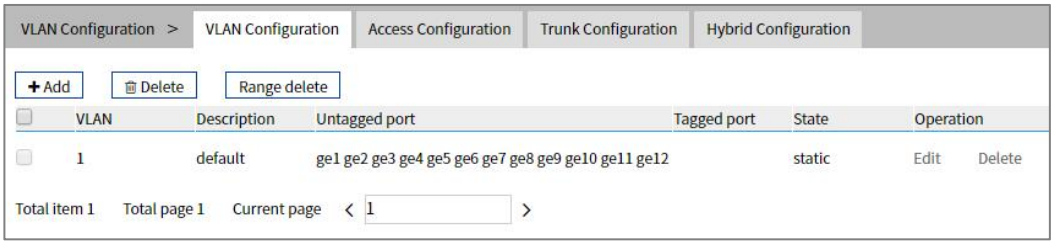
On the "VLAN-config" page, user can create VLAN and edit VLAN description.

Operation Path

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

Interface Description

VLAN configuration interface as follows:



The main element configuration description of Vlan configuration interface.

Interface Element	Description
VLAN	VLAN ID number, value range is 1-4094.
Description	VLAN ID description, maximum 16 characters.
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	Status type: • Static; • Dynamic.
Operation	Click “edit” button to add description. Click “Delete” under “operation” to delete the corresponding VLAN entry directly.
Add	Click "Add" to add VLAN entry.
Delete	Check VLAN entry and click “delete” button to delete VLAN entry.
Delete in batches	Click the "Batch Delete" button to delete range-specified VLAN entry.

5.2.2 Access Configuration

Function Description

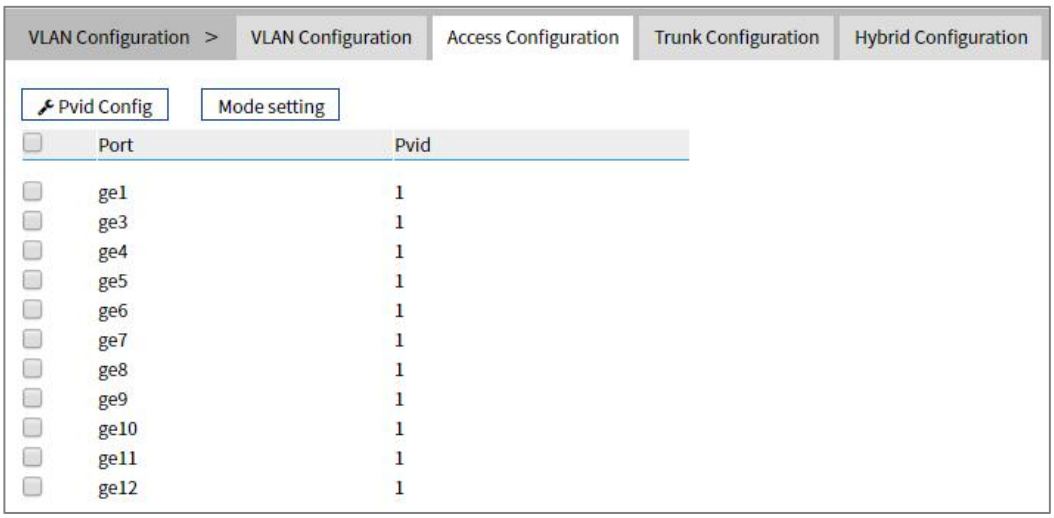
On the "Access Configuration" page, user can configure the PVID (Port Default VLAN ID) of the Access interface. User can switch Access interface to Trunk interface or Hybrid interface via “Mode Setting”.

Operation Path

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

Interface Description

Access configuration interface as follow:



The main element configuration description of Access configuration interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Pvid	Port Default VLAN ID, which is the default VLAN of the port. Default is 1, value range is 1-4094. Note: Each port has a PVID property, when the port receives Untag messages, it adds Tag mark on them according to PVID. When the port transmits data message with the same Tag mark as PVID, it would erase the Tag mark and then transmit the message. The PVID of all ports default to 1.
Pvid Configuration	Check the entries of pvid value that need to be reset, click "Pvid Config" button to reset pvid value.
Mode setting	There are three port link types that the switch supports: • Access: port only belongs to 1 VLAN (which is the default VLAN), all ports of the switch are Access mode by default and all PVID are 1. • Trunk: port can belong to multiple VLAN, Trunk port can allow the messages of multiple VLANs to pass with Tag, but only allow the messages of one VLAN to transmit without tag (strip Tag) from this kind of interface. Commonly used in the connection between network devices. • Hybrid: port can belong to multiple VLANs. Hybrid port allows messages of multiple VLANs to pass with tag, and allows the messages sent from this kind of interface to configure whether the messages of some VLANs is with tag (not strip Tag) or not (strip Tag) . It could be used in the connection between network devices, as well as user devices. Note:

Interface Element	Description
	If the port mode is set to Trunk or Hybrid, the port display will be updated to the tab corresponding to “Trunk Configuration” or “Hybrid Configuration”.

5.2.3 Trunk Configuration

Function Description

On the "Trunk Configuration" page, a list of ports in mode "Trunk" is displayed. Users can:

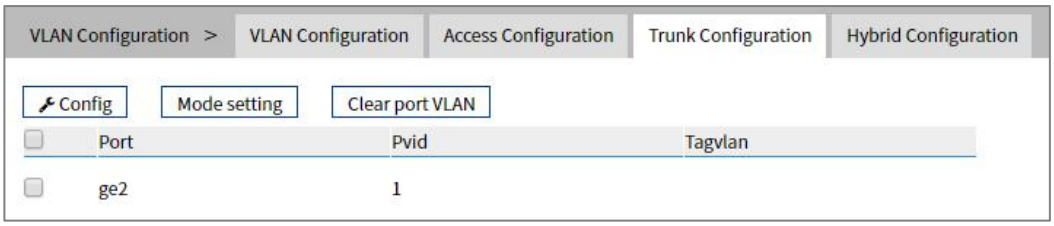
- Configure Trunk port PVID value and Tagvlan, and Tagvlan is the port tag value.
- Configure VLAN mode, switch Trunk interface to Access interface or Hybrid interface.

Operation Path

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

Interface Description

Trunk configuration interface as follows:



The main element configuration description of Trunk configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Pvid	VLAN ID number, value range is 1-4094.
Tagvlan	An tagged value, a single value or range (range denoted by a "-"), such as 9 or 10-15.
Config	Check the entries that need to be reconfigured, click configure to reset pvid value and tagvlan parameters.
Mode Setting	Click mode setting to set the mode to Access or Hybrid. Note: If the port mode is set to Access or Hybrid, the port display will be updated to the tab corresponding to “Access Configuration” or “Hybrid Configuration”.
Clear Port VLAN	Check the entries that need to be configured, click to clear

Interface Element	Description
	port VLAN, input Tagvlan value to delete Tagvlan.

5.2.4 Hybrid Configuration

Function Description

In the "Hybrid Configuration" page, the list of ports in mode "Hybrid" is displayed. The functions can be achieved as follows:

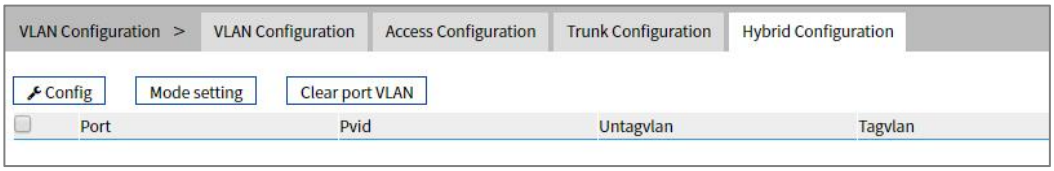
- Configure Hybrid port Pvid value, Untagvlan and Tagvlan, and Tagvlan is the port tag value.
- Configure VLAN mode, switch Hybrid interface to access interface or trunk interface.

Operation Path

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

Interface Description

Hybrid configuration interface as follow:



The main element configuration description of Hybrid configuration interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Pvid	VLAN ID number, value range is 1-4094.
Untagvlan	An untagged value, a single value or range (range denoted by a "-"), such as 9 or 10-15.
Tagvlan	An tagged value, a single value or range (range denoted by a "-"), such as 9 or 10-15.
Config	Check the entries that need to be reconfigured, click configure to reset pvid value and tagvlan parameters.
Mode setting	Click mode setting to set the mode to Access or Trunk Note: If the port mode is set to Access or Trunk, the port display will be updated to the tab corresponding to “Access Configuration” or “Hybrid Configuration”.

Process for Port Receiving Message

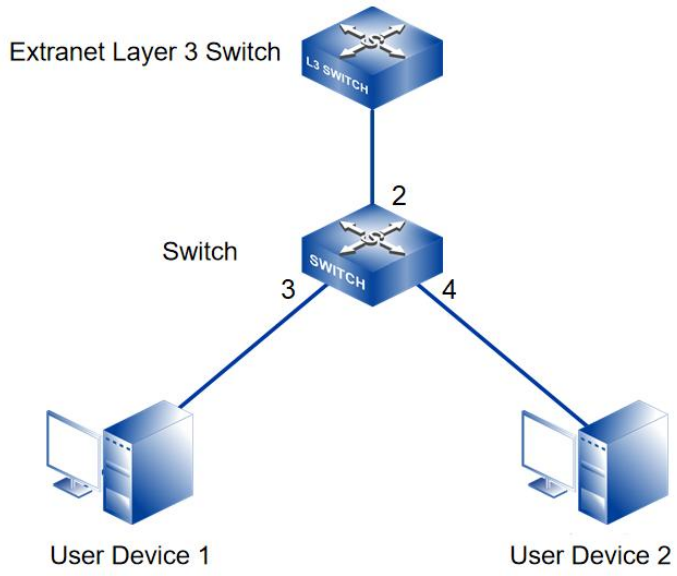
Interface type	Process for Receiving Untagged Message	Process for Receiving Tagged Message
Access	Receive this message and tag it with default VLAN ID.	• Receive the message when the VLAN ID is the same as default VLAN ID. • Discard the message when the VLAN ID is different from the default VLAN ID.
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. • 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.

Instance: typical VLAN configuration

If the switch port 2, 3, 4 meet the following requirements: port2 that connects the external network device is the upper interface, Port3/4 that connect the user device are the downward interface. Port2 communicates with Port3, Port2 communicates with Port4, and Port3 cannot communicate with Port4. As shown below. Do not consider other ports, how to set the VLAN?



Instance analysis

Port2, Port3 and Port4 are set with different port types to realize the communication between the ports. Analyse the configuration of each port as below:

- Port3

Port3 is upper interface, set Ports to Access type. Configure the PVID value of Port3 to 3.

- Port 4

Port4 is downward interface, set Ports to Access type. The PVID value of Port4 is set to 4.

- Port2

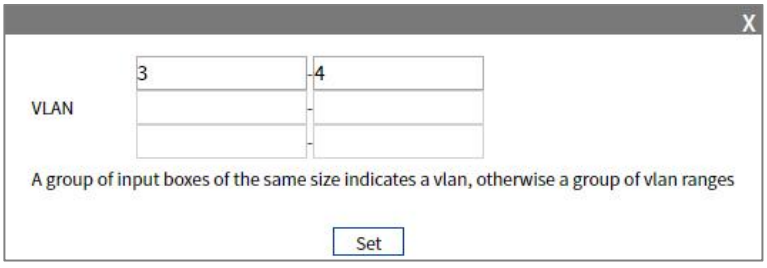
Port2 is upper interface, set Port2 to Trunk type. Add Port2 into VLAN3 and VLAN4. Port2 can communicate with Port3 and Port4.

Operation Steps

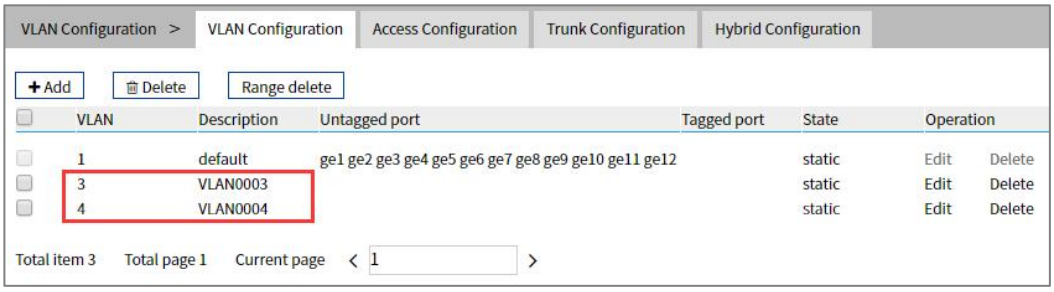
Step 1 Access "Layer 2 Configuration > VLAN Configuration > VLAN Config".

Step 2 Set VLAN value: VLAN3 and VLAN4.

1 Click “Add”, enter 3 and 4 in "VLAN " text box as shown below:



2 Click "Apply" button, the VLAN settings are as the picture below.



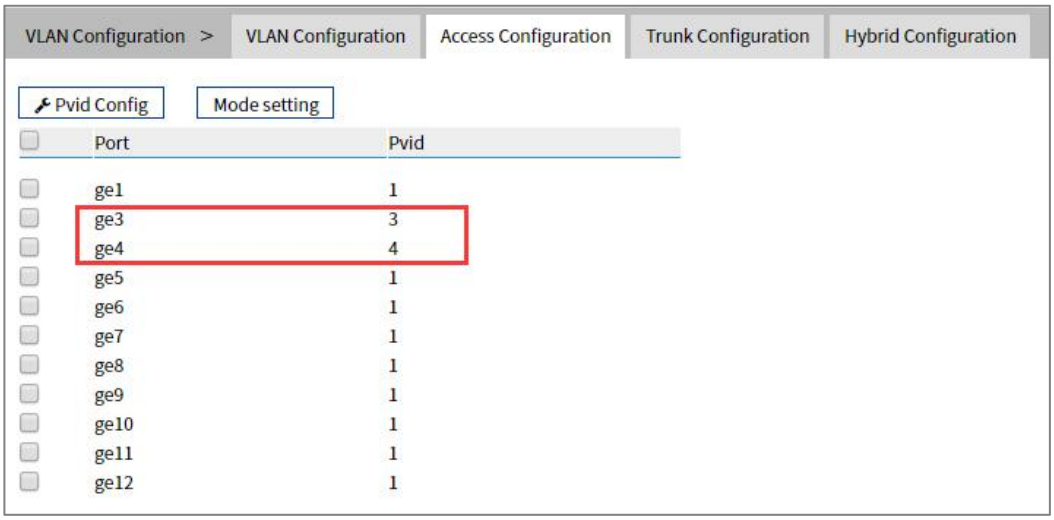
Step 3 Set the corresponding pvid of port3 and port4, as well as the type of port2, port 3 and port4.

1 Access "Layer 2 Configuration > VLAN Configuration > Access Configuration".

2 Check port ge3, click “Configure”, enter “Pvid” as “3”, and click “set”.

3 Check port ge4, click “Configure”, enter “Pvid” as “4”, and click “set”.

4 Check port ge2, click “mode setting”, select “trunk” as “type”, and click “set”.



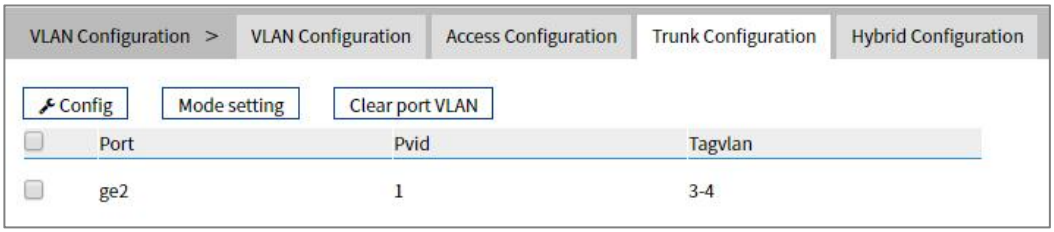
Step 4 Set the tagvlan value of port 2.

1 Access "Layer 2 Configuration > VLAN Configuration > Trunk Configuration".

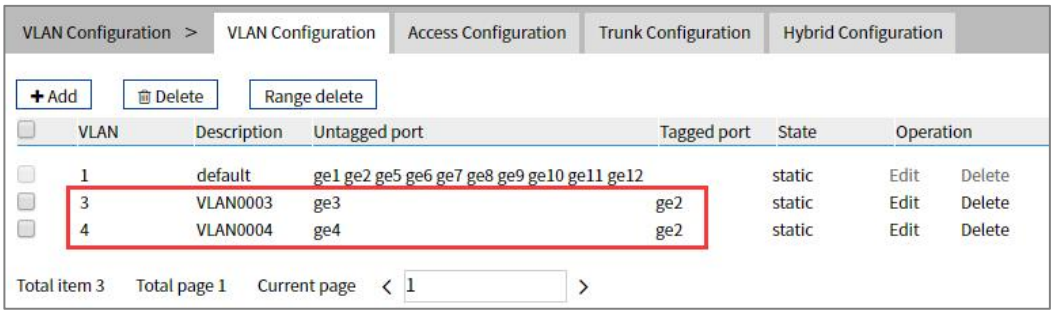
2 Check the item and click “Apply”.

3 Enter “1” in “Pvid” and “3-4” in “Tagvlan”.

4 Click "Apply" button, as the picture below.



5 Enter “layer 2 configuration > VLAN configuration”, check configuration result as show below.



Step 5 End.

5.3 Spanning-tree Configuration

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 Bridge Configuration

Function Description

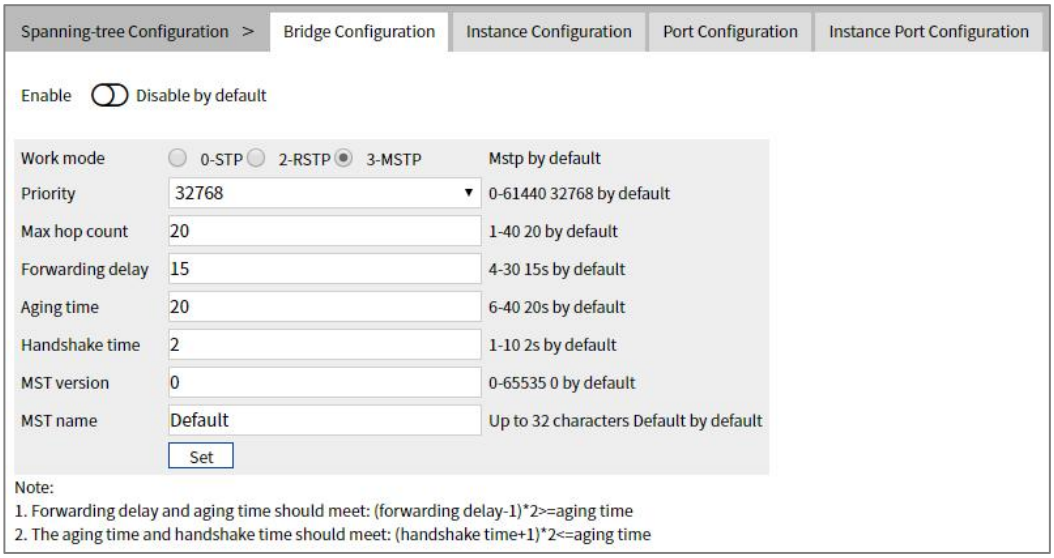
On the "Bridge Configuration" page, user can configure relative parameters of spanning-tree.

Operation Path

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

Interface Description

Bridge configuration interface as follows:



The main element configuration description of bridge configuration interface:

Interface Element	Description
Enable	Spanning-tree enable switch. Disable by default
Work mode	Defaults to MSTP, there are three modes for spanning-tree protocol choice: • 0-STP: Spanning-tree; • 2-RSTP: Rapid spanning tree; • 3-MSTP: Multiple spanning-trees.
Priority	Bridge priority level, value range is 0-61440. Note: Smaller the priority level value is, higher the priority level is.
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.
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:

Interface Element	Description
	The spanning tree protocol sends configuration information every Hello time to check whether the link is faulty.
MST version	MSTP revision level, defaults to 0, the value range is 0-65535. Note: When the MST region name, revision level, instance-to-VLAN mapping relation are the same, the two or more bridges will belong to a same MST region.
MST name	MST domain name, defaults to Default, up to 32 characters.

5.3.2 Instance Configuration

Function Description

On the "Instance Configuration" page, user can configure instance-to-VLAN mapping. Multiple Spanning Tree Regions (MST Regions) are composed of multiple devices in the switched network and the network segments between them.

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

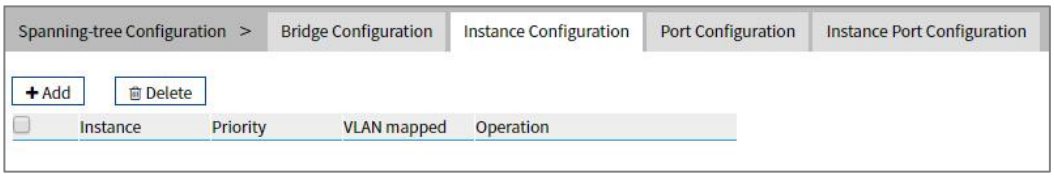
VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI.

Operation Path

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

Interface Description

Instance configuration interface as follows:



The main element configuration description of instance configuration interface:

Interface Element	Description
Instance	Instance ID number of Multiple Spanning-tree. The value range is 1-16.
Priority	Device priority level, value range is 0-61440, default to 32769, step is 4096. During adding, choose a priority based on 0-15 times the value on the 4096.

Interface Element	Description
	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 Mapped	VLAN mapping table is separated by commas, such as: 4, 5, 6, 7; "-" represents range, such as: 4-7. Note: VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI. MSTP achieves load balancing based on the VLAN mapping table.

5.3.3 Port Configuration

Function Description

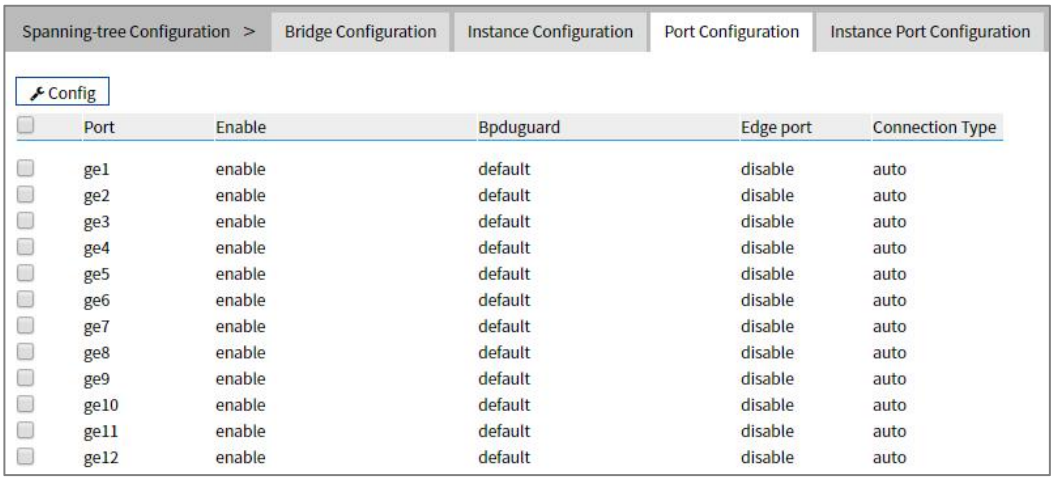
On the "Port Configuration" page, user can enable port to participate in spanning-tree and configure port type, link type and BPDU protection function.

Operation Path

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

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
Port	The corresponding port name of the device Ethernet port.
Enable	Status of participating in spanning tree enable switch.
BPDU Guard	BPDU (Bridge Protocol Data Unit) protection function status:

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
	• Enable; • Disable; • Default.
Edge port	Configure port type: • Enable; • Disable.
Connection Type	Port link type: • Auto: Automatic system detection; • Point-to-point: point-to-point link; • Shared: Non point-to-point link.

