TNS5800 Series (12 Ports)

Layer 3 Industrial Ethernet Switch for Rail Transit

User Manual

Version 03

Issue Date: 06/09/2022

Industrial Ethernet communication solution experts **3onedata Co., Ltd.**

Copyright © 2022 3onedata Co., Ltd. All rights reserved.

No company or individual is allowed to duplicate or transmit this manual in any forms without written permission issued by 3onedata Co., Ltd.

Trademark statement

3onedata, 3onedata and 3One data® are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Note

Purchased product, service or features should be constrained by 3onedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.

3onedata

Please scan our QR code for more details

Embedded Industrial Ethernet Switch Modules

Embedded Serial Device Server Modules

Industry-specialized Products
(Rail Transit, Power, Smart City, Pipe Gallery…)

3onedata
Make network communication more reliable

Honor·Quality·Service

Layer 2 (Unmanaged) Managed Industrial Ethernet Switch

Layer 3 Managed Industrial Ethernet Switch

Industrial PoE Switch

BlueEyes pro

BlueEyes Pro Management Software

VSP Virtual Serial Port Management Software

SNMP Management Software

Modbus Gateway

Serial Device Server

Media Converter

CAN Device Server

Interface Converter

Industrial Wireless Products

3onedata Co., Ltd.

Headquart	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District,
Technolog	tech-support@3onedata.com
Service	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86-0755-26703485
Website:	http://www.3onedata.com

Preface

Layer 3 Industrial Ethernet Switch User Manual has introduced this switch:

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

Note

The screenshot reference model of this manual is 8 100M M12 + 4 Gigabit Bypass M12, 110VDC power supply, except the supported Ethernet port and power supply number and type, its interface function and operation is same to other models products.

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 paths are 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	2021-03-16	Document format changes
03	2022-06-09	Document maintenance

Contents

Part One: Operation

1 Log in the Web Interface

1.1WEB 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 • Windows 7 • Windows 10

1.2Set the IP ddress of the Computer

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.

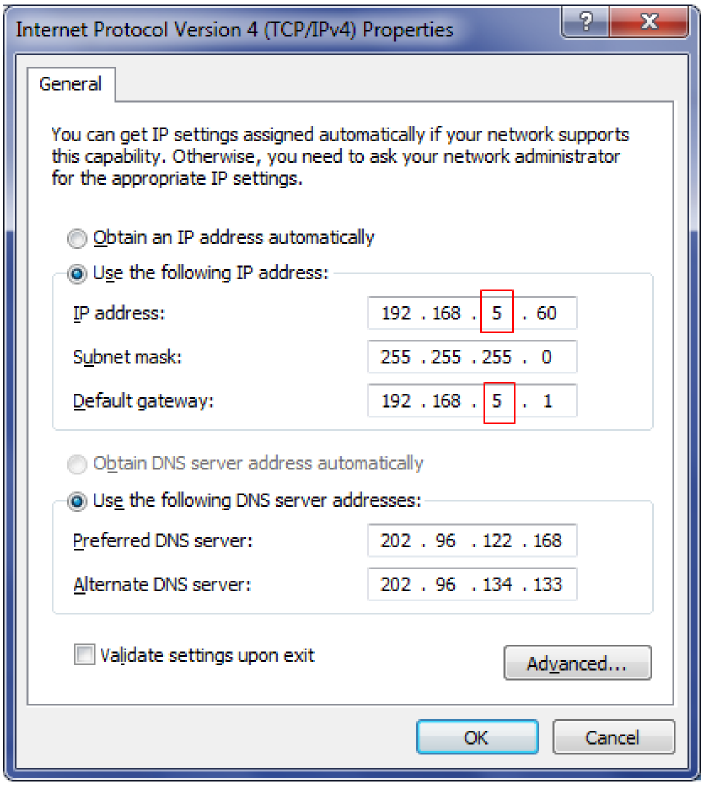
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

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".



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 5 . 60

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 5 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 202 . 96 . 122 . 168

Alternate DNS server: 202 . 96 . 134 . 133

□ Validate settings upon exit

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

Step 4 End.

1.3 Log in the Web Configuration Interface

Operation Steps

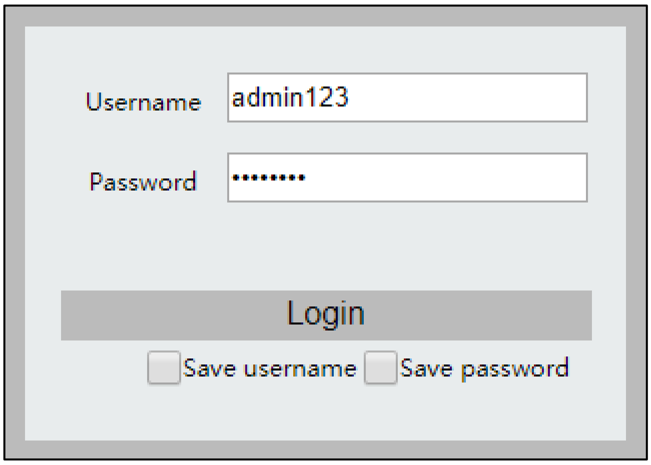
Login in the web configuration interface as follow:

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.