5.3.4 Instance Port Configuration

Function Description

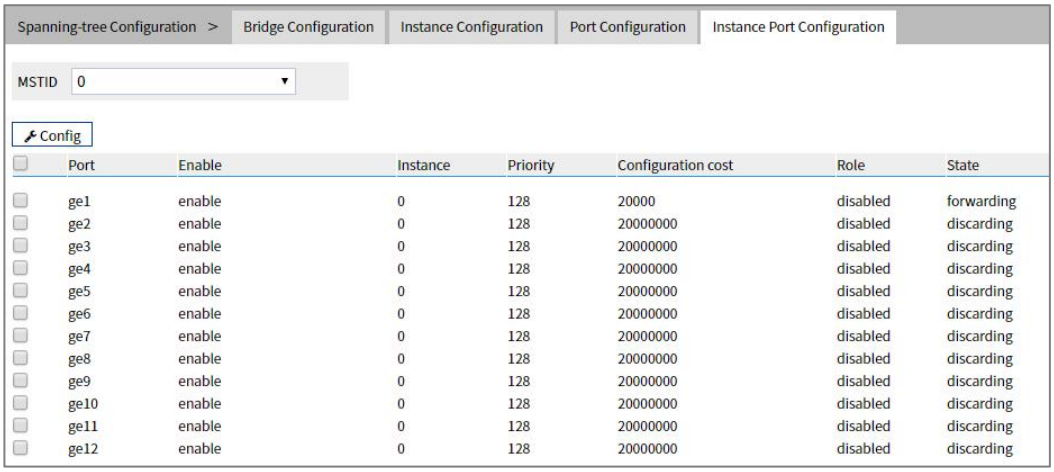
On the "Inst Port Config" page, user can configure port priority level and cost.

Operation Path

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

Interface Description

Instance port configuration interface as follows:



The main element configuration description of instance port configuration interface:

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
MSTID	Choose multiple Spanning-tree ID number.

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
Port	The corresponding port name of the device Ethernet port.
Enable	Port enable status: • Enable: participate in spanning-tree; • Disable: not participate in spanning-tree.
Instance	Instance ID number port belongs to.
Priority	Port priority level, the value range is 0-240. Note: Port priority level in bridge, port priority level is higher when the value is smaller. The higher the priority, the more likely it is to be a root port.
Configuration Cost	The path cost from network bridge to root bridge. Value range: 1-200000000.
Role	Port role. • unkn: Unknown; • root: Root port; • desg: Designated port; • altn: Alternate port; • back: Backup port; • disa: Disable port.
Status	Port status in spanning-tree: • Disable: Port close status; • Blocking: Blocked state; • Listening: Monitoring state. • Learning: Learning state; • Forwarding: Forwarding state;

5.4 ERPS Configuration

Ethernet Ring Protection Switching (ERPS) is the Ethernet Ring Network Link Layer Technology with high reliability and stability. 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.

5.4.1 Timer Configuration

Function Description

On the "Timer configuration" page, user could configure ring network.

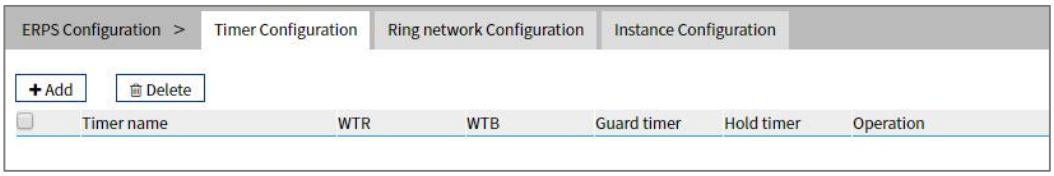
An Ethernet network topology connected in ring is called a ERPS Ring. It could be divided into main ring and subring. Each device in ERPS ring is called a node. The main node is in charge of blocking and opening ports on this node, preventing loops from forming.

Operation Path

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

Interface Description

Timer configuration interface as follows:



Main elements configuration description of timer configuration interface:

Interface Element	Description
Timer Name	The default name of timer is timer, which is up to 32 bytes.
WTR	WTR(Wait To Restore)timer, its value range is 1-12 minutes. Under revertive mode, the timer starts when the owner node in protection state receives NR packet. The owner node blocks the RPL port and unblocks the fault port after the timer expires.
WTB	WTB (Wait To Block)timer, its value range is 1-12 minutes. Under revertive mode, when the owner node is in MS (Manual Switch) or FS (Forced Switch) status, WTB timer will start if user carries out clean command on the owner node. After the timer expires, the owner node will block the RPL port and unblock temporary blocking port.
Guard Timer	Guard timer, its value range is 10-2000ms. The timer starts when the port detects the link restoration, before the timer expires, the port won't deal with R-APS (Ring Automatic Protection Switching) packet.
Hold Timer	Hold timer, its value range is 0-10ms. The timer starts when the port detects the link restoration, delay the fault report speed. When the link fails, the timer should report the fault if it

Interface Element	Description
	exists after Hold timer expires.
Add	Clicking “Add” button can add the configuration of timer.
Delete	Check the radio box of timer entry, click “delete” button to delete timer entry.

5.4.2 Ring Configuration

Function Description

On the "Ring configuration" page, user could configure ring network.

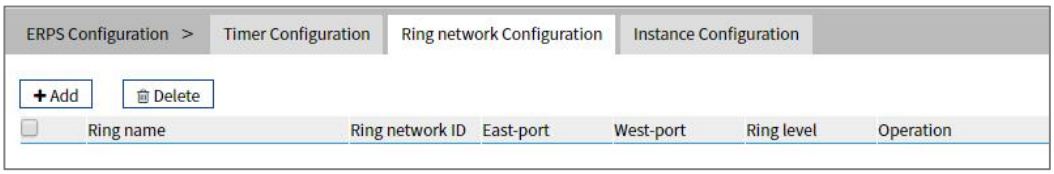
An Ethernet network topology connected in ring is called a ERPS Ring. It could be divided into main ring and subring. Each device in ERPS ring is called a node. The main node is in charge of blocking and opening ports on this node, preventing loops from forming.

Operation Path

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

Interface Description

Ring configuration interface as follows:



The main element configuration description of ring configuration interface.

Interface Element	Description
Ring Name	The default name of ring network is ring, which is up to 32 bytes.
Ring Network ID	The ID of ring network, its value range is 1-255.
East-port	Ring network 1, its value range is 1-port number.
West-port	Ring network 2, its value range is 1-port number.
Ring Level	The higher the ring network level is, the greater the value is, its value range is 1-7.
Add	Click “Add” button to add ring network configuration.
Delete	Check the radio box of ring network entry, click “delete” button to delete ring network entry.

5.4.3 Instance Configuration

Function Description

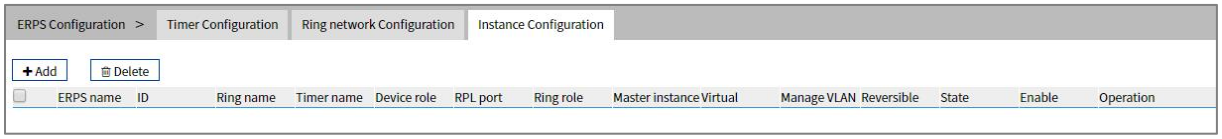
On the "Instance configuration" page, user could configure instance.

Operation Path

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

Interface Description

Instance configuration interface as follows:



The main element configuration description of instance configuration interface:

Interface Element	Description
ERPS name	The default name of ERPS is erp, which is up to 32 bytes
ID	The ID of instance, its value range is 0-16
Ring Name	The default name of ring network is the ring name that has been added in the ring network list
Timer Name	The default name of timer is the name that has been added in the timer list
Device Role	Each device in ERPS ring is called a node. The node role is decided by user configuration, they are divided into following types: • rpl-owner: owner node is responsible for blocking and unblocking the port in RPL of the node to prevent loop forming and conduct link switching. • rpl-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. • interconnection: interconnected node is the node to connect multiple rings in the multi-loop model, it belongs to the subring, and the primary ring has no interconnected node. In the link protocol packet upload mode between the two subring interconnected nodes, the subring protocol packet ends in the interconnected node, but the data packet won't end.

Interface Element	Description
	• other: normal node is the other node in addition to the above three nodes. Normal node is responsible for receiving and forwarding the protocol packet and data packet in the link.
RPL-Port	RPL (Ring Protection Link) port is the appointed ring network port for Owner node to establish RPL.
Ring Role	Options of Ring Role drop-down box: • Major-ring: main ring network • Sub-ring: subring network
Master Instance	The major instance name could be set and need to be set as ERPS instance name only when the ring role is Sub-ring
Virtual	After enable virtual channel, the subring protocol packet could transmit across the primary ring; otherwise, the subring protocol packet can only transmit in the ring. Options: • enable • disable
Manage VLAN	The VLAN channel of protocol packet, its value range is 1-4094
Reversible	Options: • Enable: In revertive mode, WTR timer starts when the owner node receives the link recovery packet after the clearing of fault. The timer will change from fault link protection status to idle status after expiring. • Disable: Irreversible mode: Owner node doesn't conduct any action after receiving the link recovery packet and keeps the port status set before.
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	Instance ring protection protocol switch: • ON: enable Ethernet ring protection protocol; • OFF: disable Ethernet ring protection protocol.
Operation	Click “operation-edit” button to modify instance configuration. Click “Delete” under “operation” to delete the corresponding instance entry directly.
Add	Click “Add” button to add instance configuration.
Delete	Check the radio box of instance configuration entry, click “delete” button to delete instance configuration.

5.5 Ring Configuration

Ring provides automatic recovery and reconnection mechanism for the disconnected Ethernet network, which has link redundancy and self-recovery ability in case of network interruption or network failure.

The core of Ring technology adopt non-master station setting. In a multi-ring network of up to 250 switches, the network self-recovery time is less than 20 milliseconds. Each port in this series of switches can be used as a ring port and connected with other switches. When an interruption occurs in the network connection, the relay for fault alarm will be activated and the Ring redundant mechanism enables the backup link to quickly recover the network communication.

Function Description

On the "Ring Configuration" page, user can enable/disable the ring network.

Operation Path

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

Interface Description

Ring configuration interface as follow:

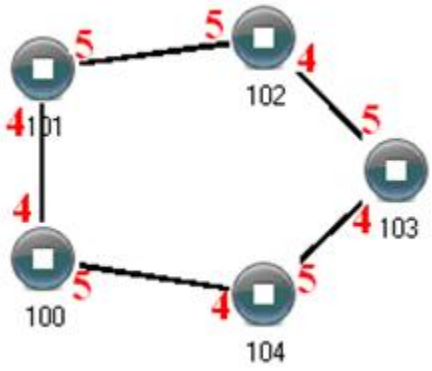
The main element configuration description of Ring configuration interface.

Interface Element	Description
Enable	Enable switch, slide to the right to enable the Ring ring network function.
Ring group	Support ring group 1-12, it can create 12 ring networks at the same time.
Network 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 a ring . Note: When the ring network type is "Couple", port 1 is the "Coupled Port". Coupling port is the port that connects different network identities.
Port1 Status	The current state of the port 2. • block; • forward.
Ring port 2	The network port 2 on the switch used to form a ring. Note: • When the ring network type is “Couple”,port 2 is the “console port”. Console port is the port in the chain where two rings intersect. • “Port 1” and “Port 2” cannot be set to the same port, and the port number it sets must be the same as it actually connects without sequential order;
Port2 Status	The current state of the port 2. • block; • forward.
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

Interface Element	Description
	different switching equipments in one network.
Hello Time	Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends information packet to adjacent device for confirming the connection is normal or not. Value range is 0-300.
Master-slave	Single loop network supports no-master station structure and one-master multi-slave structure. • When all the single-loop devices are slave stations, the single-loop structure is no-master station. • When a single ring device is a master and multiple slave station, one device can be designated as the master device and the other devices as the slave device. One end of the main device of the ring network is the backup link. When the ring network fails, the backup link is enabled from the master station to ensure the normal operation of the 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. Swipe the "  " button to the right to activate the heartbeat function.
Add	Click "Add" button to add ring network configuration.
Delete	Check the radio box of ring network configuration entry and click "delete" button to delete ring network configuration.

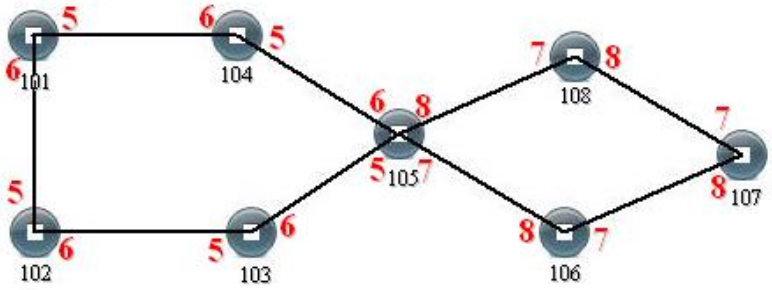
Single Ring Configuration

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



Double Ring Configuration

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



Configuration Method:

Step 1 Adopt single ring configuration method to configure port 5 and port 6 of NO. 101, 102, 103, 104, 105 switches as the ring port, and the ring group is 1;

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

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

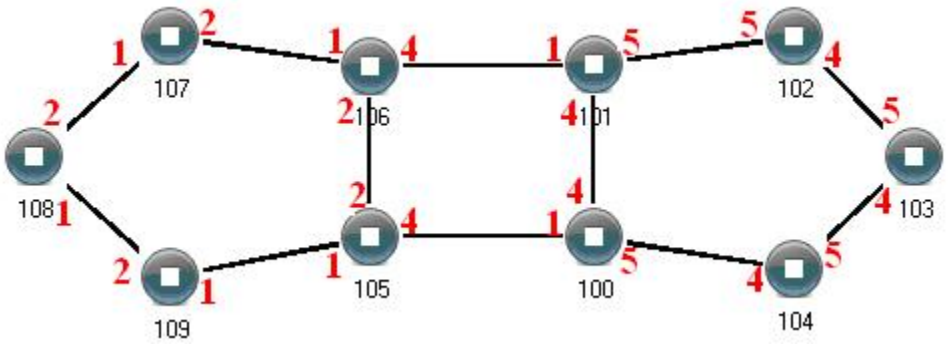
Step 4 Adopt network cable to connect the ring group 2;

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

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

Coupling Ring Configuration

Coupling ring basic framework as the picture below:



Operation method:

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

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

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

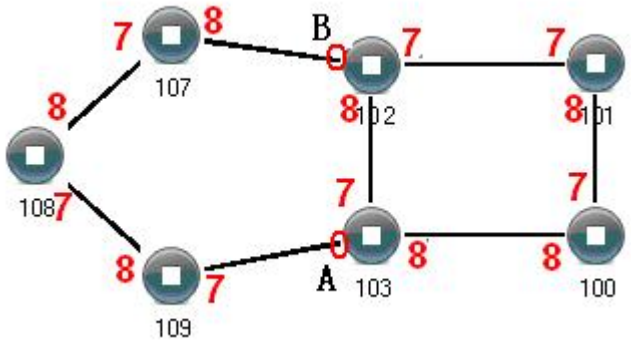
Step 4 Set the ring port of NO. 107, 108 and 109 device ring group 1 to port 1 and port 2, network identification to 1, ring type to Single; Set the ring port of NO. 102, 103 and 104 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single.

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

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

Chain Configuration

Chain basic framework as the picture below:



Operation method:

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

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

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

Note

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

5.6 IGMP-Snooping Configuration

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.

After IGMP Snooping is configured, the layer 2 multicast device can snoop and analyze the IGMP messages between the multicast user and the upstream router. Based on these information, the layer 2 multicast forwarding and publishing items can be established to control the forwarding of multicast data message. This prevents multicast data from being broadcast in the layer 2 network.

The ways of IGMP Snooping processing different messages:

1 IGMP universal group query message: IGMP universal group query message is sent periodically to all hosts and routers in the local network segment to query which multicast group members are in the network segment.

2 Specific group query message: when receiving a specific group query message for a multicast group, if there are member ports in the forwarding table entry corresponding to the group, reply the report message of the group to all router ports.

3 IGMP report message, when receiving the report message of a multicast group from a certain port, is handled in three situations:

- If the forwarding table entry corresponding to the group already exists and the dynamic member port is included in the outgoing port list, reset its aging timer;
- If the forwarding table entry corresponding to the group already exists, but the port is not included in the out port list, the port is added to the out port list as a dynamic member port and its aging timer is started;
- If there is no forwarding table entry corresponding to the group, create a forwarding table entry, add the port as a dynamic member port to the out port list, start its aging timer, and then send the report message of the group to all router ports.

4 IGMP leave message: After receiving the leave message of a multicast group from a port, send a specific group inquiry message for the group to the port. Only when the last member port in the forwarding table entry corresponding to a multicast group is deleted, the leaving message of the group will be sent to all router ports.

5.6.1 Global Configuration

Function Description

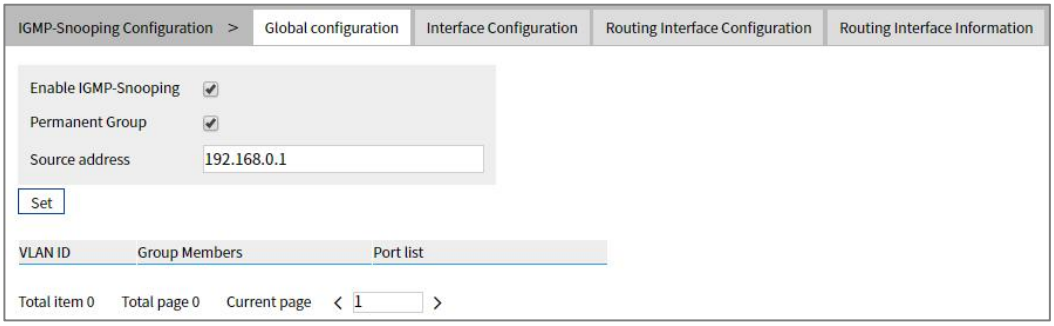
On the "Global Configuration" page, user can enable/disable IGMP monitoring and resident multicast.

Operation Path

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

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Enable IGMP-snooping	Check to enable IGMP listening configuration.
Permanent Group	Configure the multicast group as a resident multicast group, and the multicast address will not age in the forwarding table.
Source Address	When there is no IP address in the VLAN, you can specify the address from which to send an IGMP listener message.
VLAN ID	The VLAN ID number of multicast was listened.
Group Members	The multicast address that was listened.
Port list	List of multicast member group ports and routing ports listened to.

5.6.2 Interface Configuration

Function Description

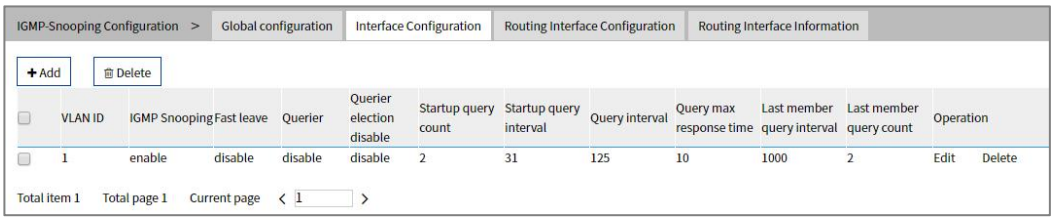
On the "Interface Configuration" page, user can configure the related parameters of interface IGMP Snooping.

Operation Path

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

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
VLAN ID	VLAN ID number, value range is 1-4094.
IGMP Snooping	IGMP Snooping 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.
Fast Leave	The enabled state of the multicast group fast leave. After fast leaving is enabled, when the switch receives the IGMP leaving group message sent by the host from a port, it directly deletes the port from the outgoing port list of the corresponding forwarding table entry. • Enable: enable the multicast fast leave function. • Disable: disable the multicast fast leave function.
Querier	Enable status of IGMP inquirer. IGMP querier can send general query messages to all hosts and other multicast routers in this network segment.
Querier Election Disable	Enable non-election status of IGMP-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.
Startup Query Count	The number of times an IGMP query is started
Startup Query Interval	The starting query interval of IGMP querier, in seconds.
Query Interval	Time interval for the inquirer to send IGMP universal group

Interface Element	Description
	inquiry message. Note: The query interval of universal group must be greater than the maximum response of universal group.
Query Max Response Time	Maximum response time of IGMP universal group query.
Last Member Query Interval	Time interval when the inquirer sends IGMP specific group inquiry message.
Last Member Query Count	Number of IGMP specific group inquiry messages sent by the inquirer.
Operation	Click the "Edit" button to edit relevant parameters; Click the “Delete” button to delete the entry.

5.6.3 Routing Port Configuration

Function Description

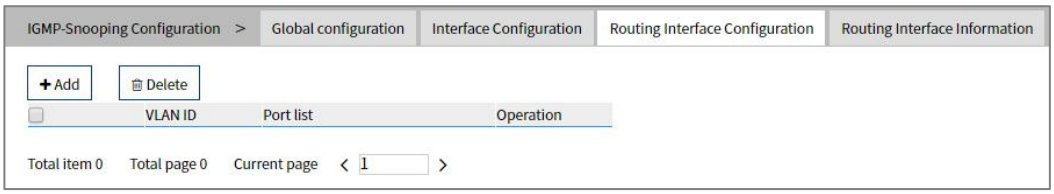
On the "Routing Port Configuration" page, user can configure the port of multicast router.

Operation Path

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

Interface Description

Routing port configuration interface is as below:



Main elements configuration description of routing port configuration interface:

Interface Element	Description
VLAN ID	VLAN ID number, value range is 1-4094.
Port List	Check the checkbox of port list, select device port as the static router port that connects router.
Operation	Click the "Delete" button to delete the entry.

5.6.4 Routing Port Information

Function Description

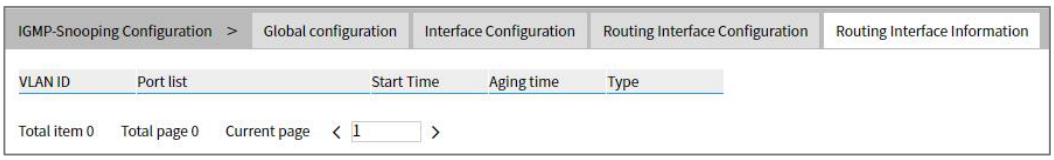
On the Routing Port Information page, you can view the startup time, aging time and port type of the routing port. The startup time starts from the port setting as the routing port.

Operation Path

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

Interface Description

Routing port information interface is as follows:



Main element description of routing port information interface:

Interface Element	Description
VLAN ID	VLAN ID number, value range is 1-4094.
Port List	List of online routing ports.
Start Time	The length of time the routing port has been started.
Aging Time	Aging time of routing port: • The dynamic routing port. Aging time calculated according to the query message interval of snooping IGMP and related items in the message. • The static routing port displays "stopped", indicating that the port will not age.
Type	Two types: • S: Static routing port • D: Dynamic routing port

5.7 Port Loopback Detection

Loop Detection technology is to periodically send a special detection message from the interface, and then detect whether the message returns to the device, and then

judge whether there is a loop between the interface, the device's down-link network or the device and the device's dual interfaces:

- If detection packets are received by the same interface, a loopback occurs on the interface or a loop occurs on the downstream network or device connected to the interface.
- If detection packets are received by another interface on the same device, a loop occurs on the device or network connected to the interface.

After discovering the loop, the device will send an alarm to the network management and record the log, and close the interface at the same time to reduce the impact of the loop on the device and even the network. After the interface is closed, do not participate in any calculation or forwarding completely to prevent network storms.

After a certain period of time, if the device does not receive the detection message sent by the interface, the loop is considered to have been eliminated and the controlled interface will automatically return to the normal state. This process is called controlled interface automatic recovery. After the loop elimination, the recovery port can also be manually configured.

5.7.1 Global Configuration

Function Description

On the “Global Configuration” page, you can use the enable switch to enable the loop detection technology and check the configuration information of port loop detection.

Note:

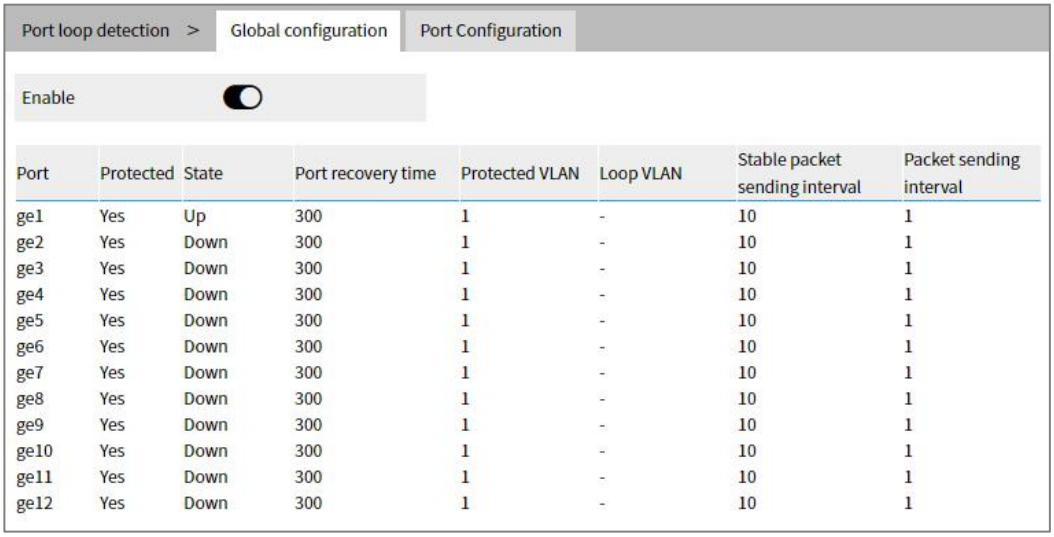
If the loop monitoring function is enabled in the VLAN, it is not recommended to configure the port mirroring function on the ports belonging to the VLAN, otherwise it may cause errors in the loop monitoring function.

Operation Path

Open in order: "Layer 2 Config > Port Loop-detect > Global Config".

Interface Description

Global configuration interface is as follows:



Port	Protected	State	Port recovery time	Protected VLAN	Loop VLAN	Stable packet sending interval	Packet sending interval
ge1	Yes	Up	300	1	-	10	1
ge2	Yes	Down	300	1	-	10	1
ge3	Yes	Down	300	1	-	10	1
ge4	Yes	Down	300	1	-	10	1
ge5	Yes	Down	300	1	-	10	1
ge6	Yes	Down	300	1	-	10	1
ge7	Yes	Down	300	1	-	10	1
ge8	Yes	Down	300	1	-	10	1
ge9	Yes	Down	300	1	-	10	1
ge10	Yes	Down	300	1	-	10	1
ge11	Yes	Down	300	1	-	10	1
ge12	Yes	Down	300	1	-	10	1

The main element configuration description of global configuration interface:

Interface Element	Description
Enable	Global enable switch of port loop detection.
Port	The corresponding port number of this device's Ethernet port.
Protected	The state of the port protected by a loop.
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
Port Recovery Time	Recovery time after detection of loop action. If the disabled port does not receive the loop monitoring message after the "port recovery time", it is judged that the loop has been eliminated and the port is reactivated.
Protected VLAN	The VLAN ID of the loop protection.
Loop VLAN	The VLAN ID of the currently generated loop.
Stable Packet Sending Interval	After the ports are started stably, that is, after three "packet-sending intervals", a loop monitoring message is sent at a "stable packet-sending interval" to determine whether there is a loop at each port and whether the loop on the port has been eliminated.
Packet Sending Interval	When the port is just started, the default time interval for sending loop monitoring messages is 1s, a total of 3 times, and then the packet issuing interval returns to the normal

Interface Element	Description
	packet issuing interval.

5.7.2 Port Configuration

Function Description

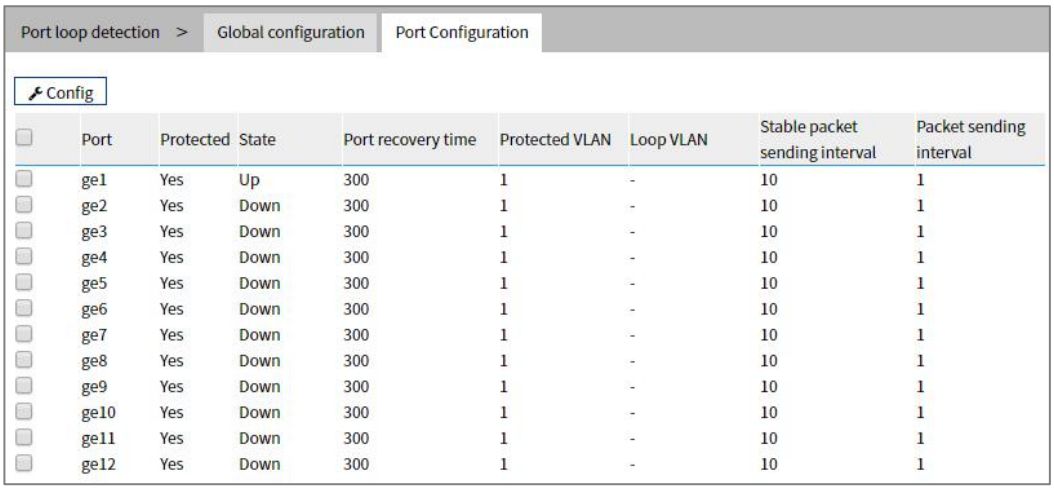
On the "Port config" page, user can implement relevant configuration of port loop detection.

Operation Path

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

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port number of this device's Ethernet port.
Protected	The state of the port protected by a loop.
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
Port Recovery Time	The resume time after the action of detecting loop, value range: 300-600, its unit is second.

Interface Element	Description
Protected VLAN	The VLAN ID of loop protection. It is None by default. 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	After the ports are started stably, that is, after three "packet-sending intervals", a loop monitoring message is sent at a "stable packet-sending interval" to determine whether there is a loop at each port and whether the loop on the port has been eliminated. Stable packet issuing interval time, the value range is 10-300, and the unit is seconds.
Packet Sending Interval	When the port is just started, the default time interval for sending loop monitoring messages is 1s, a total of 3 times, and then the packet issuing interval returns to the normal packet issuing interval.

6 Layer 3 Configuration

6.1 Interface Configuration

Interface configuration mainly refers to setting the device's interface IPv4 address. The interface configuration only supports manual configuration, doesn't support automatic acquisition (DHCP). User chooses the interface, and fill in IPv4 address. IPv6 address setting can be achieved via command line.

IPV4 address:

The IP address is a 32-bit address assigned to the device connected to Internet. IP address is composed of two fields: Network number field (net-id) and host number field (host-id). IP addresses are allotted by the Network Information Center (NIC) of U.S. Defense Data Network. IP addresses are divided into five categories for the convenience of IP address management. As the table below:

Network Type	Address Range	Usable IP Network Range
A	0.0.0.0～126.255.255.255	1.0.0.0～126.0.0.0
B	128.0.0.0～191.255.255.255	128.0.0.0～191.254.0.0
C	192.0.0.0～223.255.255.255	192.0.0.0～223.255.254.0
D	224.0.0.0～239.255.255.255	None
E	240.0.0.0～246.255.255.255	None
Other addresses	255.255.255.255	255.255.255.255

Thereinto, category A, B, C address are unicast address; category D address is multicast address; category E address is reserved address for the future special purpose. Now, most of the using IP addresses belong to category A, B, C address.

IP address adopts dotted decimal notation recording mode. Each IP address is expressed as four decimal integers separated by radix point, each integer is corresponding to a byte, such as 10.110.50.101.

IPv6 address:

IPv6 (Internet Protocol Version 6) is the second standard protocol of network layer protocol, also called IPng (IP Next Generation); it's a set of standards designed by IETF (Internet Engineering Task Force) and is the upgrade version of IPv4. The most significant difference between IPv4 and IPv6: IP address length is increased from 32 bits to 128 bits.

IPv6 address is expressed as a series of 16 bits hexadecimal number separated by colon. Each IPv6 address is divided into eight groups, 16 bits in each group is expressed by four hexadecimal numbers, two groups are separated by colon, such as: 2001:0000:130F:0000:0000:09C0:876A:130B. In order to simplify the expression of IPv6 address, "0" in IPv6 address can be handled in the following way: The leading "0" in each group can be omitted, that is above address can be written as 2001:0:130F:0:0:9C0:876A:130B. If the address contains two or more successive 0 group, it can be replaced by double colon "::", that is, above address can be written as 2001:0:130F::9C0:876A:130B.

 Notice

One IPv6 address can only use the double colon "::" once, otherwise, when the device changes "::" to 0 for restoring 128 bits address, 0 number represented by "::" won't be able to confirm.

IPv6 address is composed of two parts: address prefix and interface identification. Thereinto, address prefix is the network number field part in IPv4 address, interface identification is the host number part in IPv4 address.

The expression method of address prefix is: IPv6 address/prefix length. Thereinto, IPv6 address is any form listed before, and prefix length is a decimal number, it represents how many bits in the leftmost of IPv6 address is the address prefix.

6.1.1 Layer 3 Interface

The IP of layer 3 switch could be used as the device management address or gateway. The IP of layer 3 switch needs to be configured at layer 3 interface.

Function Description

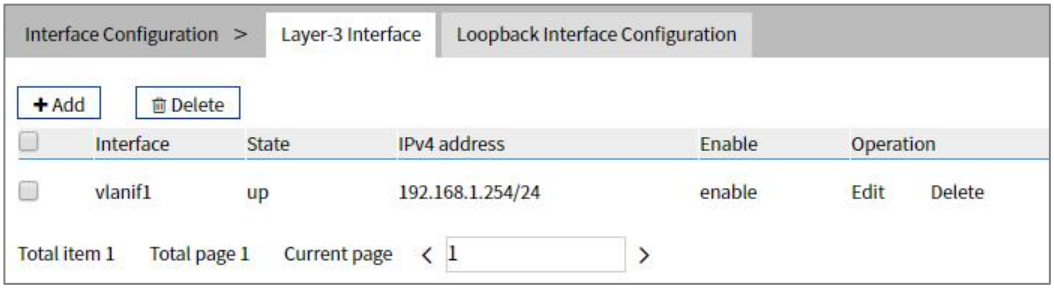
On the "Interface Configuration" page, user can configure the Layer 3 interface IP address.

Operation Path

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

Interface Description

L3 interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	Layer 3 interface names, such as, vlanif1, value range: vlanif1-vlanif4094.
State	Interface state information, options: • Up; • Down.
IPv4 address	IPv4 address and subnet mask, such as 192.168.1.1/24.
Enable	Interface switch options as follows: • enable; • disable.
Operation	Click “Edit” button to set interface and IPv4 address, enable/disable interface switch. Click “Delete” under “operation” to delete the corresponding interface configuration directly.
Add	Click “edit” button to add the configuration of layer 3 interface.
Delete	Check the radio box of layer 3 interface entry, and click “delete” button to delete layer 3 interface entry.

6.1.2 Loopback Interface

Loopback interface is virtual interface, and most of the platforms support using it to simulate real interface. This interface is in virtual forever UP state, which is more stable than any other physical interface. As long as the router starts, the loopback interface would be in an active state. If there are multiple routes that arrive at this loopback address, they would not be unreachable when one of the interface of the device is down. It only be invalid when the router no longer has effect.

Function Description

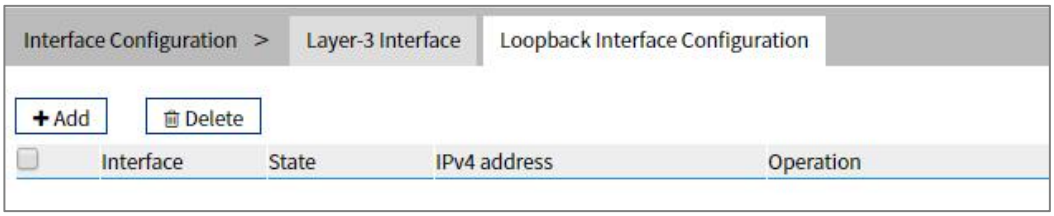
On the "Loopback Interface" page, user can configure the parameter of loopback interface.

Operation Path

Open in order: "L3 forward Config > Interface Config > Loopback Interface".

Interface Description

Loopback interface configuration interface as follows:



The main element configuration description of loopback interface interface:

Interface Element	Description
Interface	The name of loopback interface, value range: loopback0 or loopback1.
State	Loopback interface state information, options are: • Up; • Down.
IPv4 address	IPv4 address and subnet mask, such as 10.1.1.0/24.
Operation	Click the "Edit" button to set the interface and IPv4 address. Click "Delete" under "operation" to delete the relevant loop back interface directly.
Add	Click “add” button to add the configuration of loopback interface.
Delete	Check the radio box of loopback interface entry, click “Delete” button to delete loopback interface entry.

6.2 ARP Configuration

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 Show ARP

Function Description

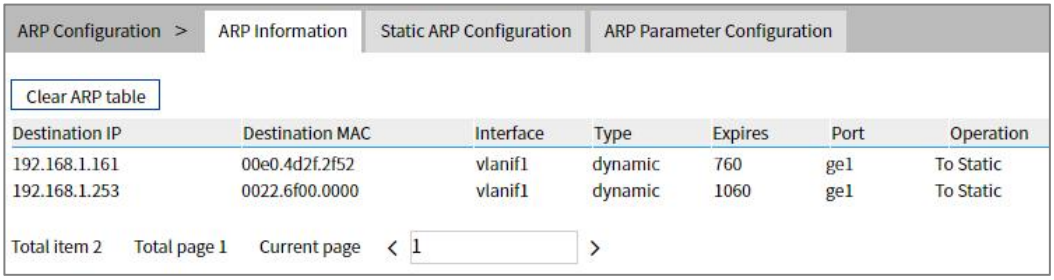
On the "ARP Information" page, user can check the ARP address, MAC, output port and other parameters.

Operation Path

Open in order: "L3 Configuration > ARP Configuration > ARP Information".

Interface Description

ARP Information interface as follow:



The main element configuration description of ARP information interface:

Interface Element	Description
Destination IP	Destination IP address of accessing device.
Destination MAC	Destination MAC address of accessing device.
Interface	Output port of accessing device data transmission.
Type	ARP mode of accessing device.
Expires	ARP age-time of accessing device.
Port	Port number of the accessing device.
Operation	Click “convert to Static” to convert dynamic address to static address.

6.2.2 Static ARP

Function Description

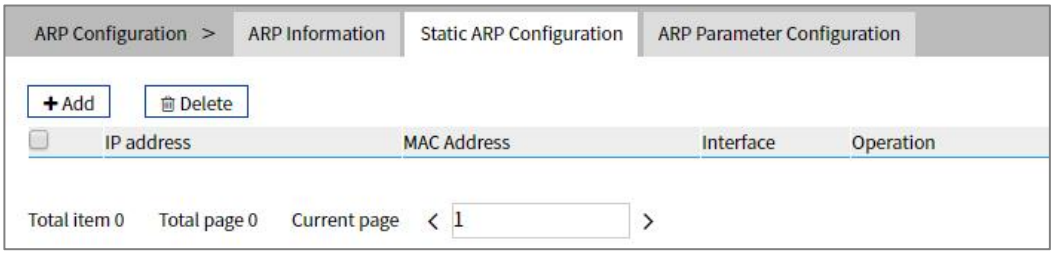
On the "Static ARP" page, user can conduct static ARP configuration.

Operation Path

Open in order: "L3 forward Configuration > ARP Configuration > Static ARP".

Interface Description

Static ARP interface as follows:



The main element configuration description of static ARP interface:

Interface Element	Description
IP Address	IP address of accessing device, such as 192.168.1.1.
MAC Address;	MAC address of the access device, such as 0001.0001.0001.
Interface	Output port of accessing device data transmission.
Operation	Click "Edit" under "operation" to edit the MAC address information again. Click "Delete" under "operation" to delete the entry directly.

6.2.3 ARP Parameter Configuration

Function Description

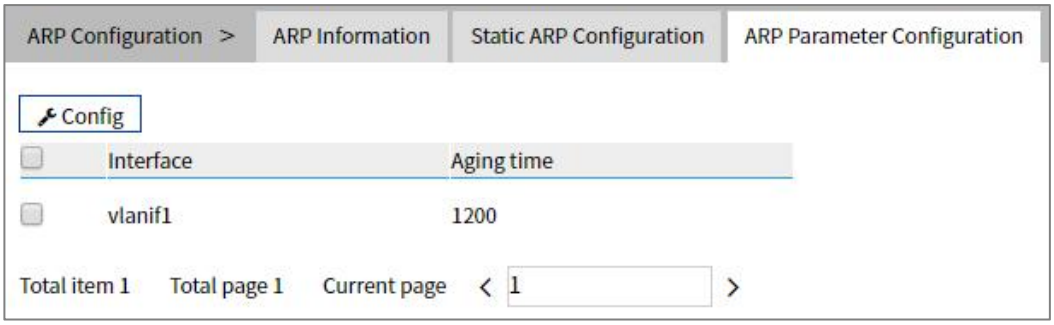
On the "ARP age-time" page, user can conduct ARP age-time configuration.

Operation Path

Open in order: "L3 Configuration > ARP Configuration > ARP Parameters Configuration".

Interface Description

ARP parameter configuration interface as follows:



The main element configuration description of ARP age-time interface:

Interface Element	Description
Interface	Interface Name.
Aging Time	Ageing time display.
Configuration	Check the ARP interface entry checkbox and click the “Config” button to configure the aging time of the specified interface. It is 1200 by default, valid input range is 30-1200 (second).

6.3 NAT Configuration

NAT(Network Address Translation) is a process of translating an IP address in an IP data header into another IP address. In practical application, NAT is mainly used to realize the function of private network accessing public network. This way of using a few public IP addresses to represent more private IP addresses will help to slow down the exhaustion of available IP address space.

Function Description

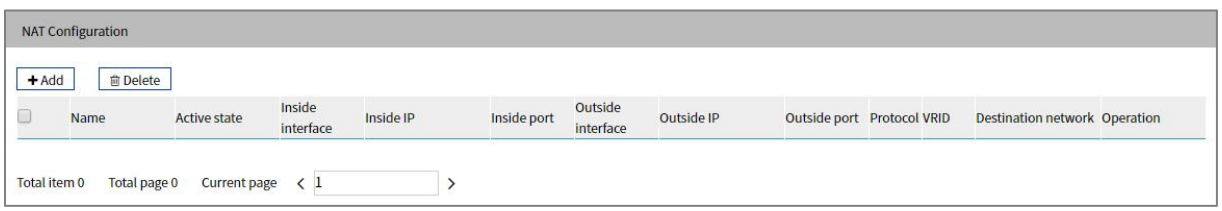
On the "NAT Configuration" page, user can add or remove NAT entries and set up the Intranet and extranet interfaces of the device.

Operation Path

Open in order: "L3 Configuration > NAT Configuration".

Interface Description

NAT configuration interface as follows:



Main elements configuration description of NAT configuration interface:

Interface Element	Description
Add	Click the “Add” button and set the Intranet and external interfaces of the device.
Delete	Check NAT port binding information to be deleted, and click “Delete” to delete it
Name	NAT entry name. Note: Support input of up to 32 characters of letters, numbers or @_! .
Active State	Whether NAT rule is activated or not, the status is as follows: • Activated: enable; • Inactive: disable.
Inside Interface	Connect the VLAN of the intranet device, access the IP of this VLAN, and access the public network through NAT.
Inside IP	Intranet IP that can be mapped to external network through NAT.
Inside Port	Port number of intranet VLAN corresponding to port mapping protocol. Note: tcp/udp :1-65535/ no filling indicates any port; all/icmp: No distinction between port numbers.
Outside Interface	The VLAN connecting the external network device, through which the external network can access the internal network device through NAT.
Outside IP	The external network IP mapped by the internal network IP through NAT.
Outside Port	The port number of the external VLAN corresponding to the port mapping protocol. Note: tcp/udp :1-65535/ no filling indicates any port; all/icmp: No distinction between port numbers.
Protocol	Mapping port protocol, options are as follows: • All: supports tcp, udp and icmp protocol forwarding; • tcp: supports tcp protocol forwarding; • udp: supports udp protocol forwarding; • icmp: supports icmp protocol forwarding. Note: When all and icmp protocols are selected, it is not supported to input internal network port and external network port. please keep the internal network port and external network port blank.
VRID	VRID is the VRRP ID, with values ranging from 1 to 255. When the devices in the VRRP backup group are configured

Interface Element	Description
	with the NAT address pool, it is possible for both devices to perform NAT translation on the packet, resulting in a conflict. Configuring the VRID allows you to optionally specify the Master device to do the NAT conversion, effectively avoiding collisions.
Destination Network	The destination network of internal terminal device, namely the IP address and subnet mask of the destination network, such as 10.1.1.0/24.
Operation: delete	Delete the NAT entry of the current line.

6.4 VRRP Configuration

VRRP (Virtual Router Redundancy Protocol) is a fault-tolerant protocol. In general, all hosts in a network will set a default route, when the destination address of the message sent by host isn't in the network segment; the message will be sent to the Router A via default router, achieving the communication between the host and external network. When the Router A breaks down, all hosts that takes Router A as default router in the network segment will disconnect communication to the outside, generating single point of failure. VRRP is proposed to solve the problem above, and it's designed for the local area network (such as: Ethernet) with multicast or broadcast capability.

VRRP organizes a set of routers (including a Master, that is the active router and several Backup, that is the standby router) in the local area network into a virtual router, which is called a backup team. The virtual router possesses its own IP address 10.100.10.1 (The IP address can be same to a router interface address in the backup team, it's called IP owner), routers in the backup team have their own IP address (such as IP address of Master is 10.100.10.2, IP address of Backup is 10.100.10.3). Hosts in the local area network only knows the virtual router IP address is 10.100.10.1, it doesn't know that the specific Master router IP address is 10.100.10.2 and Backup router IP address is 10.100.10.3. Hosts set their own default router next hop address to the virtual router IP address 10.100.10.1. Thereupon, hosts in the network start to communicate with other networks via the virtual router. If the Master router in backup team breaks down, Backup router will elect a new Master router via election strategy

and provide router service for hosts in the network. Therefore, hosts in the network can uninterruptedly communicate with outside network.

Principle of realization

A VRRP router has the only identification: VRID, range is 0-255. The router has only one virtual MAC address, and the address format is 00-00-5E-00-01-[VRID]. Master router is responsible for replying the ARP request by MAC address. Regardless of the switching, it's ensured to give the only consistent IP and MAC address to the terminal device, declining the switching influence to terminal device.

VRRP control message includes only one type: VRRP announce (advertisement). It's packaged by IP multicast data packet, the multicast address is 224.0.0.18, issue range can be only in the same local area network. It has ensured that VRID can be repeatedly used in different network. In order to decrease the network bandwidth consumption, only the master router can periodically send VRRP announce message. Backup router will start new VRRP election if it can't receive VRRP in three consecutive announce intervals or receives announce with 0 priority.

In the VRRP router group, the master router is elected by priority. The priority range in VRRP protocol is 0-255. If VRRP router IP address is the same to virtual router interface IP address, then the virtual router is called IP address owner in VRRP group; IP address owner automatically has the highest priority: 255. Priority 0 is usually used when IP address owner forwardly gives up the master role. Configurable priority range is 1-254. Priority configuration principle is set according to the link speed and cost, router performance and reliability, and other management strategies. In the election of master router, virtual router with high priority wins; therefore, if there exists IP address owner in VRRP group, it will appear as the master router. Candidate router with the same priority can be elected according to IP address size order. VRRP has also provided priority preemption strategy, if the strategy is configured, backup router with high priority will deprive current master router with low priority and become the new master router.