Username admin123

Password ••••••••

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

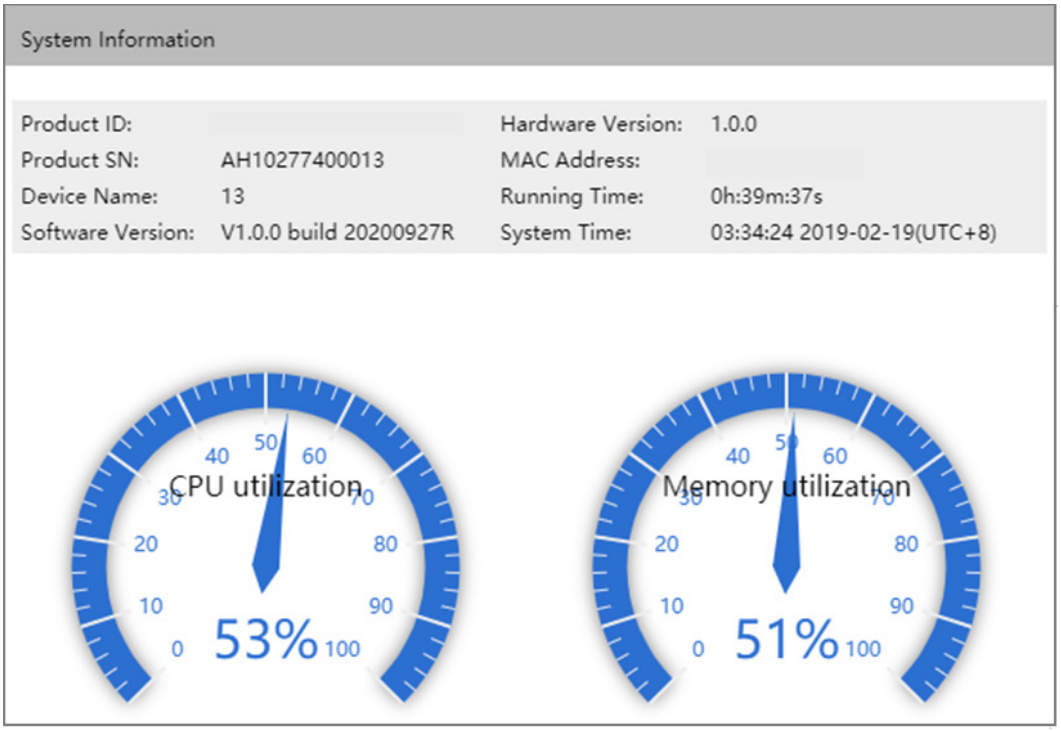
In "System Information" page, user can check "Device Information".

Operation Path

Open: “System Information”.

Interface Description

System information interface as follows:



System Information

Product ID:		Hardware Version:	1.0.0
Product SN:	AH10277400013	MAC Address:	
Device Name:	13	Running Time:	0h:39m:37s
Software Version:	V1.0.0 build 20200927R	System Time:	03:34:24 2019-02-19(UTC+8)

The main element configuration description of state information interface:

Interface Element	Description
CPU Utilization	CPU usage of the current device.
Memory Utilization	Memory usage of the current device.

Interface Element	Description
Product ID	The batch number used by the device to facilitate the management of device tags.
Hardware Version	Current hardware version information, pay attention to the hardware version limits in software version.
Product SN	Product SN
MAC Address	Hardware address of device factory configuration.
Device name	Network identity used by the device.
Running time	Running time of the current device.
Software Version	Current software version information, updated software version with more features.
System Time	Current time information. Users can specify the time zone and server in “NTP Configuration”.

3 System Configuration

3.1 IP Address Configuration

Function Description

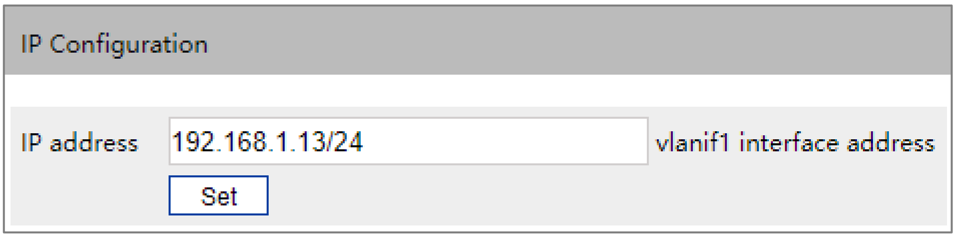
On the “IP Address Configuration” page, users can modify the IP address and subnet mask information of the device.

Operation Path

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

Interface Description

IP address configuration interface is as follow:



IP address: 192.168.1.13/24 vlanif1 interface address

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

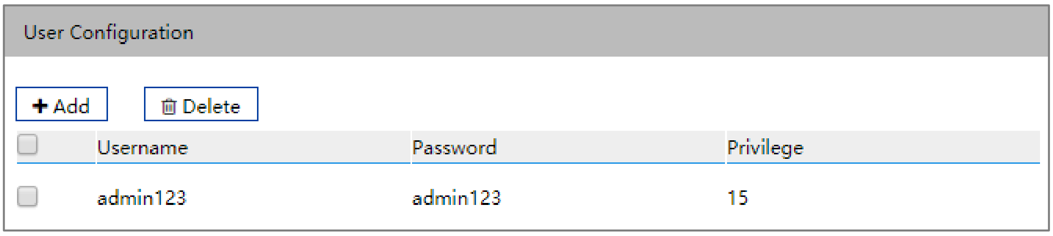
On the "User Config" page, user is free to add and delete username, user needs to enter username and password to access the device, the initial username and password are: admin123.

Operation Path

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

Interface Description

User configuration interface as follows:



User Configuration

□	Username	Password	Privilege
□	admin123	admin123	15

The main elements configuration description of user configuration interface:

Interface Element	Description
Username	Identification of the visitor. Note: Password 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	The visitor's privilege is 0-15, and it supports 16 priorities in 4 categories. • 0: visit level: user can only check device version information and some simple configuration. • 1: check level; user can check device configuration information without modifying it. • 2: configuration level; user can check and configure device information. But cannot manage devices. • 3-15: manage level, user has all privileges of the device, including downloading, uploading, rebooting, modifying device information and other operations. • The username and password length are limited to 32 characters.

3.3 Network Diagnosis

3.3.1 Ping

Function Description

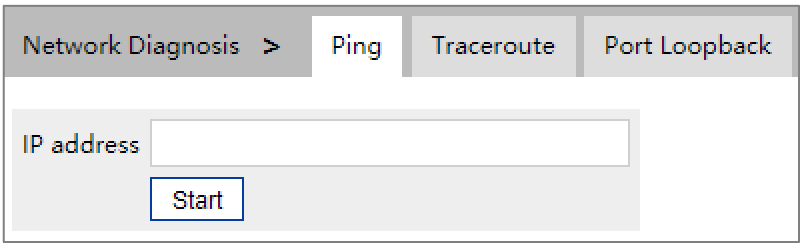
On the "Ping" page, Ping is used to check whether the network is open or network connection speed. Ping utilizes the uniqueness of network machine IP address to send a data packet to the target IP address, and then ask the other side to return a similarly sized packet to determine whether two network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

Operation Path

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

Interface Description

Ping information interface as follows:



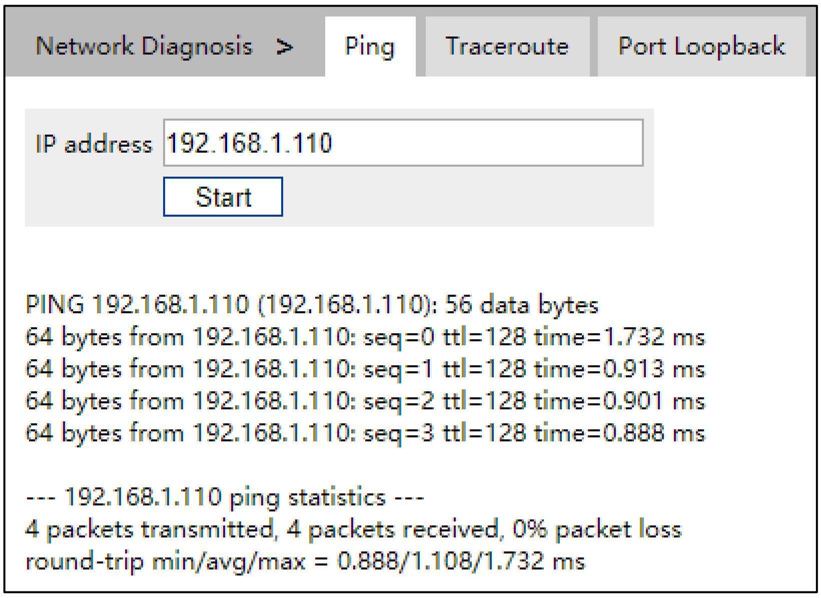
The main elements configuration description of Ping configuration interface:

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;



IP address 192.168.1.110

```
PING 192.168.1.110 (192.168.1.110): 56 data bytes
64 bytes from 192.168.1.110: seq=0 ttl=128 time=1.732 ms
64 bytes from 192.168.1.110: seq=1 ttl=128 time=0.913 ms
64 bytes from 192.168.1.110: seq=2 ttl=128 time=0.901 ms
64 bytes from 192.168.1.110: seq=3 ttl=128 time=0.888 ms

--- 192.168.1.110 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.888/1.108/1.732 ms
```

Step 3 End.