In order to ensure the safety of VRRP protocol, two safety certification measures are provided: Plaintext authentication and IP header authentication. Plaintext authentication method requirements: User must provide the VRID and plaintext password while joining a VRRP router. It suits for avoiding the configuration error in the local area network but can't prevent gaining the password via network monitoring

method. IP header authentication method has provided higher security, and it can prevent message replay and modification attack.

Function Description

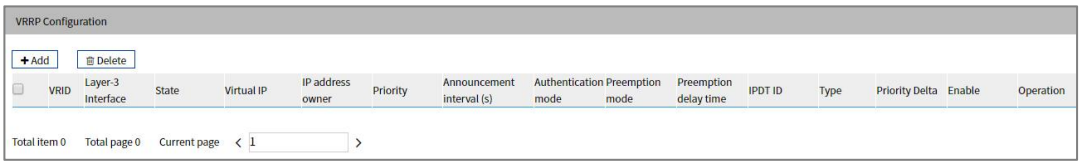
On the "VRRP Configuration" page, user can configure VRRP parameters.

Operation Path

Open in order: "L3 Configuration > VRRP Configuration".

Interface Description

VRRP configuration interface as follow:



The main element configuration description of VRRP configuration interface:

Interface Element	Description
VRID	Virtual router ID, valid range is 1-255.
Layer 3 Interface	Layer 3 interface information, such as, vlanif1.
State	Current status, options as follows: • Master; • Backup
Virtual IP	Virtual router IP address, such as 192.168.1.253.
IP Address Owner	The IP address owner takes the virtual router IP address as the real interface address.
Priority	Priority defaults to 100, valid range is 1-254. Note: When the IP address owner is configured, the default priority can only be 255.
Announcement Interval (s)	The Master router in the VRRP backup group will send a notification message to notify the routers in the VRRP backup group that they are working normally, unit: second, default: 1 second, valid range: 1-10 seconds.
Authentication Mode	Configure how the backup group sends and receives VRRP messages. By default, no authentication is performed. Options are as follows: • disable; • text. Note: • Different backup groups on an interface can set different authentication methods.

Interface Element	Description
	• Members joining the same backup group need to set up the same authentication mode.
Preemption Mode	In the preemption mode, once the routers in the backup group find that their priority is higher than that of the current Master router, they will send VRRP announcement messages to the outside. It causes the router in the backup group to reelect the Master router and eventually replace the original Master router. Accordingly, the original Master router will become the Backup router. Preemption mode, options as follows: • false; • true.
Preemption Delay Time	Set a preemption delay for a VRRP backup group to avoid frequent primary and standby state transitions among members of the backup group. Valid range is 0-255s, the default value is 0s.
IPDT ID	The value range of IPDT ID is 1-8.
Type	IPDT priority type, options are as follows: • Increased: After "Track" is enabled, the VRRP priority value is equal to the original VRRP priority value plus the IPDT priority value when the IPDT link fails. • Reduced: After "Track" is enabled, the VRRP priority value is equal to the original VRRP priority value minus the IPDT priority value when the IPDT link fails.
IPDT priority	Port priority level, the value range is 1-253.
Enable	Enable switch, options are as follows: • Enable; • Disable.
Operation	Click “Edit” under “Operation” to re-edit VRRP configuration information; Click “Delete” under “Operation” to delete the entry directly.

7 Unicast routing table

7.1 IPv4 Configuration

7.1.1 IPv4 Routing Table

Function Description

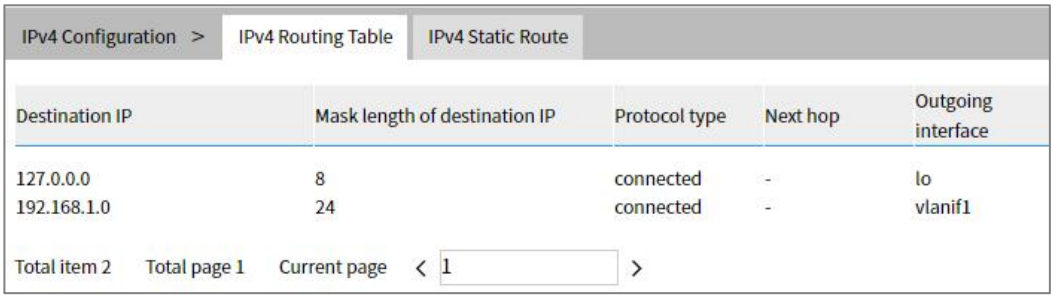
On the "IPv4 Routing Table" page, user can check various router configuration methods.

Operation Path

Open in order: "unicast routing > IPv4 Configure > IPv4 routing table".

Interface Description

The IPv4 routing table interface as follows:



The main element configuration description of show route interface:

Interface Element	Description
Destination IP	Destination IP addresses.
Mask Length of Destination IP	The length of destination subnet mask.
Protocol Type	Protocol type, corresponding full name relationship as below: • K-kernel route;

Interface Element	Description
	• C - connected; • S – static; • R – RIP; • O – OSPF; • I - IS-IS; • B – BGP; • A – Babel; • > - selected route; • * - FIB route.
Next Hop	Gateway address information of next hop.
Output Port	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

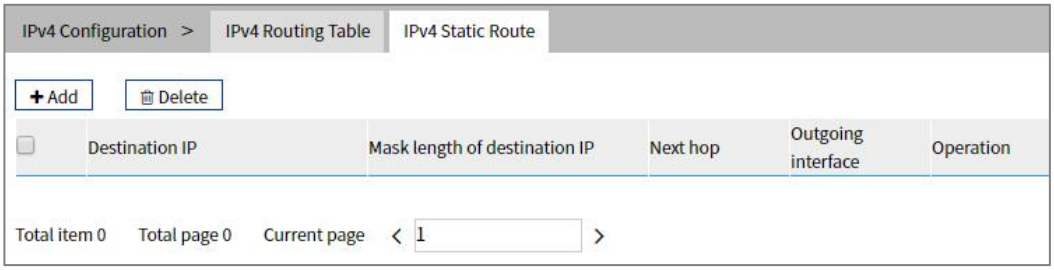
On the "IPv4 Static Route" page, user can configure static route.

Operation Path

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

Interface Description

The IPv4 Static Route interface as follows:



The main element configuration description of IPv4 Static Route interface:

Interface Element	Description

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.
Outgoing Interface	Interface Name.
Operation	Click the "Delete" button to delete the the current entry.

7.2 RIP Configuration

RIP (Routing Information Protocol) is a simple Interior Gateway Protocol (IGP) and mainly used in small network, such as Campus Network and Local Area Network with simple structure. RIP isn't used in more complex environment and large network.

RIP is simple to achieve and easier in configuration and maintenance than OSPF or IS-IS, so it's widely used in actual networking.

7.2.1 RIP Global Configuration

Function Description

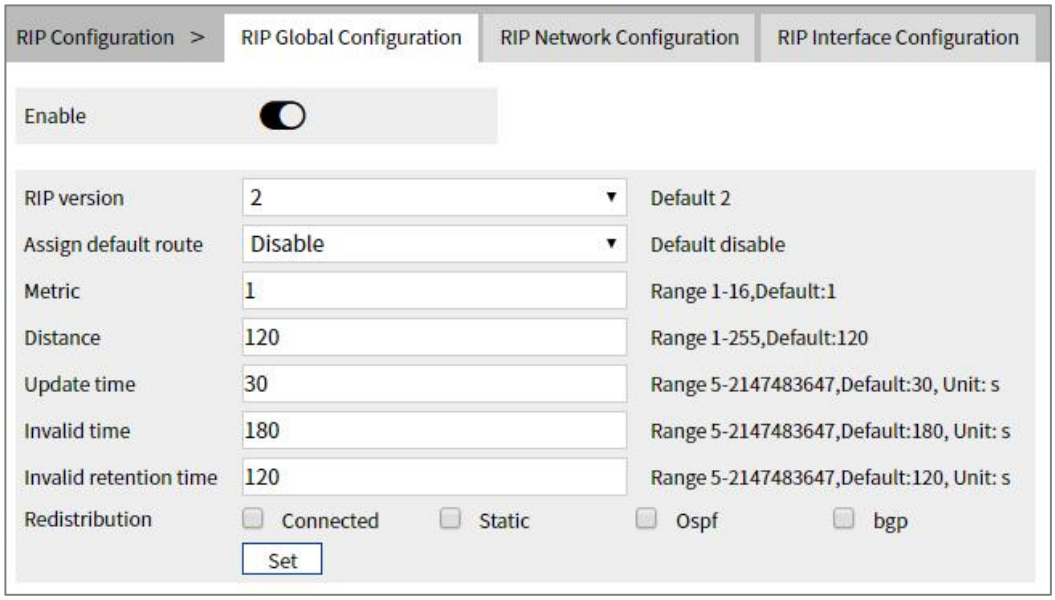
On the "RIP Global Config" page, user can conduct RIP global relative parameters configuration.

Operation Path

Open in order: "Unicast Routing > RIP Configuration > RIP Global Configuration".

Interface Description

RIP global configuration interface as follows:



The main element configuration description of RIP global configuration interface:

Interface Element	Description
Enable	RIP function enable switch. RIP-related parameter configuration will appear when it is enabled.
RIP Version	RIP version drop-down list, the default version is RIP-2, the options of version are as follows: • 1: RIP-1 is Classful Routing Protocol, it only supports releasing protocol message via broadcast mode, only natural network segments such as A, B and C can be identified. • 2: RIP-2 is a non-classified routing protocol, which is extended on the basis of RIP-1. Note: Interface can only send/receive data packets of the RIP version configured.
Assign Default Route	The default route with the destination address of 0.0.0.0 is assigned to RIP routing database, which is disabled by default. The options are as follows: • Enable; • Disable.
Metric	The metric is equal to the number of devices from this route to the destination route, with a default value of 1 and a value range of 1-16. Hops greater than or equal to 16 are defined as infinite, i.e. the destination network or host is unreachable.
Distance	RIP route management distance, the default distance is 120, the value range is 1-255. When there are routes from two different routing protocols to the same destination, the smaller the management distance value of the routing protocol is, the

Interface Element	Description
	more reliable the route obtained by the protocol is.
Update Time	Routing information update time. When the timer timeout, immediately send update message, update messages are sent every 30 seconds by default. Value range is 5-2147483647 seconds. Note: When the routing information changes, the trigger update message is immediately sent to the neighbor device instead of waiting for the update timer timeout, thus avoiding the routing loop.
Invalid Time	If no routing update message is received from the neighbor within the invalid time, the route is considered unreachable. By default it is 180 seconds, value range is 5-2147483647 seconds.
Invalid Retention Time	If the unreachable route does not receive an update message from the same neighbor before the invalid retention timer countdown ends, the route will be completely deleted from the RIP routing table. By default it is 120 seconds, value range is 5-2147483647 seconds.
Redistribution	To reallocate routes learned from other routing protocols to RIP, options are as follows: • connected: direct connection routing. • static: static route; • ospf: OSPF route. • bgp: BGP border gateway protocol.
Set	Click the “Set” button to save and validate the configuration of RIP related parameters.

7.2.2 RIP Network Setting

Function Description

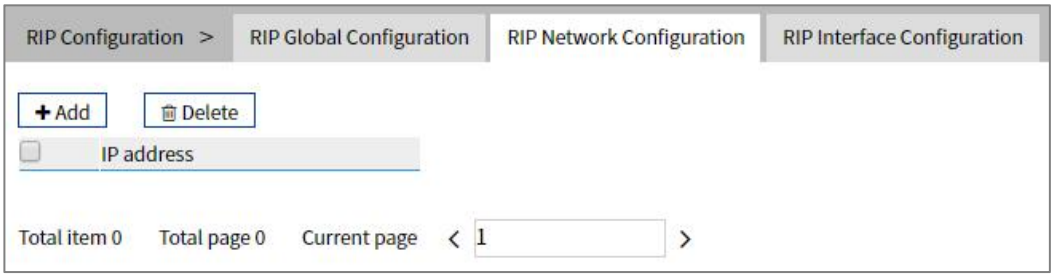
On the “RIP Network Configuration” page, user can configure the RIP network address.

Operation Path

Open in order: "Unicast Routing > RIP Configuration > RIP Network Configuration".

Interface Description

RIP network setting interface as follows:



The main element configuration description of RIP global configuration interface:

Interface Element	Description
Add	Click the “Add” button to specify the IP address of the network interface to enable RIP, such as 35.0.0.0/8.
Delete	Check the network entry to be deleted, and then click the “Delete” button to delete the specified network entry.
IP Address	Displays IP address information of the configured network interface.

7.2.3 RIP Interface Configuration

Function Description

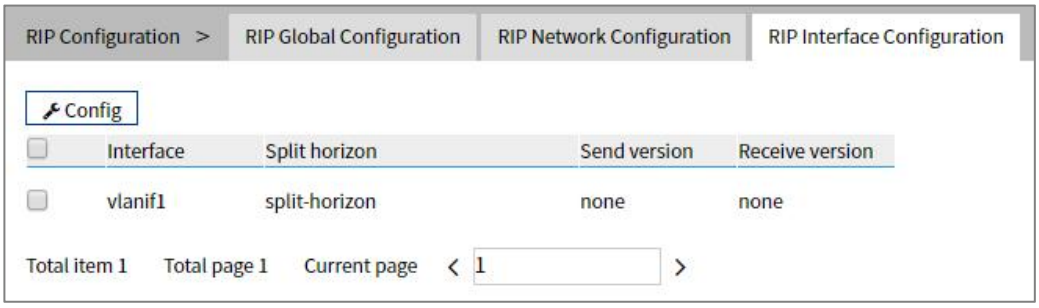
On the "RIP Interface Configuration" page, user can conduct RIP network parameter configuration.

Operation Path

Open in order: "Unicast Routing > RIP Configuration > RIP Interface Configuration".

Interface Description

RIP interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	RIP interface information

Interface Element	Description
Split Horizon	Horizontal partition. Options are as follows: • None; • Split-horizon; • Poison-reverse. Note: Route that RIP learns from an interface, it won't be sent from the interface to neighbor router. It can not only reduce bandwidth consumption but also prevent routing loops.
Send Version	RIP protocol version of sending data, options as follows: • None; • 1; • 2; • 1 and 2; • 1-compatible.
Receive Version	RIP protocol version of receiving data, options as follows: • None; • 1; • 2; • 1 and 2.

8 Multicast Routing

8.1 Multicast Routing

8.1.1 Multicast Routing

Function Description

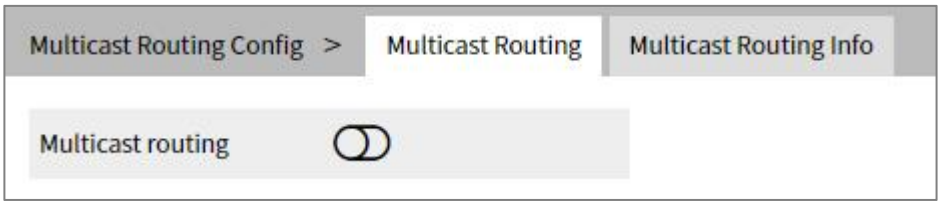
On the Multicast Routing page, user can enable or disable the layer 3 multicast routing feature.

Operation Path

Open in order: "Multicast Routing > Multicast Routing > Multicast Routing".

Interface Description

The multicast routing interface is shown as follows:



Main elements of the multicast routing interface:

Interface Element	Description
Multicast routing	Click the button to enable or disable multicast routing, swipe right to enable it, swipe left to disable it.

8.1.2 Multicast Routing Information

Function Description

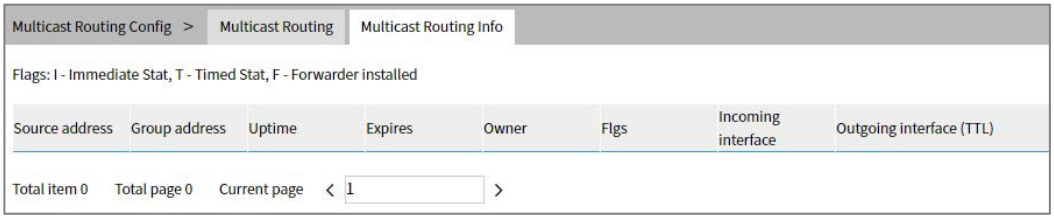
On the "Multicast Routing Information" page, user can view the layer 3 multicast routing information.

Operation Path

Open in order: "Multicast Routing > Multicast Routing > Multicast Routing Information".

Interface Description

The multicast routing information interface is as follows:



Main elements of the multicast routing information interface:

Interface Element	Description
Source Address	Multicast source address
Group Address	Multicast group address
Uptime	The existed time of the multicast route.
Expires	Multicast routing aging time.
Owner	The owner of a multicast route may be a multicast routing protocol.
Flags	Multicast routing protocol flag: • I: Immediate Stat (Immediately the statistics) • T: Timed Stat (Statistics Timer) • F: Forwarder installed (Set to forward table)
Incoming Interface	Multicast data ingress interface. The interface on the local device that receives multicast data.
Outcoming Interface (TTL)	Multicast data egress interface. The interface that forwards multicast data out.

8.2 IGMP Configuration

8.2.1 Interface Configuration

Function Description

On the interface configuration page, user can add or delete IGMP configuration of Ethernet ports.

Operation Path

Open in order: "Multicast Routing > IGMP Configuration > Interface Configuration".

Interface Description

Interface configuration interface as follows:

The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	Layer 3 interface, such as vlanif1.
IGMP	IGMP status: • enable; • disable.
Version	IGMP version, options are: • 1: IGMPv1, it defines the basic querying and reporting process of group members; • 2: IGMPv2, it adds the mechanism of polling and leaving group members on IGMPv1; • 3: IGMPv3, members are added to IGMPv2 to specify whether to receive or not to receive messages from certain multicast sources.
Router-Alert Option	RA(Router-Alert). When a network device receives a message, only the message whose destination IP address is the interface address of the device will be sent to the corresponding protocol module for processing. If the destination address of the protocol message is not the interface address of the device, check whether the IP

Interface Element	Description
	message header carries the Router-Alert option, if so, it will be directly sent to the corresponding protocol module for processing without checking the destination address. Note: For compatibility reasons, after receiving IGMP message, the current switch will send it to IGMP protocol module for processing by default regardless of whether its IP header contains Router-Alert option.
Unlimited Same Subnet	Limit the multicast source and interface to the same subnet, otherwise the port cannot receive multicast messages.
Robustness Coefficient	Specify the robustness of the IGMP query, ranging from 2 to 7. This coefficient is used to specify the default value of the number of times an IGMP query message is sent by the IGMP query at startup, and the number of times an IGMP query message is sent by the IGMP query after the IGMP query receives the message leaving the group.
Other Querier Present Timer	Timer time of non-inquirer. • Before the timer expires, if the inquiry message from the inquirer is received, reset the timer; • Otherwise, the original inquirer is considered invalid, and a new inquirer election process is initiated.
Fast Leave ACL	By default, when the interface works in IGMP v2 or v3, after receiving IGMP leave message, it will send a specific group query message to determine whether to age multicast member entries. After configuring the fast leave ACL, if the group address specified by the leave message is within the group address range specified by the ACL, the multicast member table entry can be aged immediately.
Deny Multicast ACL	List of restricted multicast groups.
Multicast Group Max	The maximum number of multicast supported.
Operation: edit	Modify IGMP entries.
Operation: delete	Delete the current IGMP entry.

8.2.2 SSM-Map Configuration

SSM(Source-Specific Multicast) requires routers to know the multicast source designated by member hosts when they join the multicast group. A host running IGMPv3 can specify multicast source addresses in IGMPv3 Report messages. However, hosts running IGMPv1 or IGMPv2 rely on the IGMP SSM mapping function to obtain the SSM service.

The mechanism of IGMP SSM Mapping is: by statically configuring SSM address Mapping rules on the router, information in IGMPv1 and IGMPv2 report packets is converted into corresponding information to provide SSM multicast service.

After the configuration of SSM Mapping rules, when the IGMP query receives the IGMPv1 or IGMPv2 report packets from the member host, it first checks the multicast group addresses carried in the paper, and then processes them separately according to the different inspection results.

- If the Multicast group is within the range of ANY-Source Multicast, then only ASM services are provided.
- If the multicast group is within the SSM group address range (the default is 232.0.0.0 ~ 232.255.255.255) :
  - If the router does not have the SSM Mapping rule corresponding to the multicast group, the SSM service cannot be provided and the article is discarded.
  - If there are SSM Mapping rules corresponding to the multicast group on the router, according to the rules, the information contained in the report packet (member, multicast group) will be mapped to (multicast group, INCLUDE, member) information, and SSM service will be provided.

Note:

By default, the IGMP SSM Mapping function is disabled. The switch can be turned on after sliding to the right.

Function Description

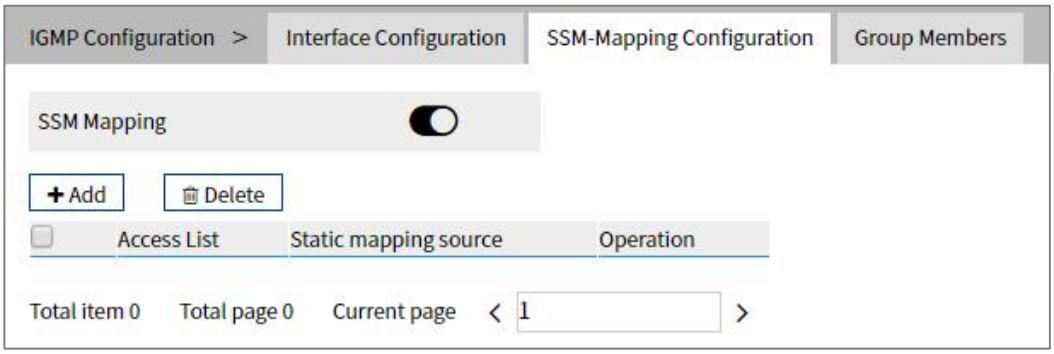
On the interface configuration page, user can add or delete IGMP configuration of Ethernet ports.

Operation Path

Open in order: "Multicast Routing > IGMP Configuration > SSM-Map Configuration

Interface Description

The SSM-Map configuration interface is as follows:



Main element configuration description of SSM-Map configuration interface:

Interface Element	Description
SSM Mapping	IGMP SSM Mapping function switch is closed by default and turned on after sliding the switch to the right.
Access List	Access list.
Static Mapping Source	The specified multicast source address in the access list.

8.2.3 Multicast Group Information

Function Description

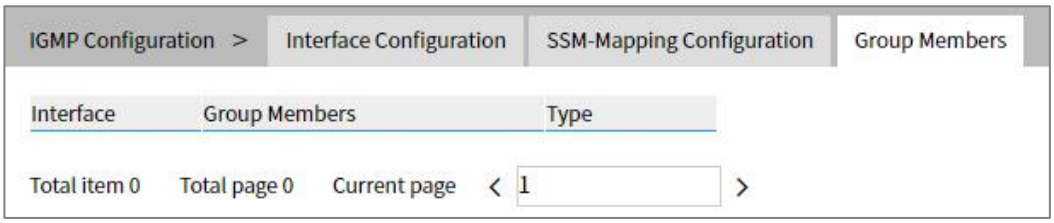
On the "Multicast Group Information" page, display the multicast information received by the device interface.

Operation Path

Open in order: "Multicast Routing > IGMP Configuration > Multicast Group Information".

Interface Description

The multicast group information interface is as follows:



Main element configuration description of multicast group information interface:

Interface Element	Description
Interface	Ethernet port.

Interface Element	Description
Group Members	The multicast address received by the interface.
Type	Multicast type: • dynamic • static

8.3 PIM-SM Configuration

PIM-SM is a multicast routing protocol in sparse mode, which uses "Pull mode" to transmit multicast data. It is usually suitable for large and medium-sized networks with relatively scattered multicast group members and a wide range. Its basic principle is as follows:

- PIM-SM assumes that all hosts do not need to receive multicast data, but only forward it to the hosts that explicitly propose that they need multicast data. The core task of PIM-SM to realize multicast forwarding is to construct and maintain RPT(Rendezvous Point Tree). RPT selects a router in PIM domain as a common root node RP(Rendezvous Point), and multicast data is forwarded to receivers along RPT through RP.
- The router connecting the receiver sends a Join Message to the RP corresponding to a multicast group, and the message is delivered to the RP hop by hop, and the path it passes forms a branch of RPT;
- If a multicast source wants to send multicast data to a multicast group, the DR(Designated Router (DR) on the multicast source side is responsible for registering with the RP, and sending a Register Message to the RP by unicast, which triggers the establishment of SPT after reaching the RP. After that, the multicast source sends the multicast data to RP along SPT. When the multicast data reaches RP, it is copied and sent to the receiver along RPT.

The working mechanism of PIM-SM can be summarized as follows:

- Neighbor Discovery
- DR election
- RP Discovery
- Construct RPT
- Multicast source note
- SPT Switchover
- Assertion

8.3.1 Global Configuration

Function Description

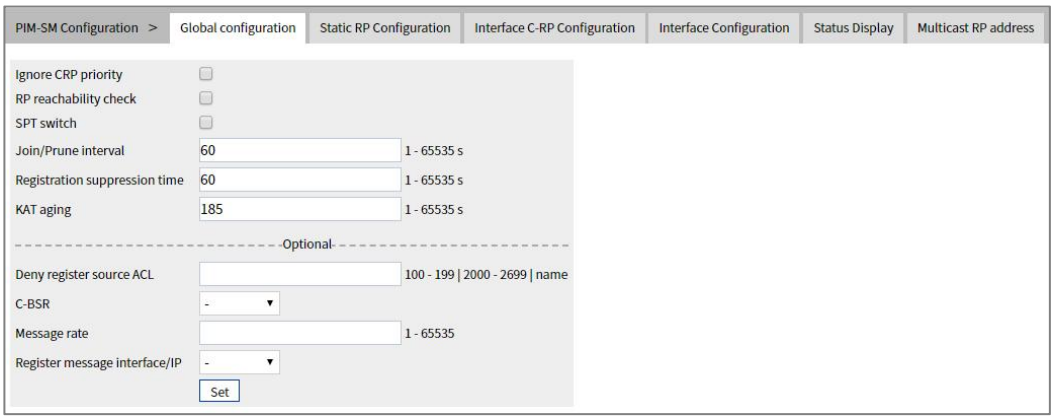
On the global configuration page, user can configure the global parameters of PIM-SM.

Operation Path

Open in order: "Multicast Routing > PM-SM Configuration > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Ignore CRP Priority	When selecting the RP corresponding to multicast, whether to ignore the priority of CRP and choose according to IP address. The one with the larger IP address is elected.
RP Reachability Check	Whether it is necessary to check the reachability of RP when sending the registration message; if it is not, it means that it cannot be registered.
SPT Switch	RP is a necessary transit station for all multicast messages. when the multicast message rate gradually increases, it will create a huge burden on RP. PIM-SM allows RP or group member DR to reduce the burden of RP by triggering SPT switching.
Join/Prune Interval	Time interval for PIM router to send join/pruning messages. Note: By default, the join/pruning message is sent at an interval of 60 seconds.
Registration	The time interval for sending the registration message again

Interface Element	Description
Suppression Time	after receiving the registration stop message ranges from 1 to 65535, and the unit is seconds. The default value is 60 seconds.
KAT Aging	The aging time of KAT timer after receiving the registration message ranges from 1 to 65535 in seconds. Note: By default, after receiving the registration message, the aging time of KAT timer = registration inhibition time * 3+registration detection time (the default is 5 seconds).
Deny Register Source ACL	Configure illegal neighbor source address range. Note: By default, there are no restrictions on the neighbor source addresses that an interface can learn from.
C-BSR	C-BSR Interface Configuration. • vlanif: vlanif interface; • Loopback: loopback interface.
Message Rate	The rate of receiving and processing multicast service messages ranges from 1 to 65535, and the unit is one/second.
Register Message Interface /IP	The VLAN interface, source IP address or loopback interface that sends the registration message.

8.3.2 Static RP Configuration

Function Description

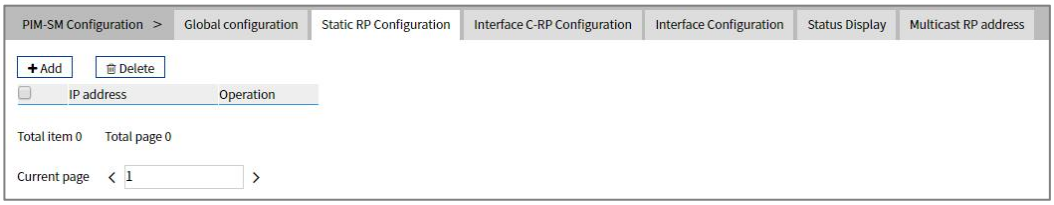
On the static RP configuration page, you can set up the static RP manually.

Operation Path

Open in order: "Multicast Routing > PIM-SM Configuration > Static RP Configuration".

Interface Description

Static RP configuration interface as follow:



The main element configuration description of static RP configuration interface:

Interface Element	Description
IP Address	Configure the IP address of the static RP. Note: The address must be a legal unicast IP address, and should not be configured as the address of the 127.0.0.0/8 network segment.
Operation: delete	Delete the static RP entry of the current line.

8.3.3 Interface C-RP Configuration

Function Description

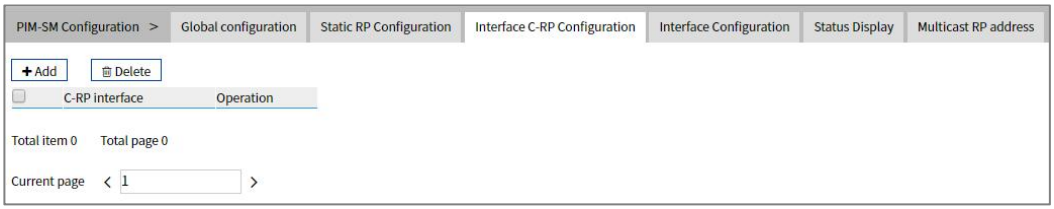
On the interface C-RP configuration page, you can add or delete C-RP interfaces.

Operation Path

Open in order: "Multicast Routing > PM-SM Configuration > Interface C-RP Configuration".

Interface Description

The interface C-RP configuration interface is as follows:



Main element configuration description of interface C-RP configuration interface:

Interface Element	Description
C-RP Interface	To configure the C-RP interface: • vlanif: vlanif interface; • Loopback: loopback interface.
Operation: delete	Delete the candidate convergence point entry in the current line.

8.3.4 Interface Configuration

Function Description

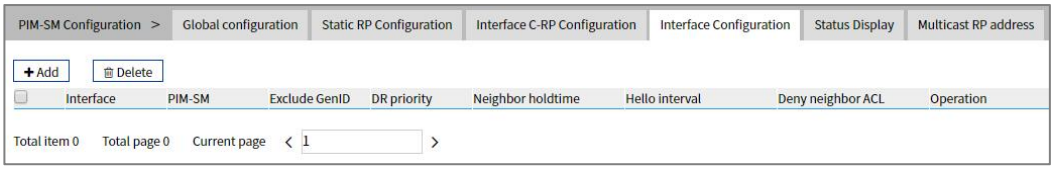
On the "Interface Configuration" page, user can set interface PIM- SM parameters.

Operation Path

Open in order: "Multicast Routing > PM-SM Configuration > Interface Configuration".

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	Configure interface: • vlanif: vlanif interface; • Loopback: loopback interface.
PIM-SM	PIM-SM status. • enable; • disable.
Exclude GenID	The interface is configured to send hello messages without carrying GenID information. Note: GenID is a random value at the initial creation of the interface to identify unique interface information. With this information, users can detect whether the neighbor device has been restarted.
DR Priority	Specify the priority of running for DR from 0 to 4294967294. Note: The higher the value, the higher the priority.
Neighbor Holdtime	Specify the time to keep PIM neighbor reachable, the value range is 1 ~ 65535, and the unit is seconds. Note: If specified as 65535 seconds, the PIM neighbor is always reachable.
Hello Interval	Time period for sending Hello messages between PIM routers.
Deny Neighbor ACL	Illegal neighbor source address range.
Operation: edit	Modify and delete interface configuration items.
Operation: delete	Delete the interface configuration item of the current line.

8.3.5 Status Display

Function Description

On the "Status Display" page, you can view the parameter configuration of PIM multicast, including:

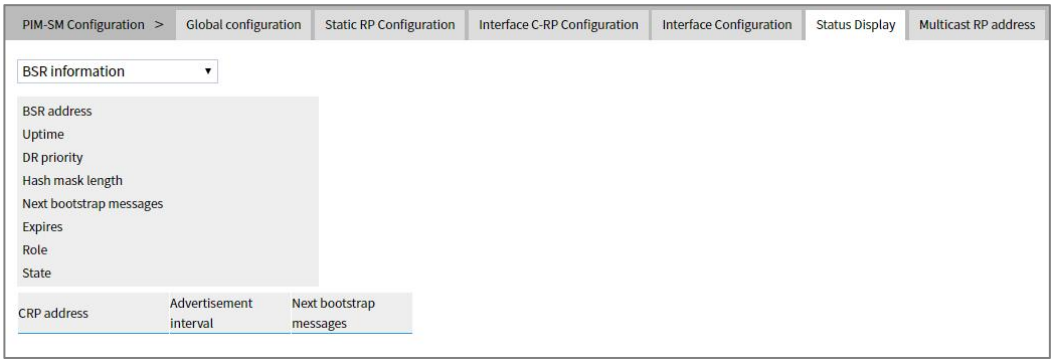
- BSR information
- Interface information
- Local multicast
- Multicast routing table
- Neighbor
- Next hop information
- RP-Set information

Operation Path

Open in order: "Multicast Routing > PIM-SM Configure > Status Display".

Interface Description

The status display interface is as follows:



8.3.6 Multicast PR Address

Function Description

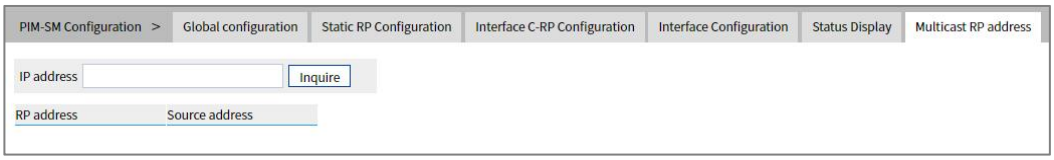
In multicast RP address, user can query the multicast RP address.

Operation Path

Open in order: "Multicast Routing > PIM-SM Configure > Multicast RP Address".

Interface Description

The multicast RP address interface is as follows:



Main element configuration description of multicast RP address interface:

Interface Element	Description
IP Address	Multicast address.
RP Address	RP address.
Source Address	CRP source address.

8.4 PIM-DM Configuration

PIM-DM is a multicast routing protocol in dense mode, which uses "Push mode" to transmit multicast data. It is usually suitable for small networks with relatively dense multicast group members. Its basic principle is as follows:

- PIM-DM assumes that each subnet in the network has at least one multicast group member, so multicast data will be Flooding to all nodes in the network. Then, PIM-DM prune the branches without multicast data forwarding, leaving only the branches containing receivers. This "Flooding-Prune" phenomenon occurs periodically, and the pruned branches can also be restored to forwarding status periodically.
- In order to reduce the time required for the node to return to the forwarding state when the multicast group members appear on the branched node, PIM-DM actively resumes its forwarding of multicast data by using the Graft mechanism.

Generally speaking, the forwarding path of data packets in dense mode is a Source Tree (a forwarding tree with multicast source as its root and multicast group members as its branches and leaves). Source Tree is also called SPT(Shortest Path Tree) because it uses the shortest path from multicast source to receiver.

The working mechanism of PIM-DM can be summarized as follows:

- Neighbor Discovery
- Build SPT
- Graft
- Assertion

8.4.1 Global Configuration

Function Description

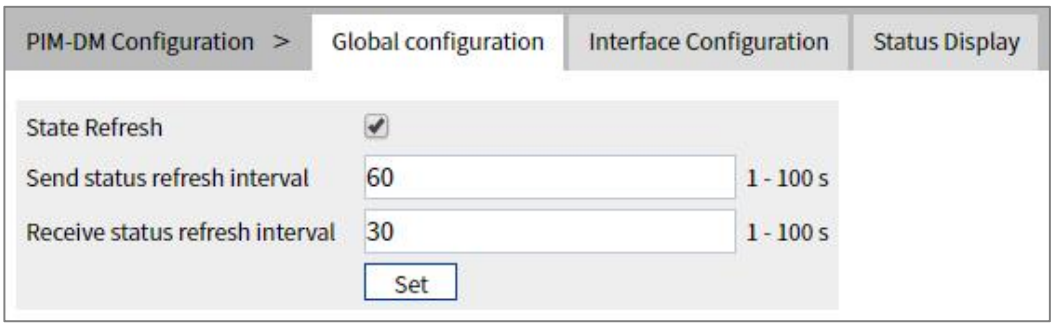
On the Global Configuration page, user can refresh the pruning timer status and set the time interval between sending status and receiving status.

Operation Path

Open in order: "Multicast Routing > PM-DM Configuration > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
State Refresh	When checked, refresh the status of pruning timer to prevent the clipped interface from resuming forwarding due to timeout of pruning timer.
Send Status Refresh Interval	The pruning timer updates the sending state time interval.
Receive Status Refresh Interval	The pruning timer updates the receiving state time interval.

8.4.2 Interface Configuration

Function Description

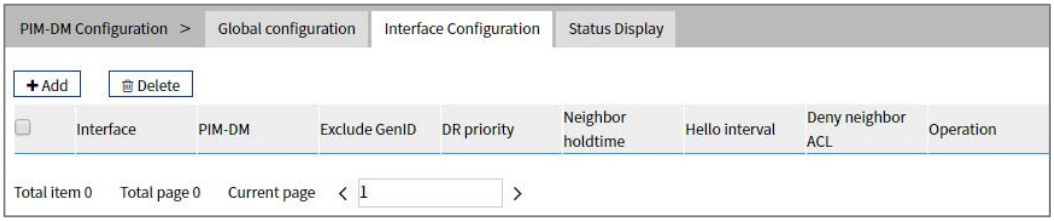
On the "Interface Configuration" page, user can configure interface PIM-DM parameters.

Operation Path

Open in order: "Multicast Routing > PIM-DM Configure > Interface Configuration".

Interface Description

Interface configuration interface as follows:



The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	Configure interface: • vlanif: vlanif interface; • Loopback: loopback interface.
PIM-DM	PIM-DM status. • enable; • disable.
Exclude GenID	The interface is configured to send hello messages without carrying GenID information. Note: GenID is a random value at the initial creation of the interface to identify unique interface information. With this information, users can detect whether the neighbor device has been restarted.
DR Priority	Specify the priority of running for DR from 0 to 4294967294. Note: The higher the value, the higher the priority.
Neighbor Holdtime	Specify the time to keep PIM neighbor reachable, the value range is 1 ~ 65535, and the unit is seconds. Note: If specified as 65535 seconds, the PIM neighbor is always reachable.
Hello Interval	Time period for sending Hello messages between PIM routers.
Deny Neighbor ACL	Illegal neighbor source address range.
Operation: edit	Modify and delete interface configuration items.
Operation: delete	Delete the interface configuration item of the current line.

8.4.3 Status Display

Function Description

On the "Status Display" page, you can view the parameter configuration of PIM multicast, including:

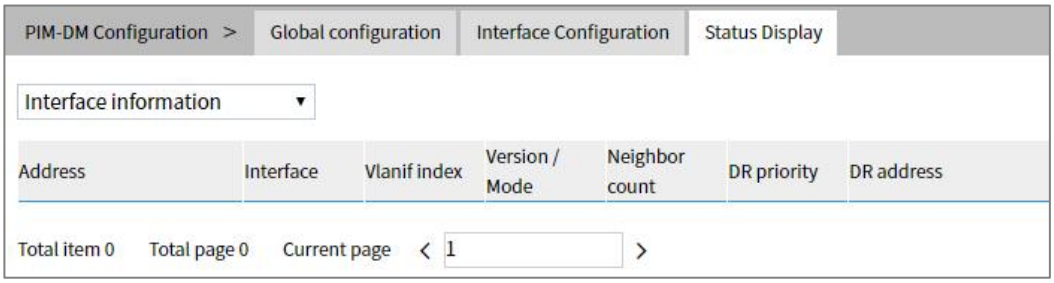
- BSR information
- Interface information
- Local multicast
- Multicast routing table
- Neighbor
- Next hop information
- RP-Set information

Operation Path

Open in order: "Multicast Routing > PIM-DM Configure > Status Display".

Interface Description

The status display interface is as follows:



9 Advanced Configuration

9.1 DHCP-Server Configuration

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.

9.1.1 DHCP Switch

Function Description

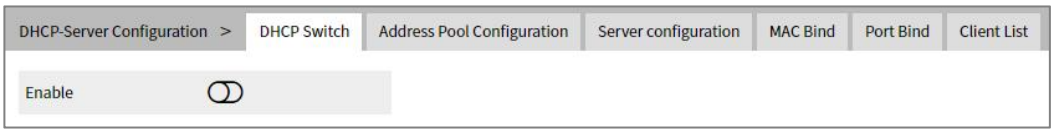
On the "DHCP Switch" page, user can enable/disable DHCP.

Operation Path

Open in order: "Advanced Configuration > DHCP Configuration > DHCP Switch".

Interface Description

DHCP switch configuration interface as follows:



The main element configuration description of DHCP switch configuration interface.

Interface Element	Description
Enable	After enabling the switch, set the device as a DHCP server by setting static allocation address table, the device can distribute IP address to devices connected to it.

9.1.2 DHCP 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

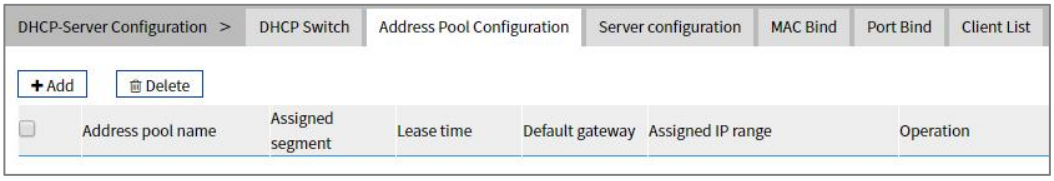
On the "DHCP Pool Config" page, user can add, delete the address pool and look over the configuration information of address pool.

Operation Path

Open in order: "Advanced Configuration > DHCP Configuration > Pool Configuration".

Interface Description

DHCP address pool configuration interface as follows:



The main element configuration description of DHCP pool configuration interface:

Interface Element	Description
Address Pool Name	The name of address pool, up to 32 characters.
Assigned 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
Assigned 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.
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.

9.1.3 Server Configuration

Function Description

On the "Address Pool Server Config" page, user can add, delete DNS/WINS/Log Server Address Pool.

Operation Path

Open in order: "Advanced Configuration > DHCP Configuration > Server Configuration".

Interface Description

Server configuration interface as follows:

The main element configuration description of server configuration interface:

Interface Element	Description
Add	Click the “Add” button to configure IP address pools for DNS servers, WINS servers, and log servers, with three IP addresses per server.
Type	Three kinds of address pool servers are supported, as shown below: • DNS server: parse the domain name to be visited to an IP address, realizing domain name access network. • WINS server: parse the NetBIOS host name using the Windows Microsoft operating system to an IP address. • Log server.
IP	Server address pool, which supports up to three different server IP addresses.
Operation	Click “Delete” under “operation” to delete the corresponding server address pool.

9.1.4 MAC Binding

Function Description

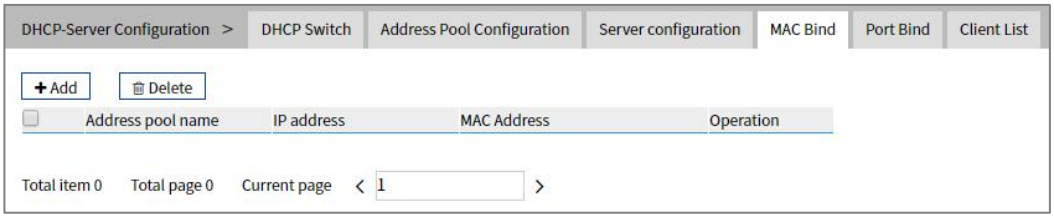
On the “MAC binding” page, users can bind the IP address assigned by the address pool to the MAC address of the device.

Operation Path

Open in order: "Advanced Configuration > DHCP Server Configuration > MAC Binding".

Interface Description

The MAC binding configuration 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 Address	IP addresses distributed by DHCP address pool, IP addresses obtained by this MAC address.
MAC Address;	The MAC address information of this device.
Operation	Click "Delete" under "operation" to delete this MAC binding.

9.1.5 Port Binding

Function Description

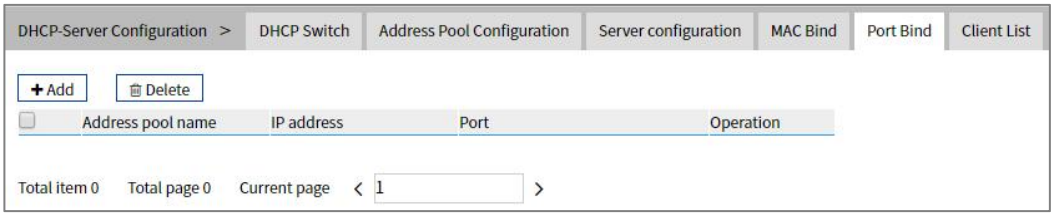
On the “Port binding” page, users can bind the relationship of IP addresses assigned by ports. Device A enables DHCP Server function and sets 2 static distribution address tables: 192.168.1.19 corresponding port is 1; 192.168.1.20 corresponding port is 2. After device B enables IP address automated acquisition function, if device A is connected to device B via port 1, device B can automatically obtain 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: "Advanced Config > DHCP Server Config > Port binding".

Interface Description

Port binding configuration interface as follows:



The main element configuration description of port binding 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 Address	IP address that DHCP address pool distributes, 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.

9.1.6 Client List

Function Description

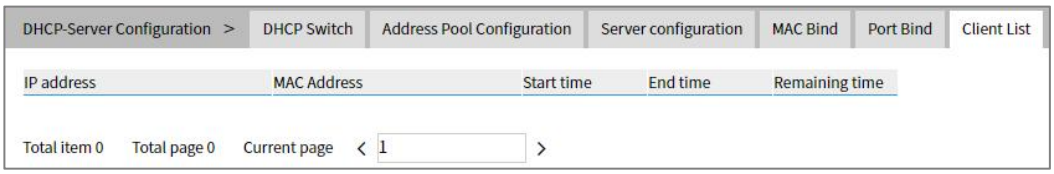
On the "Client List" page, user can look over the information of DHCP client.

Operation Path

Open in order: "Advanced Configuration > DHCP Configuration > Client List".

Interface Description

Client list interface as follows:



The main element configuration description of client list interface:

Interface Element	Description
IP Address	IP address of DHCP client-side device.

Interface Element	Description
MAC Address;	MAC address of DHCP client device.
Start Time	Valid start time of DHCP client.
End Time	Valid end time of DHCP client.
Remaining Time	Valid remaining time of DHCP client.

9.2 DHCP-Snooping Configuration

The function of DHCP Snooping

DHCP Snooping is a security feature of DHCP, which has the following functions:

1 Ensure that clients get IP addresses from legitimate servers.

If there is a pseudo-DHCP server set up privately in the network, it may cause the DHCP client to get the wrong IP address and network configuration parameters, and can't communicate normally. To enable DHCP clients to obtain IP addresses through legitimate DHCP servers, DHCP Snooping security mechanism allows ports to be set as trusted ports and untrusted ports:

- The trust port forwards the received DHCP message normally.
- The untrusted port discards the DHCP-ACK and DHCP-OFFER messages responded by the DHCP server.