3.3.2 Traceroute

Function Description

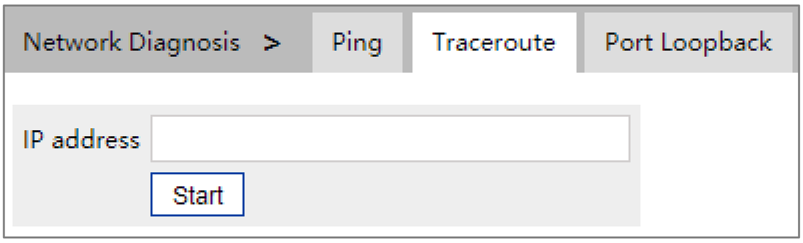
In the "Traceroute" page, users can test the network situation between the switch and the target host. Traceroute measures how long it takes by sending small packets to the destination device until they return. Each device on a path Traceroute returns three test results. Output result includes each test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

Operation Path

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

Interface Description

TRACEROUTE interface as follows:



The main element configuration description of Traceroute interfaces:

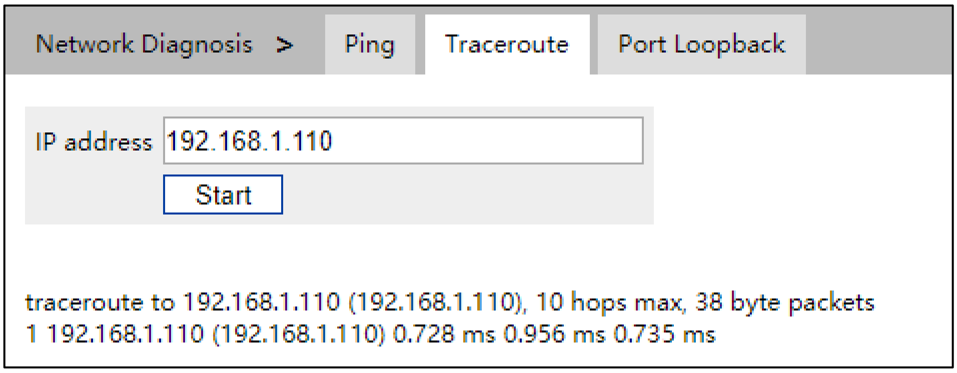
Interface Element	Description
IP Address	IP address of the destination device, fill in the IP address of

Interface Element	Description
	the opposite device that needs to be detected.

TRACEROUTE Configuration:

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

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



IP address 192.168.1.110

```
traceroute to 192.168.1.110 (192.168.1.110), 10 hops max, 38 byte packets
1 192.168.1.110 (192.168.1.110) 0.728 ms 0.956 ms 0.735 ms
```

Note:

The picture above shows the time that the device takes to get to IP address 192.168.1.188, it needs up to 30 hops and 38 bytes' data packet. The returned Traceroute time is 1.066ms and 0.853ms.

Step 3 End.

3.3.3 Port Loopback

Function Description

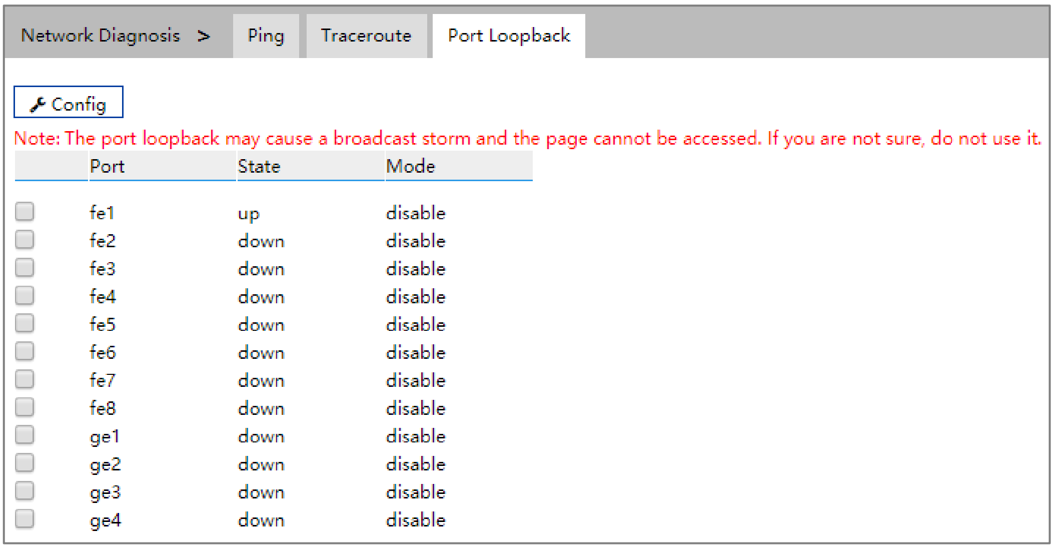
On "Port Loopback" page, user can measure the loopback situation of the switch port PHY or MAC for the convenience of troubleshooting. Port loopback is a common method for the maintenance and troubleshooting of communication port line. Connect the sending end of tested device or line to its receiving 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:



Note: The port loopback may cause a broadcast storm and the page cannot be accessed. If you are not sure, do not use it.

	Port	State	Mode
□	fe1	up	disable
□	fe2	down	disable
□	fe3	down	disable
□	fe4	down	disable
□	fe5	down	disable
□	fe6	down	disable
□	fe7	down	disable
□	fe8	down	disable
□	ge1	down	disable
□	ge2	down	disable
□	ge3	down	disable
□	ge4	down	disable

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.
Status	Display the connection status of the current port.
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

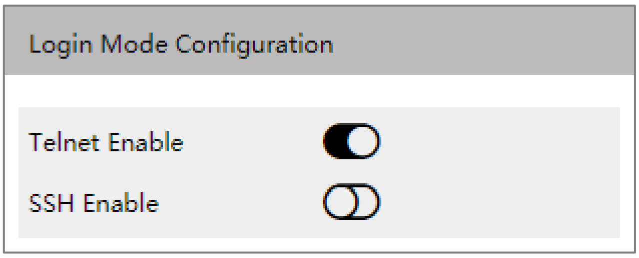
On the “Login Mode Configuration” page, TELNET service and SSH service of the device can be enabled. The CLI interface of the device can be accessed through TELNET protocol and SSH2.0 protocol. TELNET transmission process uses TCP protocol for plaintext transmission, and SSH (Secure Shell) protocol provides secure remote login, ensuring the safe transmission of data.

Operation Path

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

Interface Description

Login mode configuration interface as follow:



Login Mode Configuration

Telnet Enable ●

SSH Enable ○

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.

Note

For TELNET and SSH login methods, please refer to the section "1.2 login switch" in the CLI command line manual.

4 Port Configuration

4.1 Port Settings

Function Description

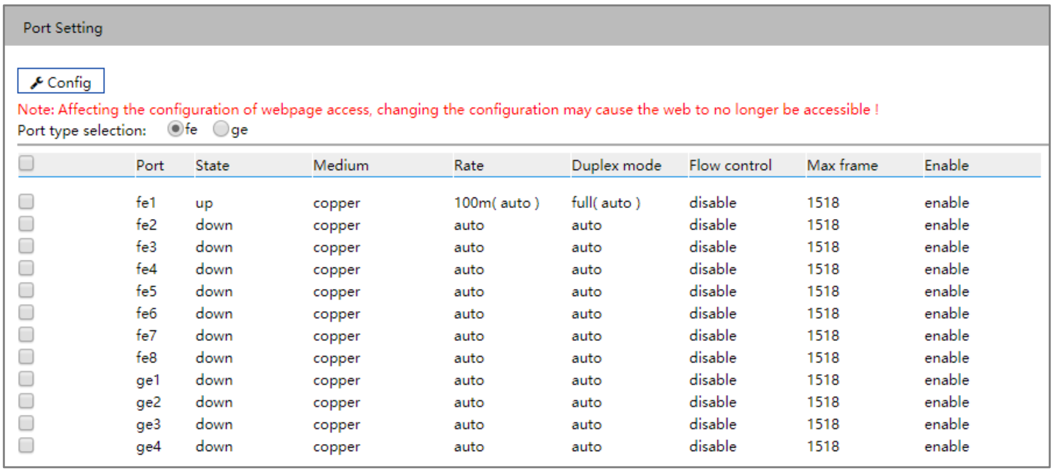
On the "Port Setting" page, user can check port type, rate and connection state, set rate mode, duplex mode, port enable, flow control and other parameters.

Operation Path

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

Interface Description

Port setting interface as follows:



Port Setting

Note: Affecting the configuration of webpage access, changing the configuration may cause the web to no longer be accessible !

Port type selection: ● fe ○ ge

□	Port	State	Medium	Rate	Duplex mode	Flow control	Max frame	Enable
□	fe1	up	copper	100m(auto)	full(auto)	disable	1518	enable
□	fe2	down	copper	auto	auto	disable	1518	enable
□	fe3	down	copper	auto	auto	disable	1518	enable
□	fe4	down	copper	auto	auto	disable	1518	enable
□	fe5	down	copper	auto	auto	disable	1518	enable
□	fe6	down	copper	auto	auto	disable	1518	enable
□	fe7	down	copper	auto	auto	disable	1518	enable
□	fe8	down	copper	auto	auto	disable	1518	enable
□	ge1	down	copper	auto	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

Main elements configuration description of port settings interface:

Interface Element	Description (check the checkbox of the port, click “config” to configure it.)
Name	The corresponding port name of the device Ethernet port.
Status	Ethernet port connection status, display status as follows: • down: represent the port is disconnected;

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
	● 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.
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 flow control of port data sending; ● 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 64~16360.
Enable	Enable or disable Ethernet port. Options are as follows: ● enable ● disable Notice: If user doesn't check the port "enable" checkbox, the port won't be connected to use.