The ports connecting DHCP server and other DHCP Snooping devices need to be set as trusted ports, and other ports should be set as untrusted ports, so as to ensure that DHCP clients can only obtain IP addresses from legitimate DHCP servers, while pseudo-DHCP servers erected privately cannot assign IP addresses to DHCP clients.

2 Record the corresponding relationship between IP address and MAC address of DHCP client

DHCP Snooping records DHCP Snooping entries by listening to DHCP-REQUEST messages and DHCP-ACK messages received by trusted ports, including MAC addresses of clients, acquired IP addresses, ports connected with DHCP clients and VLAN to which the ports belong. Using this information, you can achieve:

- ARP Detection: according to the DHCP Snooping table entry, judge whether the user sending ARP message is legal or not, so as to prevent ARP attack by illegal users.
- IP Source Guard: filter the messages forwarded by the port by dynamically obtaining DHCP Snooping entries to prevent illegal messages from passing through the port.

Option 82

Option 82 is called the relay agent information option and records the location information of the DHCP client. When the DHCP relay or DHCP Snooping device receives the request message sent by the DHCP client to the DHCP server, it adds Option 82 to the message and sends it to the DHCP server.

Administrators can obtain location information of DHCP client from Option 82, so as to locate DHCP client and realize control over security and billing of client. Servers that support Option 82 can also make allocation policies for IP addresses and other parameters based on information about that Option, providing a more flexible address allocation scheme.

Option 82 can contain up to 255 sub-option. If Option 82 is defined, define at least one sub-option. Currently, the DHCP relay supports only three sub-options: Sub-Option 1 (Circuit ID, Circuit ID sub-option) and Sub-option 2 (Remote ID, Remote ID sub-option) and sub-option 3 (Subscriber ID, Subscriber ID sub-option).

9.2.1 Global Configuration

Function Description

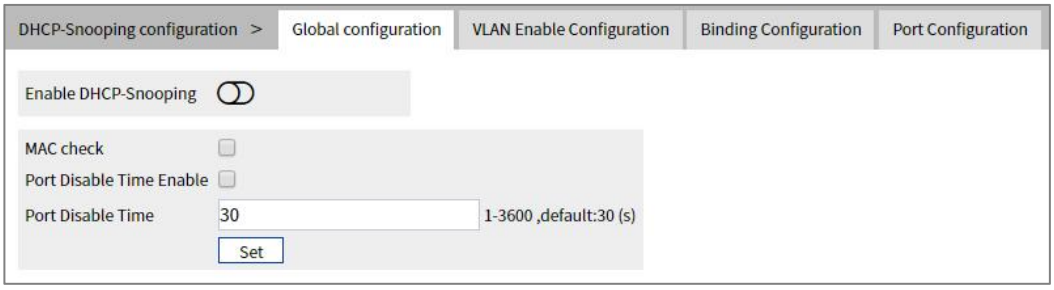
On the “Global Configuration” page, user can enable/disable DHCP Snooping.

Operation Path

Open in order: "Advanced Configuration > DHCP-Snooping Configuration > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Enable DHCP-Snooping	Swipe to the right to enable DHCP-Snooping.
MAC Check	Enable DHCP client MAC address checking.

Interface Element	Description
	Note: Enabling DHCP-Snooping will automatically turn on DHCP client MAC address checking.
Port Disable Time Enable	When the DHCP message rate of a port is lower than the configured rate of the port, the port's port disable duration will be disabled.
Port Disable Time	Port disable time, the input range is 1-3600, the unit is s, and the default is 30s.

9.2.2 VLAN Enable Configuration

Function Description

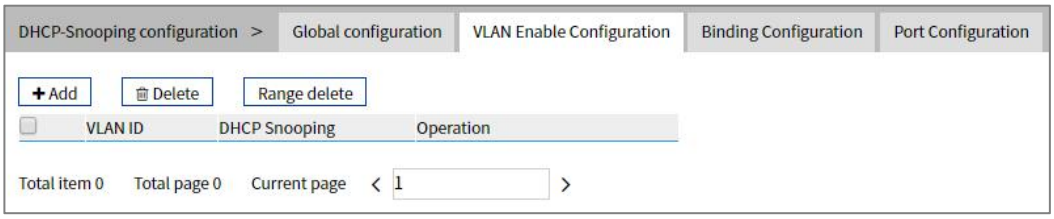
On the "VLAN Enable Configuration" page, user can specify that the VLAN to enable DHCP Snooping.

Operation Path

Open in order: "Advanced Configuration > DHCP-Snooping Configuration > Vlan enable Configuration".

Interface Description

The Vlan enable configuration interface is as follows:



Main elements configuration description of Vlan enabled configuration interface:

Interface Element	Description
VLAN ID	The VLAN number.
DHCP Snooping	Enable status of DHCP Snooping. • enable • disalbe
Operation: delete	Delete the current VLAN enable entry

9.2.3 Binding Configuration

Function Description

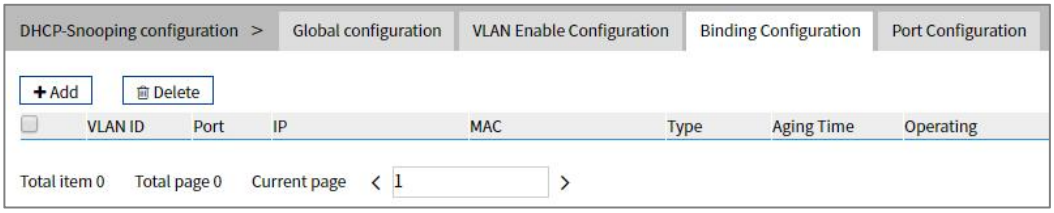
On the Binding Configuration page, user can bind ports, IP addresses and MAC addresses.

Operation Path

Open in order: "Advanced Configuration > DHCP-Snooping Configuration > Binding Configuration".

Interface Description

The binding configuration interface is as follows:



Main elements configuration description of Binding configuration interface:

Interface Element	Description
VLAN ID	Binding VLAN ID information, for example: 1-4096.
Port	The corresponding port name of the device Ethernet port.
IP	Binding IP address, for example: 192.168.1.1.
MAC	Binding MAC address, for example: 0001-0001-0001.
Type	Port type: • Static • Dynamic
Aging Time	Port aging time.
Operation: edit	Modify the port binding information.
Operation: delete	Delete the port binding configuration of the current row.

9.2.4 Port Configuration

Function Description

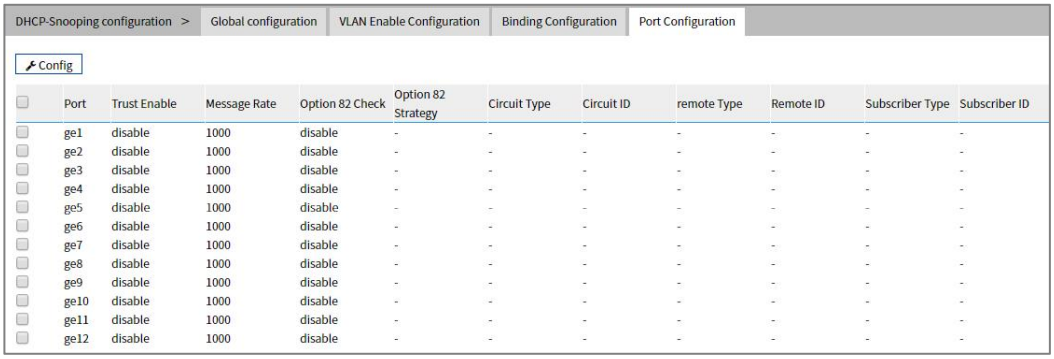
On the port configuration page, user can configure DHCP Snooping port information.

Operation Path

Open in order: "Advanced Configuration > DHCP-Snooping Configuration > Port Configuration".

Interface Description

Check port configuration interface as below:



The main element configuration description of global configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Trust Enable	Port trust enable, and the trust port forwards the received DHCP message normally.
Message Rate	Message transmission speed of port, the input range is 10-1000 (s), and the default value is 1000s.
Option 82 Check	When Option 82 check is turned on, the location information of DHCP client can be obtained from Option 82, so as to locate DHCP client.
Option 82 Strategy	Option 82 dealing strategy, options as follows: • Drop: Discard messages. • Keep: Adopt different modes to fill Option 82, replace prime Option 82 in message and forward, filling modes will be described as below. • Replace: Keep Option 82 in messages unchanged and forward.
Circuit Type	Circuit ID sub-option filling type, options as follows: • Normal: Normal mode; • String: Detailed mode.
Circuit ID	Circuit ID sub-option filling content, support ASCII and HEX mode. Note: • The input length is limited between 2 and 64;

Interface Element	Description
	• When Hex is selected, the input content is a combination of uppercase and lowercase letters and numbers. • When ASCII is selected, the content is not limited.
Remote Type	Remote ID sub-option filling type, options as follows: • Normal: Normal mode; • Sysname: Directly adopt device system name to fill Option 82; • String: Detailed mode.
Remote ID	The filling content of the remote ID sub-option supports ASCII and HEX formats. Note: • The input length is limited between 2 and 64; • When Hex is selected, the input content is a combination of uppercase and lowercase letters and numbers. • When ASCII is selected, the content is not limited.
Subscriber Type	User option fill type, which supports ASCII format.
Subscriber ID	The filling content of Subscriber ID sub-option supports ASCII and HEX formats. Note: • The input length is limited between 2 and 64; • When Hex is selected, the input content is a combination of uppercase and lowercase letters and numbers. • When ASCII is selected, the content is not limited.

9.3 DHCP-Relay Configuration

Function Description

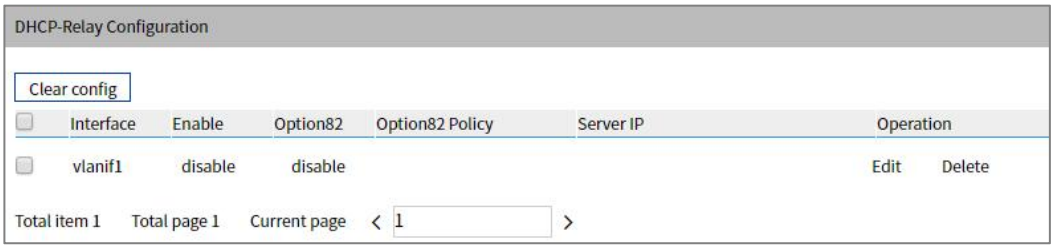
On the "DHCP-Relay Configuration" page, user can configure the relevant parameters of Relay port.

Operation Path

Open in order: "Advanced Configuration > DHCP-Relay Configuration".

Interface Description

DHCP-Relay configuration interface is as follows:



Main element configuration description of DHCP-Relay configuration interface:

Interface Element	Description
Interface	Interface Name.
Enable	Enable switch, options as follows: • Enable: enable the dhcp relay function of the interface; • Disable: disable the dhcp relay function of the interface.
Option82	Option82 function, options as follows: • - Enable: enable the option 82 function of dhcp relay; • - Disable: disable the option 82 function of dhcp relay. Note: When the option82 function is enabled, the relay message sent by relay process would carry option 82.
Option82 policy	The processing strategy of option82 is shown as follows: • untouched • append • discard • replace
Server IP	IP address information of proxy server.
Operation: edit	Click “edit” button to set the parameters of the switch and option82.
Operation: delete	Check Relay interface configuration entry, click “delete” to delete Relay interface configuration.

9.4 LLDP Configuration

LLDP is a layer 2 topology discovery protocol, its basic principle is: Devices in network send the status information message to adjacent device, and each port in the device stores its own information, if there is change in the status of local device, it can also send updated information to the adjacent device directly connected to it. Adjacent devices will store the information in standard SNMP MIB bank. The network management system could inquiry the connection status of current layer 2 from SNMP MIB bank. It should be noted that LLDP is only a remote device status information

discovery protocol, which cannot complete the network device configuration, port control and other functions.

9.4.1 Current configuration

Function Description

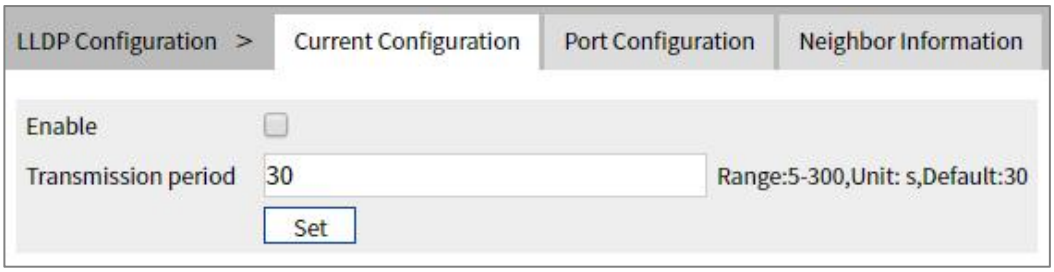
On the "Current Config" page, user can configure the relevant parameters of LLDP.

Operation Path

Open in order: "Advanced Configuration > LLDP Configuration > Current Configuration".

Interface Description

The current configuration interface is as follows:



Main elements configuration description of the current configuration interface:

Interface Element	Description
Enable	The radio box of LLDP function status, check to enable.
Transmission Period	LLDP transmission period, range 5-300, unit: second, default: 30 Note: When no device status changes, the device periodically sends LLDP packets to its adjacent nodes. The interval is called the period for sending LLDP packets.
Set	Click "Set" button to operate.

9.4.2 Port Configuration

Function Description

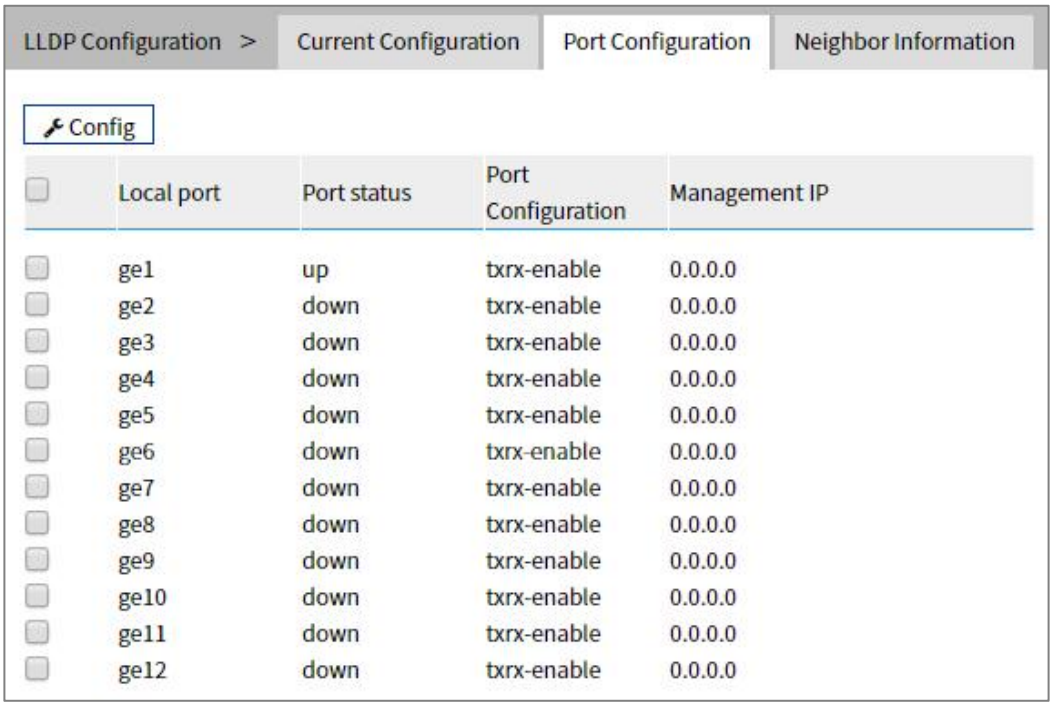
On the "Port Config" page, user can configure the sending and receiving mode and management address of the port.

Operation Path

Open in order: "Advanced Configuration > LLDP Configuration > Port Configuration".

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Local Port	The corresponding port name of the device Ethernet port.
Port Status	The LLDP working modes of device port are as follows: • tx-enable: work mode is Tx, it only transmits LLDP message and not receive it. • rx-enable: work mode is Rx, it only receives LLDP message and not transmit it. • txrx-enable: work mode is TxRx, it transmits LLDP message as well as receive it. • Disable: work mode is Disable, it neither transmits nor receives LLDP message. Note: When global LLDP is enabled, the work mode of LLDP is TxRx by default.
management 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

Interface Element	Description
	address can definitely mark a device, which is beneficial to the drawing of network topology and network management. Management address is encapsulated in Management Address TLV field of LLDP message and sent to adjacent nodes. • The management address released by the port in the LLDP message defaults to the main IP address of the smallest VLAN of the VLANs this port is in. If the VLAN is not configured with a main IP address, it will be 0.0.0.0.

9.4.3 Neighbor Information

Function Description

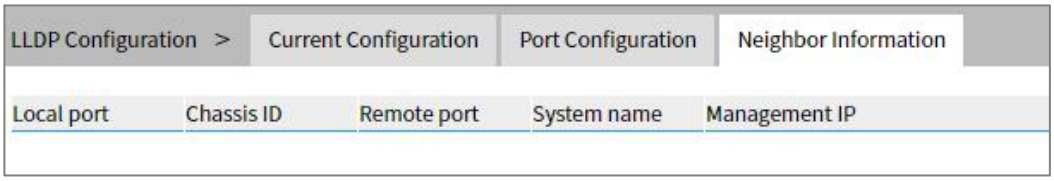
On the "Neighbors Information" page, user can look over the relative information of neighbors.

Operation Path

Open in order: "Advanced Configuration > LLDP Configuration > LLDP Neighbors".

Interface Description

Neighbor information interface as follows:



Main elements configuration description of neighbor information interface:

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

9.5 ACL Configuration

The ACL(Access Control List) is a set composed of one or more rules. Rule refers to the judgment statement describing the message matching condition. These conditions may be the source address, destination address, port number of message. ACL can realize accurate identification and control of message flow in the network, and achieve the purpose of controlling network access behavior, preventing network attacks and improving network bandwidth utilization, thus ensuring the security of network environment and the reliability of network service quality.

9.5.1 Time Range Configuration

Function Description

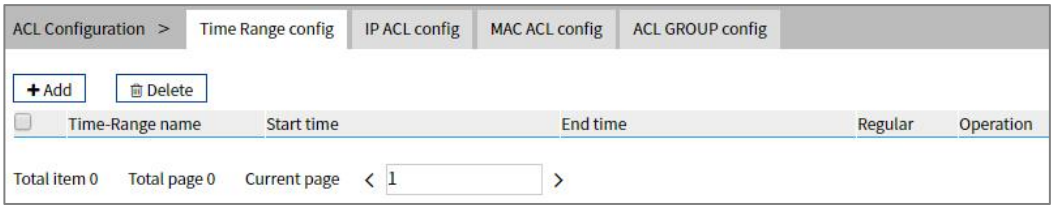
On the “Time Range Configuration” page, you can configure the effective time period of ACL rules.

Operation Path

Open in order: "Advanced Configuration > ACL Configuration > Time Range Configuration".

Interface Description

Time Range configuration interface as follows:



The main element configuration description of Time Range configuration interface:

Interface Element	Description
Add	Click "Add" to add time range entry.
Delete	Check time range entry and click “Delete” button to delete specified entries in batches.
Time-Range Name	The name of the ACL valid time period, which supports absolute time and regular time.
Start Time	The start time of the absolute time or regular time range.
End Time	The end time of the absolute time or regular time range.
Regular	Date of the regular time.

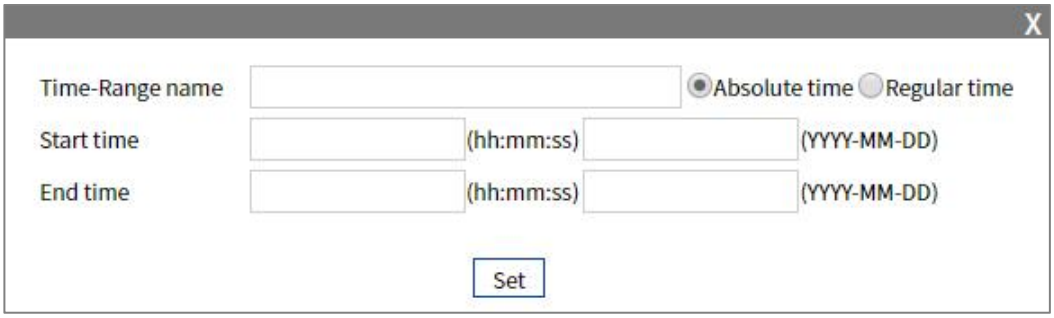
Interface Element	Description
Operation	Delete: Click the "Delete" button to delete the the current entry.

Click “Add” button to add time entry.

In the “Add” interface, check the “Absolute time” radio box.

Interface Description 1: Add-absolute time

The Add-absolute time interface as follows:



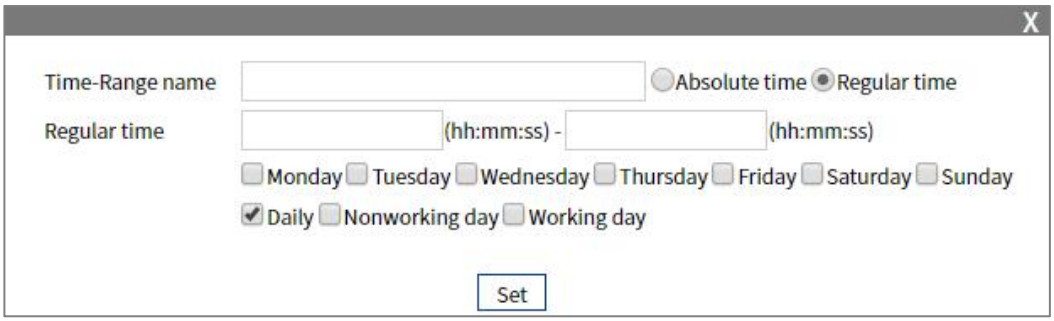
The main elements configuration description of Add-absolute time interface:

Interface Element	Description
Time-Range Name	The name of the ACL effective time period. There are two modes in the effective time period, and the options that can be checked are: • Absolute time: it starts from a certain time on a certain day of a certain year and ends at a certain time on a certain day of a certain year, which means that the rules will take effect within this time range. • Regular time: the time range is defined by taking the week or workday as the parameter, which means that the rule takes effect cyclically with a week cycle (e.g., 8: 00 to 12: 00 every Monday).
Start Time	Start time of absolute time, format: hh:mm:ss (hour:minute:second); YYYY-MM-DD (year-month-day).
End Time	End time of absolute time, format: hh:mm:ss (hour:minute:second); YYYY-MM-DD (year-month-day).

In the “Add” interface, check the “Regular time” radio box.

Interface Description 2: Add-regular time

The Add-regular time interface as follows:



The main elements configuration description of Add-regular time interface:

Interface Element	Description
Time-Range Name	The name of the ACL effective time period. There are two modes in the effective time period, and the options that can be checked are: • Absolute time: it starts from a certain time on a certain day of a certain year and ends at a certain time on a certain day of a certain year, which means that the rules will take effect within this time range. • Regular time: the time range is defined by taking the week or workday as the parameter, which means that the rule takes effect cyclically with a week cycle (e.g., 8: 00 to 12: 00 every Monday).
Regular Time	Time range of regular time, format: hh:mm:ss- hh:mm:ss (Hour:minute:second). Check the week or workday radio box to specify the date to be repeated.

9.5.2 IP ACL Configuration

Function Description

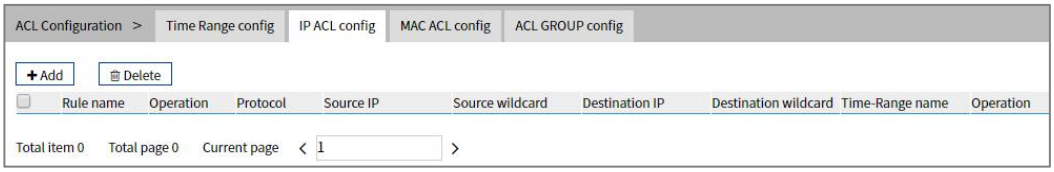
On the "IP ACL Configuration" page, user can configure IP ACL rule. Users can assign numbers to ACLs when creating them, and different numbers correspond to different types of ACLs. At the same time, in order to facilitate memory and identification, users can also create named ACLs, that is, when creating ACLs, set their names.