4.2 Storm Control

Function Description

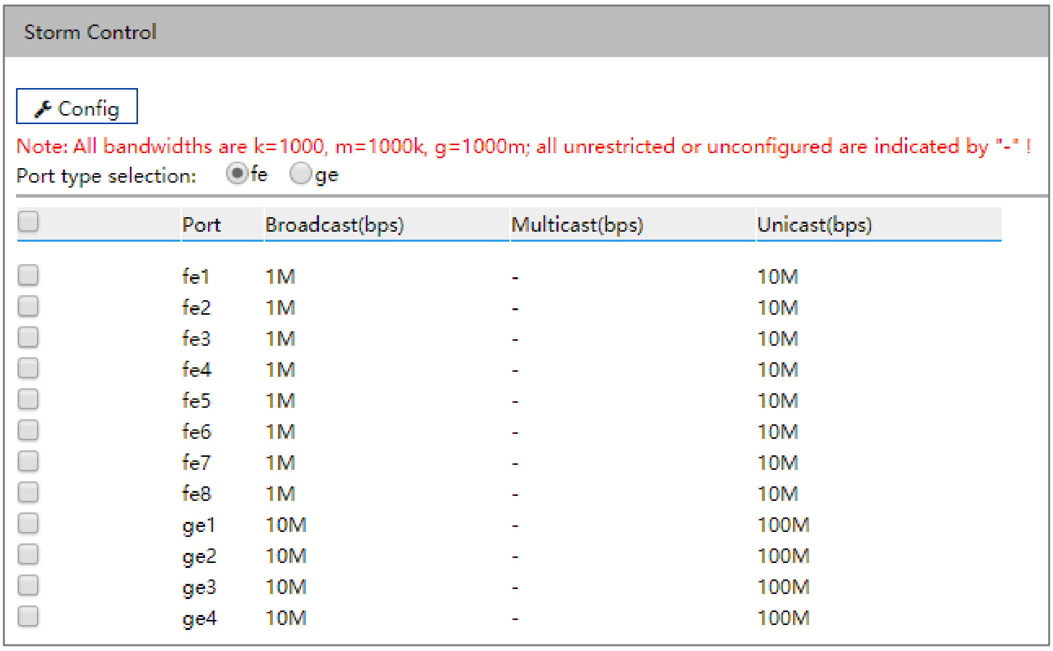
On the "Storm Control" page, user can set the maximum broadcast, multicast or unknown unicast packet flow the port allows. When the sum of each port broadcast, unknown multicast or unknown unicast flow achieves the value user sets, the system will discard the packets beyond the broadcast, unknown multicast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

Interface Description

Storm control interface as follows:



Storm Control

Config

Note: All bandwidths are k=1000, m=1000k, g=1000m; all unrestricted or unconfigured are indicated by "-" !

Port type selection: ● fe ○ ge

□	Port	Broadcast(bps)	Multicast(bps)	Unicast(bps)
□	fe1	1M	-	10M
□	fe2	1M	-	10M
□	fe3	1M	-	10M
□	fe4	1M	-	10M
□	fe5	1M	-	10M
□	fe6	1M	-	10M
□	fe7	1M	-	10M
□	fe8	1M	-	10M
□	ge1	10M	-	100M
□	ge2	10M	-	100M
□	ge3	10M	-	100M
□	ge4	10M	-	100M

Main elements configuration description of storm suppression 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.
Broadcast (bps)	The port control for broadcast packet transmission speed, input value range： • 100M interface: 0-100,000Kbps or 0-100Mbps, and 0 means that the current rate is not limited. • Gigabit interface: 0-1,000,000 kbps, 0-1,000 Mbps or 0-1Gbps, 0 means that the current rate is not limited. 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: 0-100,000Kbps or 0-100Mbps, and 0

Interface Element	Description (check the checkbox of the port, click “config” to configure it.)
	means that the current rate is not limited. ● Gigabit interface: 0-1000000Kbps or 0-1000Mbps, and 0 means that the current rate is not limited. 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: 0-100,000Kbps or 0-100Mbps, and 0 means that the current rate is not limited. ● Gigabit interface: 0-1000000Kbps or 0-1000Mbps, and 0 means that the current rate is not limited. 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.

4.3 Port Rate Limit

Function Description

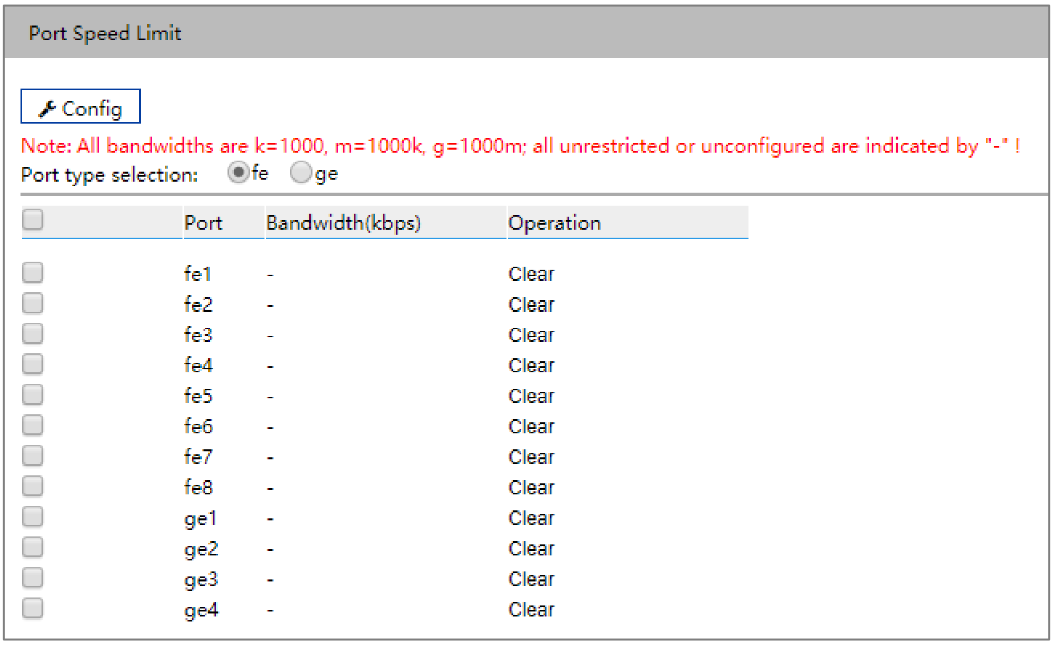
On the "Port Speed Limit" page, User can limit the communication flow of each port or cancel the port flow limit. The device provides port speed limit, including entrance and exit speed limit. User can select a fixed speed, the device will discard the packet or adopt flow control to limit the transmission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

Operation Path

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

Interface Description

Port rate limit interface as follows:



Port Speed Limit

Config

Note: All bandwidths are k=1000, m=1000k, g=1000m; all unrestricted or unconfigured are indicated by "-" !

Port type selection: ● fe ○ ge

□	Port	Bandwidth(kbps)	Operation
□	fe1	-	Clear
□	fe2	-	Clear
□	fe3	-	Clear
□	fe4	-	Clear
□	fe5	-	Clear
□	fe6	-	Clear
□	fe7	-	Clear
□	fe8	-	Clear
□	ge1	-	Clear
□	ge2	-	Clear
□	ge3	-	Clear
□	ge4	-	Clear

The main element configuration description of port speed limit 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.
Bandwidth (bps)	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. ● Gigabit interface: 64-1000000Kbps or 1-1000Mbps; 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 restores to no limit by default.

Note

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

4.4Port Mirroring

Function Description

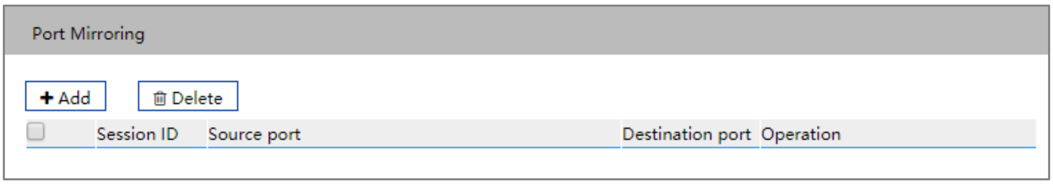
On the "Port mirroring" page, user can copy the data from the origin port to appointed port for data analysis and monitoring.

Operation Path

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

Interface Description

Port mirror interface as follows:


Port Mirroring

□	Session ID	Source port	Destination port	Operation

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	A set of monitored ports, which will collect data from these ports in the specified direction, and the mirror port can be one or more.
Destination port	The destination port of device mirroring.
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.
Add	Click "Add" to increase the port mirror entries.
Delete	Check the checkbox of port mirror entries, click “Delete”

Interface Element	Description (check the checkbox of the port, and click “Add” button to configure it.
	button to delete all mirror group entries

Note

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

4.5 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.

Function Description

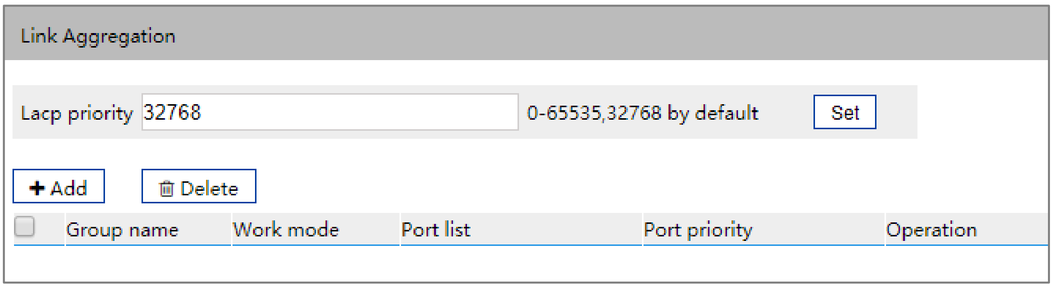
Under static aggregation mode, the member port in aggregation group disables LACP protocol, its port status is maintained manually.