Operation Path

Open in order: "Advanced Configuration > ACL Configuration > IP ACL Configuration".

Interface Description

IP ACL configuration interface as follows:



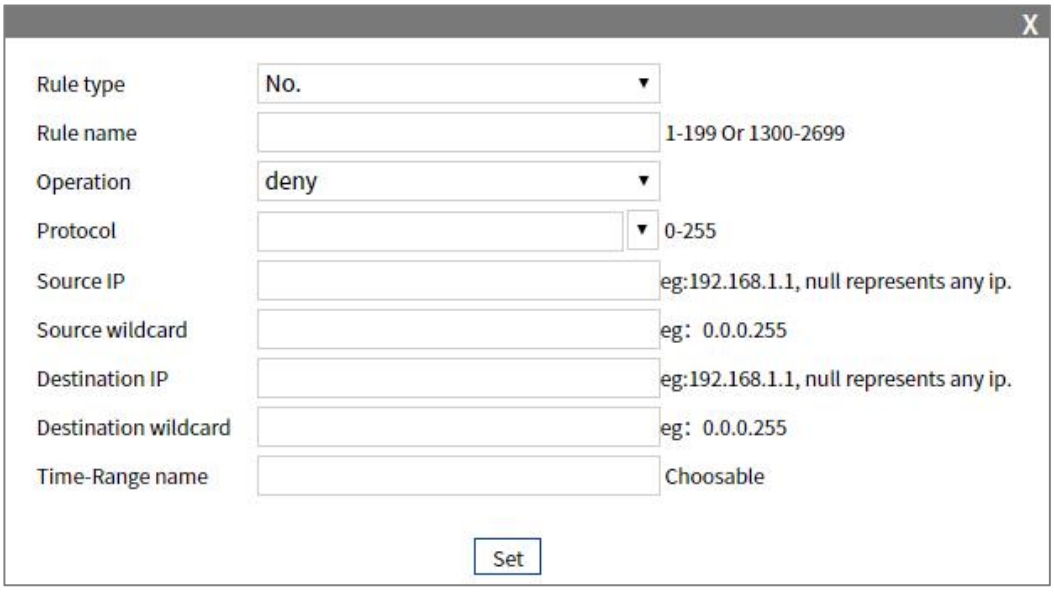
The main element configuration description of IP ACL Configuration interface:

Interface Element	Description
Add	Click "Add" button to add IP ACL rule.
Delete	Check rule entry and click “Delete” button to delete specified entries in batches.
Rule Name	IP ACL rule name or number.
Operation	Action of IP ACL rule: including permit/deny.
Protocol	Protocol type of data packets.
Source IP	Source IP address information of the packet.
Source Wildcard	Source IP address wildcard mask.
Destination IP	Destination IP address information of the packet.
Destination Wildcard	Destination IP address wildcard mask.
Time-Range Name	Effective time period of IP ACL rule.
Operation	Click “Edit” or “Delete” to modify or delete the name of Time-Range.

Click “Add” button to add IP ACL rule entry.

Interface Description: Add

The Add interface as follows:



The main elements configuration description of Add interface:

Interface Element	Description
Rule Type	The drop-down list of IP ACL rule type. The options are: • Name: ACL is identified by name instead of number. • Number: When creating an ACL, specify a unique number to identify the ACL.
Rule Name	IP ACL rule name or number. When the rule type is name, it supports the combination of @, !, _, numbers and letters that does not exceed 16 digits. When the rule type is number, 1-199 or 1300-2699 is supported. Note: • Standard ACL(1-99, 1300-1999): Only the source IP address, fragmentation information and effective time period information of the message are used to define the rule. • Extended ACL (100-199, 2000-2699): both the source IP address of IPv4 message and the destination IP address, protocol type and effective time period can be used to define rules.
Operation	The action drop-down list of ACL rules. The options are: • Permit • Deny
Protocol	The protocol type of extended ACL rules, support filtering messages based on protocol type, and the value range of protocol number is 0-255. You can click the drop-down list of “Protocol” to select an existing agreement name.

Interface Element	Description
Source IP	The source IP address information of the packet, such as 192.168.1.1. No input indicates any IP address.
Source Wildcard	Wildcard mask of source IP address, such as 0.0.0.255. The wildcard mask of IP address is a 32-bit numeric string used to indicate which bits in IP address will be checked. "0" means "check the corresponding bit", and "1" means "do not check the corresponding bit".
Destination IP	The destination IP address information of the packet, such as 192.168.1.1. No input indicates any IP address.
Destination Wildcard	Wildcard mask of destination IP address, such as 0.0.0.255. The wildcard mask of IP address is a 32-bit numeric string used to indicate which bits in IP address will be checked. "0" means "check the corresponding bit", and "1" means "do not check the corresponding bit".
Time-Range Name	The name of the effective time period of the IP ACL rule.
Operation	Click “Edit” or “Delete” to modify or delete the name of Time-Range.

9.5.3 MAC ACL Configuration

Function Description

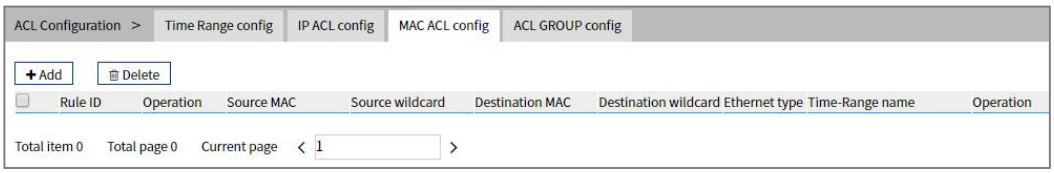
On the “MAC ACL Configuration” page, you can create MAC ACL rules. The layer-2 ACL uses the Ethernet header information of the message to define rules, such as according to the source MAC (Media Access Control) address, destination MAC address, etc.

Operation Path

Open in order: "Advanced Configuration > ACL Configuration > MAC ACL Configuration".

Interface Description

MAC ACL configuration interface as follows:



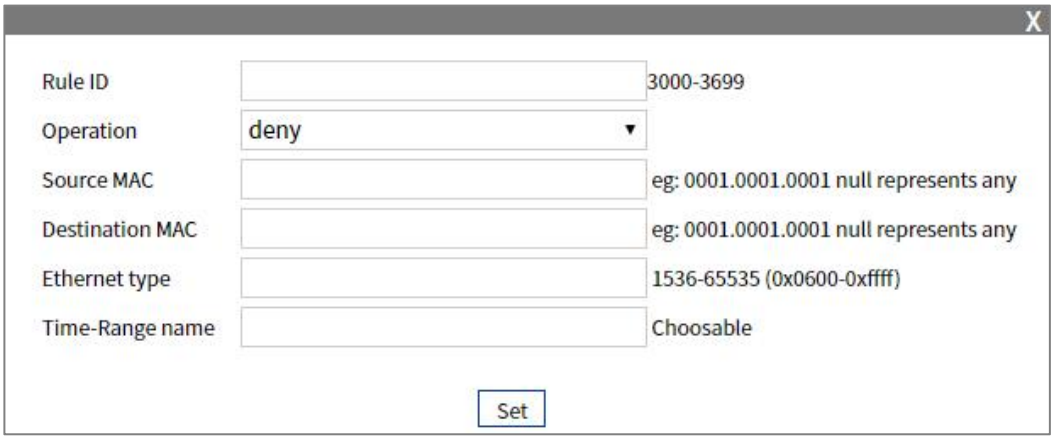
The main element configuration description of MAC ACL configuration interface:

Interface Element	Description
Add	Click "Add" button to add MAC ACL rule.
Delete	Check rule entry and click “Delete” button to delete specified entries in batches.
Rule ID	Mac ACL rule number.
Operation	Action of MAC ACL rule: including permit/deny.
Source MAC	Source MAC address information of the packet.
Source Wildcard	Source MAC address wildcard mask.
Destination MAC	Destination MAC address information of the packet.
Destination Wildcard	Destination MAC address wildcard mask.
Ethernet Type	Ethernet type of packet.
Time-Range Name	Effective time period of MAC ACL rule.
Operation	Click “Edit” or “Delete” to modify or delete the name of Time-Range.

Click the “Add” button to add MAC ACL rule entries.

Interface Description: Add

The Add interface as follows:



The main elements configuration description of Add interface:

Interface Element	Description
Rule ID	MAC ACL rule number, the value range is 3000-3699.
Operation	The action drop-down list of ACL rules. The options are: • Permit • Deny
Source MAC	The source MAC address information of the packet, such as

Interface Element	Description
	0001.0001.0001. No input indicates any MAC address.
Source Wildcard	Wildcard mask of source MAC address, such as 0001.0001.0001. Wildcard mask of MAC address, used to indicate which bits in the MAC address will be checked. "0" means "check the corresponding bit", and "1" means "do not check the corresponding bit".
Destination MAC	The destination MAC address information of the packet, such as 0001.0001.0001. No input indicates any MAC address.
Destination Wildcard	Wildcard mask of destination MAC address, such as 0001.0001.0001. Wildcard mask of MAC address, used to indicate which bits in the MAC address will be checked. "0" means "check the corresponding bit", and "1" means "do not check the corresponding bit".
Ethernet Type	Ethernet type of the packet, value range is 1536-65535 (0x0600-0xffff).
Time-Range Name	The name of the effective time period of the IP ACL rule.
Operation	Click “Edit” or “Delete” to modify or delete the name of Time-Range.

9.5.4 ACL GROUP Configuration

Function Description

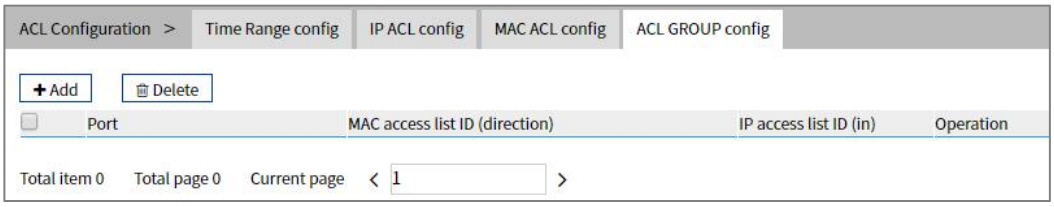
On the “ACL GROUP Configuration” page, you can configure ports to enable IP ACL and MAC ACL rules.

Operation Path

Open in order: "Advanced Configuration > ACL Configuration > ACL GROUP Configuration".

Interface Description

ACL GROUP Configuration interface as follows:



The main element configuration description of ACL GROUP Configuration interface:

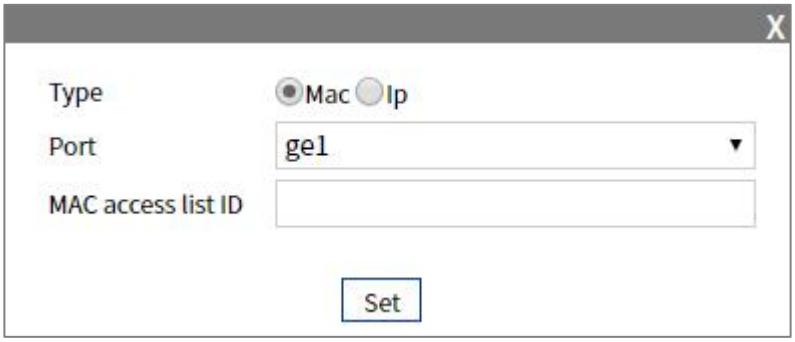
Interface Element	Description
Add	Click "Add" to add port ACL GROUP.
Delete	Check port entry and click “Delete” button to delete specified entries in batches.
Port	The Ethernet port number of the device.
MAC Access List ID (direction)	The port supports MAC ACL rules.
IP Access List ID (in)	The port supports IP ACL rules.
Operation	Click “Edit” or “Delete” to modify or delete the IP / MAC access list ID.

Click the “Add” button to add ACL GROUP.

Check the “Mac” radio box after “Type”.

Interface Description 1: Add-MAC

The Add-MAC interface as follows:



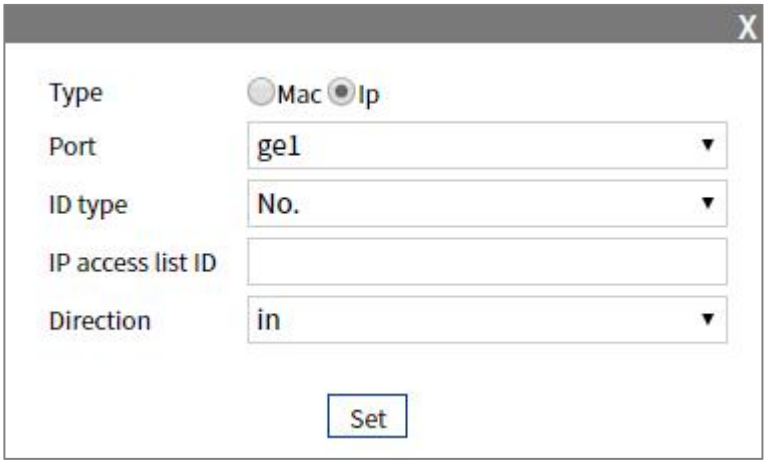
The main elements configuration description of Add-MAC interface:

Interface Element	Description
Type	Radiobox of ACL type, options are as follows: • Mac • IP
Port	Drop down list of Ethernet ports for the device.
MAC Access List ID	The number of the MAC ACL rule.

Check the "IP" radio box after "Type".

Interface Description 2: Add-IP

The Add-IP interface as follows:



The main elements configuration description of Add-IP interface:

Interface Element	Description
Type	Radiobox of ACL type, options are as follows: • Mac • IP
Port	Drop down list of Ethernet ports for the device.
ID Type	The drop-down list of IP ACL rule, options as follows: • NO. • Name
IP Access List ID	The number or name of the IP ACL rule.
Direction	The drop-down list of IP ACL rule filtering direction. The options are: • In: data ingress direction; • Out: data egress direction.

9.6 SNMP Configuration

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.

9.6.1 SNMP Switch

Function Description

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

Operation Path

Open in order: "Advanced Configuration > SNMP Configuration > SNMP Switch".

Interface Description

SNMP switch configuration interface as follows:

The main element configuration description of SNMP switch configuration interface.

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

9.6.2 View

Function Description

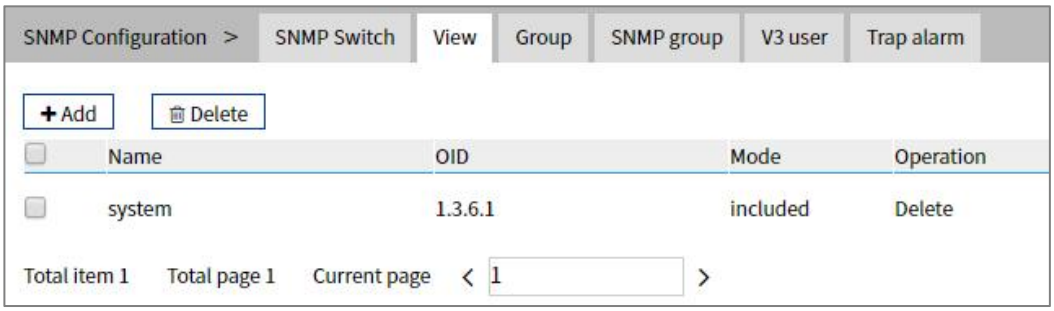
On the "View" page, user can add/delete SNMP view.

Operation Path

Open in order: "Advanced Config > SNMP Config > View".

Interface Description

View interface as below:



The main element configuration description of view interface:

Interface Element	Description
Name	SNMP view name definition, support 32 characters input. Notice: Name can't be empty or contain "&", ";", ", "\" or "/".
OID	Node location information of MIB tree where the device resides. Note: • OID object identifier, a component node of MIB, uniquely identified by a string of numbers that represent the path. • The information of OID could be viewed via the third-party software MG-SOFT MIB Browser.
Mode	Node OID dealing method, options as below: • Included: It contains all objects under the node subtree; • Excluded: Eliminate all objects beyond the node subtree.
Operation	Check the entry and click the "Delete" button to delete it.

9.6.3 Community

Function Description

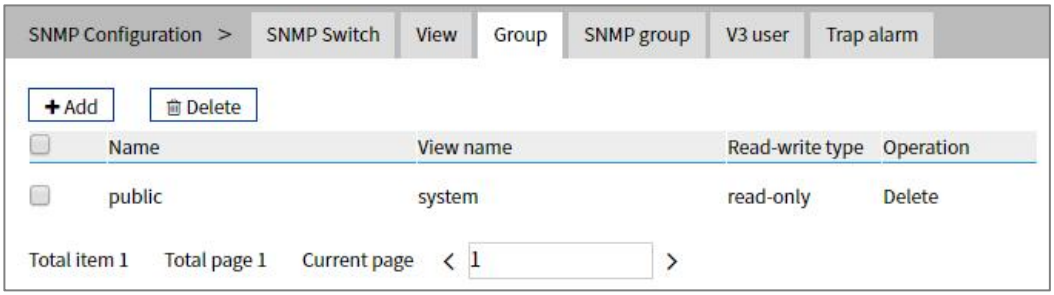
On the "Community" page, user can add/delete SNMP community. Define MIB view that community name can access, set MIB object access privilege of community name as read-write privilege or read-only privilege.

Operation Path

Open in order: "Advanced Config > SNMP Config > Community".

Interface Description

Community interface as below:



The main element configuration description of community interface:

Interface Element	Description
Name	Group name, including numbers or letters, with a length of no more than 32 characters.
View Name	SNMP view name definition, which has been configured in the View page.
Read-write Type	Read-write privilege view name selection, options:. • Read only • Read and write
Operation	You can check this item and click the "Delete" button to delete it.

9.6.4 SNMP Group

Function Description

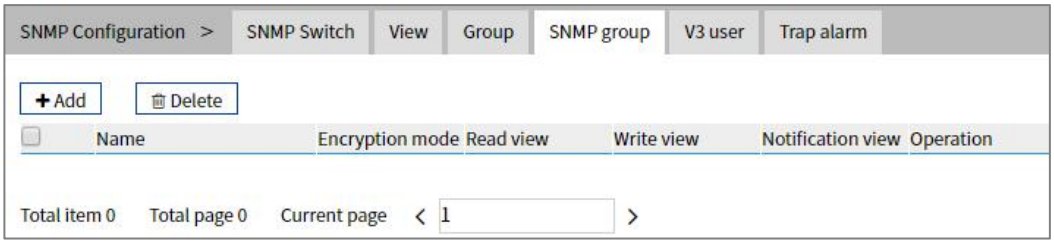
On the “SNMP Group” page, user can configure a new SNMP group and set the secure mode and corresponding SNMP view of the SNMP group.

Operation Path

Open in order: "Advanced Configuration > SNMP Configuration > SNMP Group".

Interface Description

SNMP Group interface as follows:



Main elements configuration description of SNMP Group interface:

Interface Element	Description
Name	SNMP group name, ranging from 1 to 32 bytes.
Encryption Mode	Whether to authenticate and encrypt the message, values: • auth: indicates that the message is authenticated but not encrypted; • noauth: indicates that the message is neither authenticated nor encrypted; • priv: indicates that the message is authenticated and encrypted.
Read View	Specify the read view of the group. Note: The view must be configured in the View interface.
Write View	Specify the write and read view of the group Note: The view can be matched or not. To configure, the view must be configured by the View interface.
Notification View	Specify the notification view of the group. Note: The view can be matched or not. To configure, the view must be the view configured in the View interface.
Operation	You can check this item and click the "Delete" button to delete it.

9.6.5 V3 User

Function Description

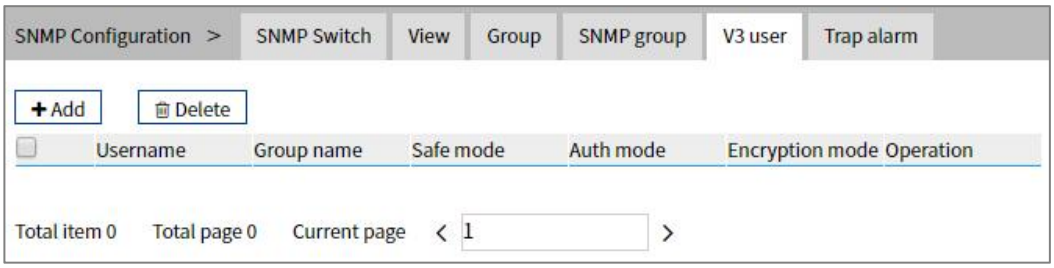
SNMPv3 adopts User-Based Security Model (USM) authentication mechanism. Network manager can configure authentication and encryption function. Authentication is used to verify the validity of the packet sender and prevent unauthorized users from accessing it. Encryption encrypts the transmission packet 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: " Advanced Config > SNMP Config > V3 User".

Interface Description

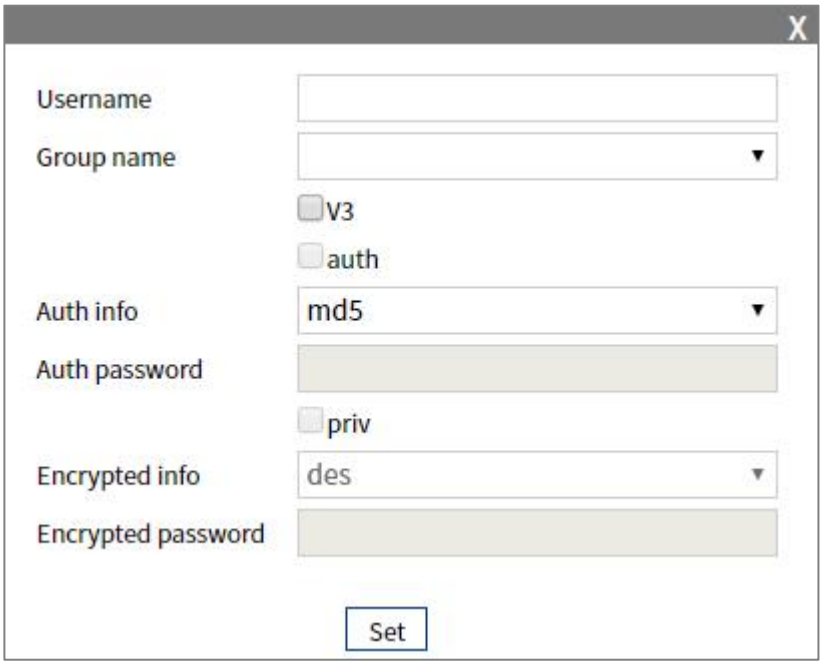
V3 user interface as follows:



The main element configuration description of V3 user interface:

Interface Element	Description
Username	SNMP v3 user name definition, can only contain numbers, letters, or @_! , no longer than 32 characters.
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.
Safe 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.
Auth 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.
Operation	You can check this item and click the "Delete" button to delete it.

V3 User: “Add” Interface Description



The main element configuration description of V3 user “add” interface:

Interface Element	Description
Username	SNMP v3 user name definition, can only contain numbers, letters, or @_! , no longer than 32 characters.
Group Name	The drop-down list of SNMP group name.
V3	It refers to SNMP V3 version user, and defaults to V1 version user.
auth	Indicate that security mode requires authentication. If do not check this parameter, the default is no authentication, no encryption mode.
Auth Info	Authentication information type, acceptable values: • Md5: Information abstract algorithm 5; • Sha: Secure hash algorithm.
Auth Password	Authentication password, character string, length greater than or equal to 8 bytes.
priv	Indicate that security mode requires encryption.
Encrypted info	V3 user data encryption algorithm, options as follows: • Des: Adopt data encryption algorithm; • Aes: Adopt advanced encryption standard.
Encrypted Password	Encrypted password, character string, length greater than or equal to 8 bytes.

9.6.6 Trap Alarm

Function Description

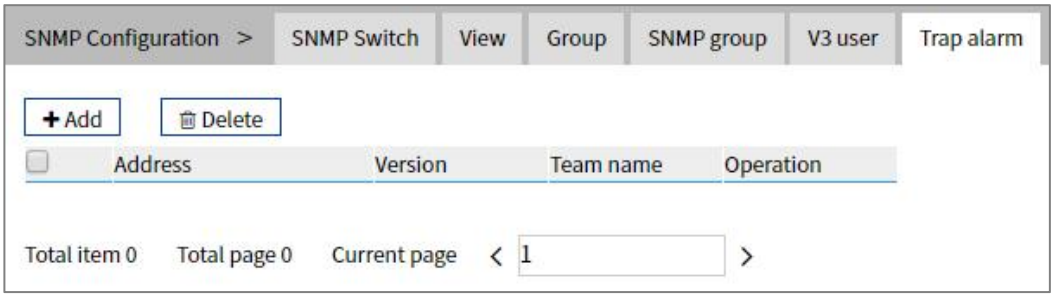
Base on TCP/IP protocol, SNMP usually adopts UDP port 161 (SNMP) and 162 (SNMP-traps), SNMP protocol agent exists in the network device and adopts information specific to the device (MIBs) as the device interface; these network devices can be monitored or controlled via Agent. When a trap event occurs,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

Operation Path

Open in order: "Advanced Config > SNMP Config > Trap Alarm".

Interface Description

Trap alarm interface as below:



The main element configuration description of Trap alarm interface:

Interface Element	Description
Address	IP address of SNMP management device, used for receiving alarm information, such as PC.
Version	SNMP management device version, options as below: • v1; • v2c; Note: V3 is not supported temporarily.
Team Name	Community name or snmpv3 user name.
Operation	You can check this item and click the "Delete" button to delete it.

9.7 RMON Configuration

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.

9.7.1 Event

Function Description

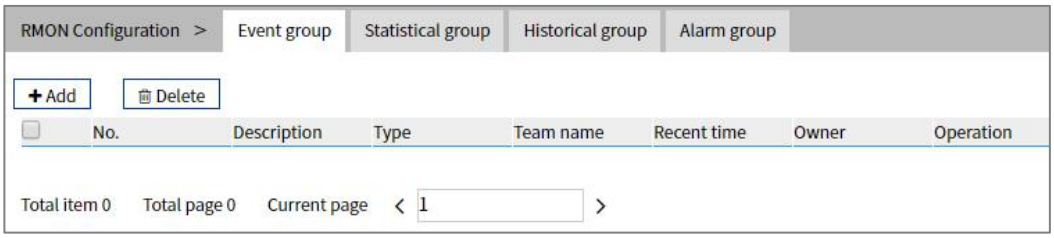
On the "Event" page, user can add, delete or check the configuration information of event.

Operation Path

Open in order: "Advanced Config > RMON Config > Event".

Interface Description

Event group interface 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.

Interface Element	Description
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.
Recent Time	The time of the last incident occurred.
Owner	The creator of the table entry.
Operation	Check the entry and click the "Delete" button to delete it.

9.7.2 Statistical

Function Description

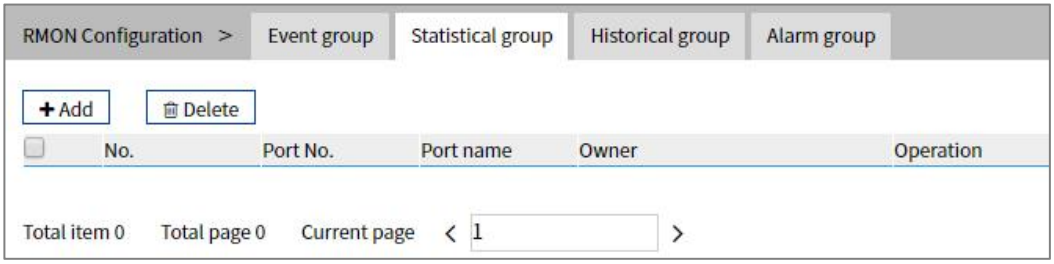
On the "Statistical" page, user can add, delete or check the configuration information of statistical.

Operation Path

Open in order: "Advanced Config > RMON Config > Statistical".

Interface Description

Statistical group interface 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 Element	Description
	interface serial number set before, previous configuration will be replaced.
Port No.	The counted port serial number.
Port Name	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.

9.7.3 History

Function Description

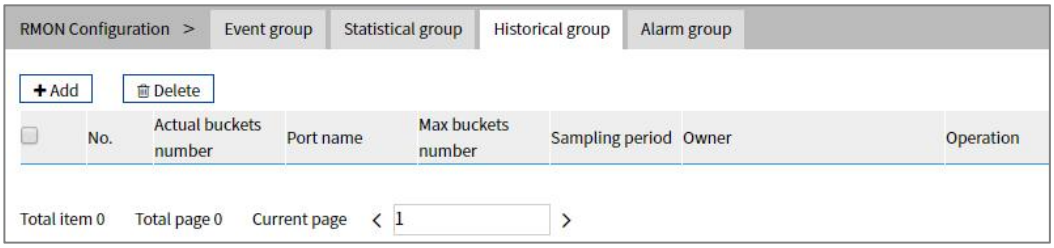
On the "History" page, user can add, delete or check the configuration information of history.

Operation Path

Open in order: "Advanced Config > RMON Config > History".

Interface Description

Historical group interface 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 Buckets Number	Set the historical statistics capacity corresponding to the history group, ranging from 1-65535.
Port Name	The recorded port name.
Max Buckets Number	Maximum capacity of historical statistics table supported by device.

Interface Element	Description
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.

9.7.4 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;

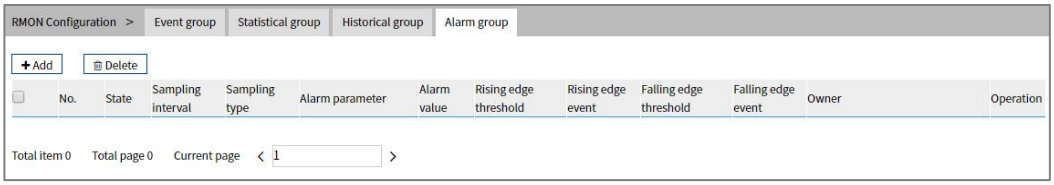
- When monitoring MIB object reaches or surpasses the rising threshold value, it will trigger corresponding event of rising event index;
- When monitoring MIB object reaches or surpasses declining threshold value, it will trigger corresponding event of declining event index;

Operation Path

Open in order: "Advanced Config > SNMP Config > Alarm Group".

Interface Description

Alarm group interface 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 as follows:

Interface Element	Description
	• 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 threshold value during each sampling, an alarm is triggered.
Alarm Parameters	The monitored MIB node supports string format instead of oid format.
Alarm Value	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 Threshold	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.
Owner	The creator of the table entry.
Operation	Check the entry and click the "Delete" button to delete it.

9.8 NTP Configuration

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

Function Description

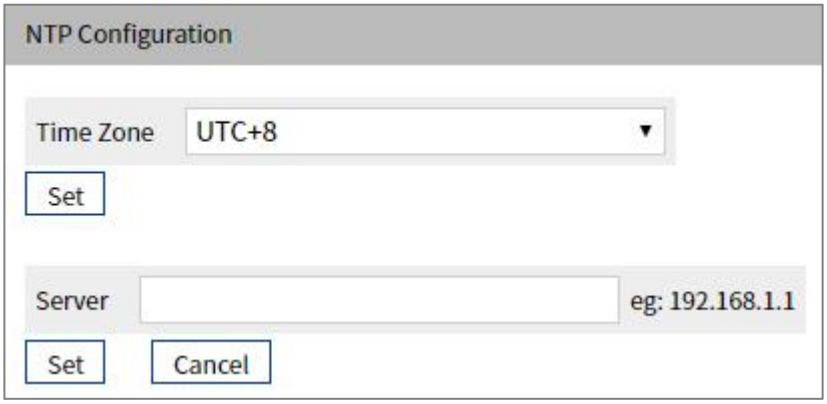
On the "NTP Config" page, user can configure the device time and NTP server information.

Operation Path

Open in order: "Advanced Configuration > NTP Configuration".

Interface Description

NTP configuration interface as follows:



The main element configuration description of NTP configuration interface:

Interface Element	Description
Time Zone	UTC(Universal Time Coordinated) time zone.
Server	IP address of NTP server, for example: 192.168.1.1. Note: As NTP client, the system will synchronize time with NTP server every 11 minutes.

10 System Maintenance

10.1 Configure File Management

10.1.1 Global Configuration

Function Description

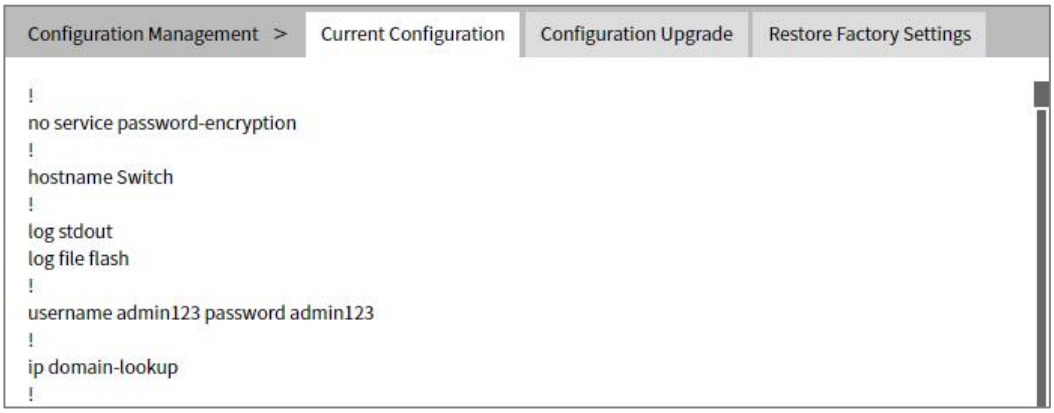
On the "Current Configuration" page, user can view current configuration information.

Operation Path

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

Interface Description

Global configuration interface is as follows:



10.1.2 Configuration File Update

Function Description

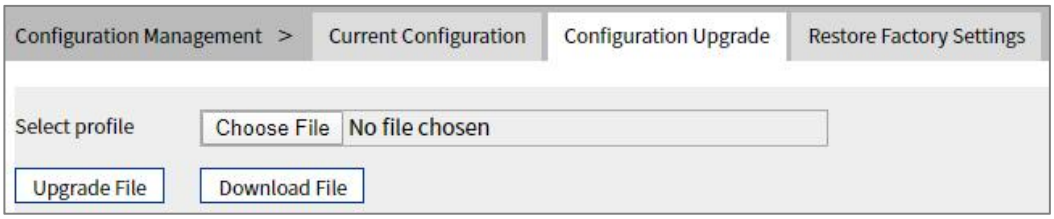
On the "Management File" page, user can download and upload configuration file.

Operation Path

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

Interface Description

Configuration file upgrade interface as follows:



The main element configuration description of configuration file upgrade interface:

Interface Element	Description
Choose Profile	Locally uploading configuration file path, click "Select File" to select required configuration file.
Upgrade File	Upload local configuration file, format: .conf.
Download File	Download the configuration file of current device, format: .conf.

10.1.3 Restore Factory Settings

Function Description

On the "Restore Factory Settings" page, user can restore the device to default setting.

Operation Path

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

Interface Description

Restore Factory Settings interface is as follows:

The main element configuration description of restore factory settings interface:

Interface Element	Description
Restore Factory Settings	Click the button to confirm, the device will lose all existing configuration and restore to default setting.

10.2 Alarm Configuration

10.2.1 Port Alarm

Function Description

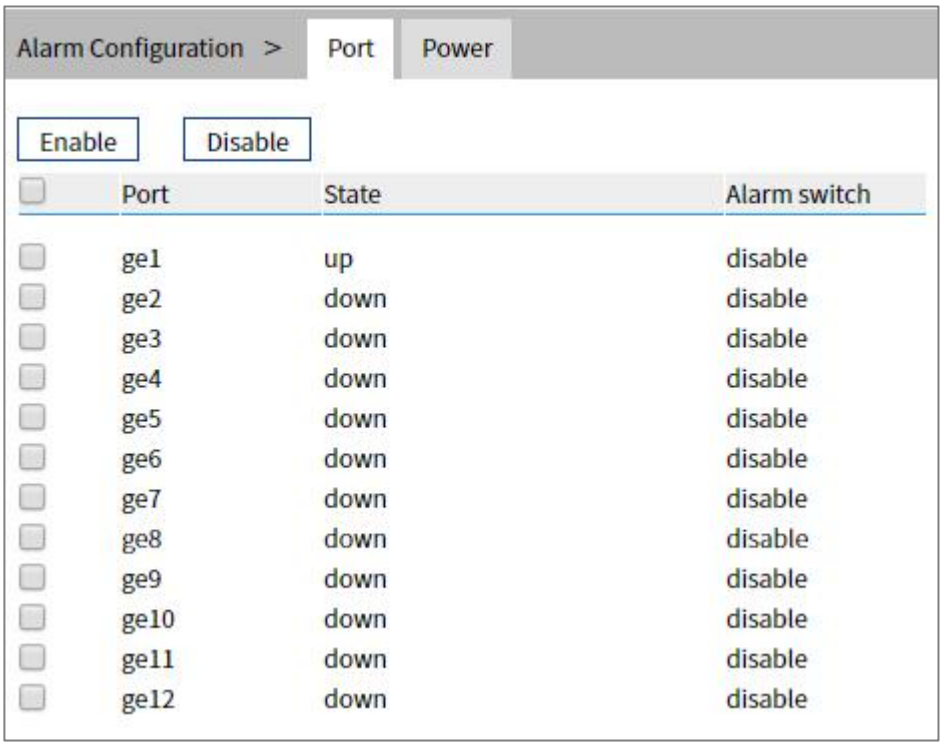
On the “Port” page, user can configure the port alarm function. When the device port is in an abnormal state, the administrator can be informed in time, and the device state can be quickly repaired to avoid excessive loss.

Operation Path

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

Interface Description

Port alarm interface as below:



The main element configuration description of global configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
State	Port link status, display items as follows: • up; • down.
Alarm Switch	Port alarm function status, options as follows: • Enable; • Disable.
Enable	Check the port that needs to enable port alarm, and click enable to enable this function. Note: After enable port alarm, when port occurs abnormal status, such as connection break down, the device will output a signal to hint the abnormal operation of device.
Disable	Check the port that needs to disable port alarm, and click disable to disable this function.

10.2.2 Power Alarm

Function Description

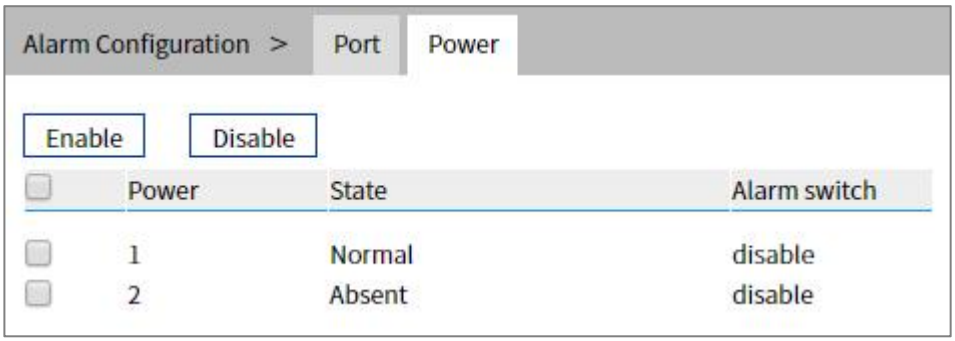
On the “Power Alarm” page, user can configure the alarm functions of the power supply.

Operation Path

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

Interface Description

Power alarm interface as below:



Main elements configuration description of power alarm interface:

Interface Element	Description
Power	The corresponding name of this device’s power supply

Interface Element	Description
State	Device power link status, display items as follows: • Normal; • Absent.
Alarm Switch	Port alarm function status, options as follows: • Enable; • Disable.
Enable	Check the port that needs to enable power alarm, and click enable to enable this function.
Disable	Check the port that needs to disable power alarm, and click disable to disable this function.

10.3 Upgrade

Function Description

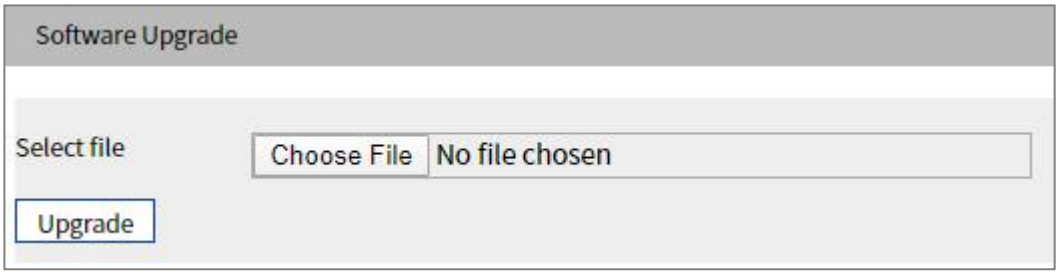
On the "Software Upgrade" page, user can update and upgrade the device procedure via TFTP server.

Operation Path

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

Interface Description

The software update interface as follows:



The main elements configuration description of software update interface:

Interface Element	Description
Select File	Choose upgrade file, format “.bin”. Supports WEB pages and software feature upgrades.

10.4 Log Information

10.4.1 Log Information

Function Description

On the page of “Log information”, user can 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.

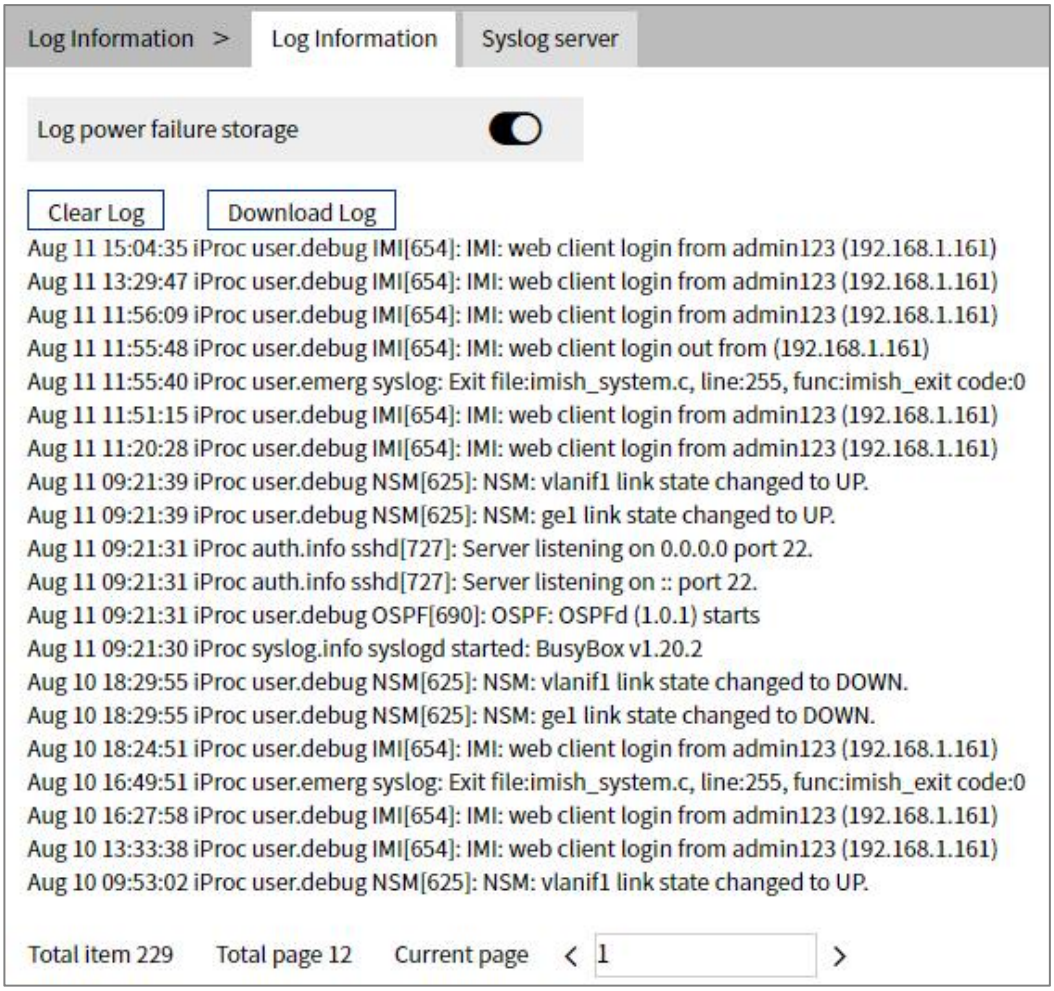
- User log: records user operations and system operation information.
- Security log: records information including account management, protocol, anti-attack and status.
- Diagnostic log: records information that assists in problem identification.

Operation Path

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

Interface Description

Log information interface as follow:



Main elements configuration description of log information interface:

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

10.4.2 Syslog Server

Function Description

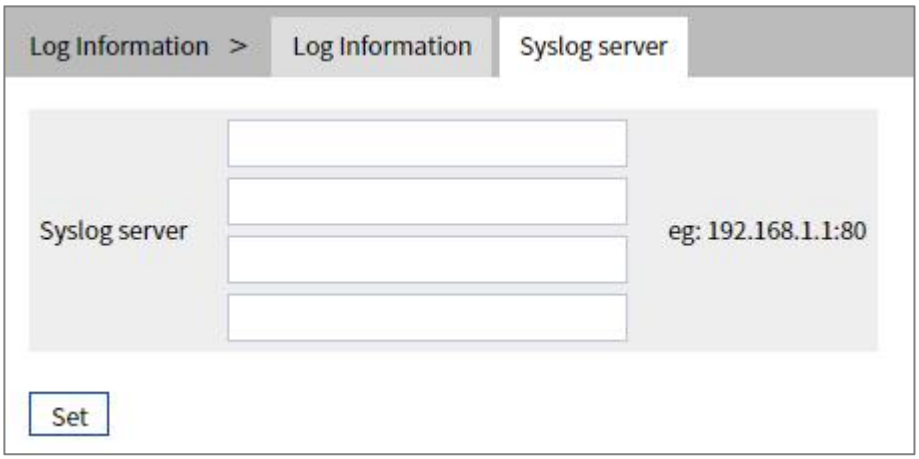
On the "Syslog server" page, user can configure the Syslog server IP address, and the system log information can be sent to the configured syslog server.

Operation Path

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

Interface Description

The Syslog server interface as follows:



Syslog server interface main elements configuration instructions:

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

The Second Part: Frequently Asked Questions

11 FAQ

11.1 Sign in Problems

1. **Why the web page display abnormally when browsing the configuration via WEB?**
   Before accessing the WEB, please eliminate IE cache buffer and cookies. Otherwise, the web page will display abnormally.

2. **What should I do if I forget my login password?**
   For forgetting the login password, the password can be initialized by restoring factory setting, specific method is adopt network management software to search and use restore factory setting function to initialize the password. Both of the initial user name and password are "admin123".

3. **Is configuring via WEB browser same to configuring via BlueEyes_Ⅱ software?**
   Both configurations are the same, without conflict.

11.2 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. **What's the difference between RING V2 and RING V3?**
   RING V2 and RING V3 are our company's ring patents. RING V2 only supports single ring and coupling ring. RING V3 supports single ring, coupling ring, chain and Dual_homing, and Hello_Time can be set to detect port connection status.

3. **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.

4. **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 from high to low, connect automatically in supported highest speed.

11.3 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. **Why is the Link/Act indicator off?**

   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.