Operation Path

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

Interface Description

Link Aggregation interface as below:



Link Aggregation

Lacp priority 32768 0-65535,32768 by default Set

□	Group name	Work mode	Port list	Port priority	Operation

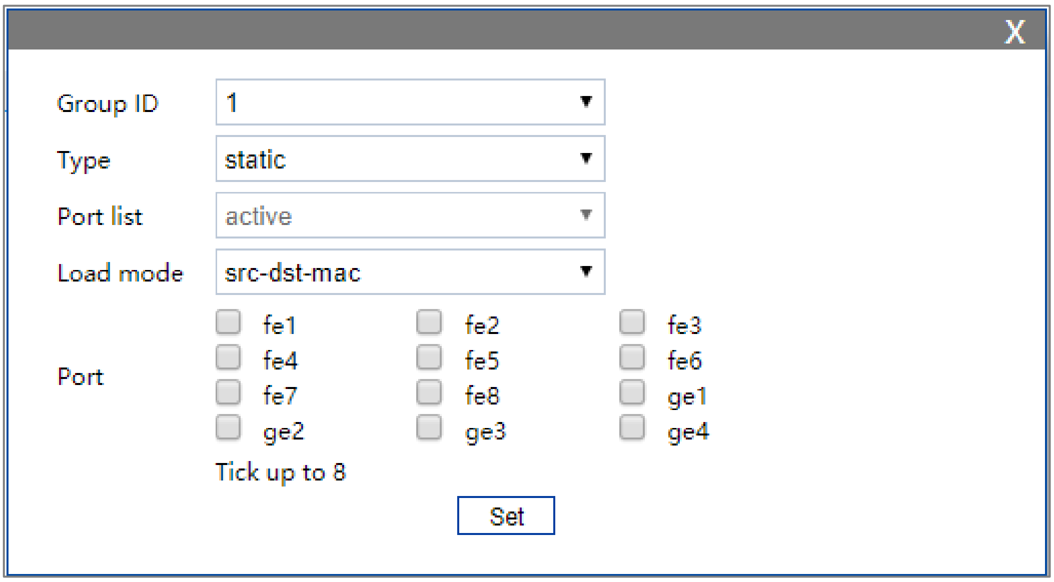
The main element configuration description of Link Aggregation interface:

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	Static aggregation link ID number, 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; • 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 and port priority 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

Interface Element	Description
	“Delete” button to delete link aggregation entry.

Interface Description: Add

The Link Aggregation-Add interface as follows:



Group ID: 1 ▾

Type: static ▾

Port list: active ▾

Load mode: src-dst-mac ▾

Port:

□ fe1	□ fe2	□ fe3
□ fe4	□ fe5	□ fe6
□ fe7	□ fe8	□ ge1
□ ge2	□ ge3	□ ge4

Tick up to 8

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

Interface Element	Description
Group ID	Static aggregation link ID number, support maximum 12 groups, each group can configure 8 ports to join aggregation.
Type	Aggregation group mode: ● Static: Static aggregation; ● Dynamic: Dynamic aggregation.
Port member	The drop-down box of port mode: ● Active; ● Passive. Note: This function needs to be set only when the type is dynamic.
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;

Interface Element	Description
	● Src-mac: Load balance mode based on source MAC.
Port	Port member in the aggregation group.

4.6 Port Statistics

4.6.1 Port Statistics-Overview

Function Description

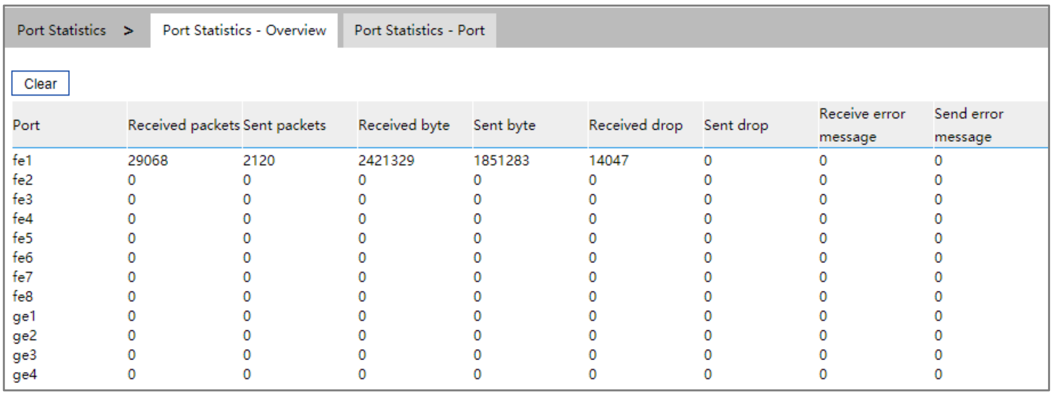
On the "Port Statistics-Overview" page, user can check the data packet and byte number that each port sends and receives and the message number it discards.

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
fe1	29068	2120	2421329	1851283	14047	0	0	0
fe2	0	0	0	0	0	0	0	0
fe3	0	0	0	0	0	0	0	0
fe4	0	0	0	0	0	0	0	0
fe5	0	0	0	0	0	0	0	0
fe6	0	0	0	0	0	0	0	0
fe7	0	0	0	0	0	0	0	0
fe8	0	0	0	0	0	0	0	0
ge1	0	0	0	0	0	0	0	0
ge2	0	0	0	0	0	0	0	0
ge3	0	0	0	0	0	0	0	0
ge4	0	0	0	0	0	0	0	0

4.6.2 Port Statistics-Port

Function Description

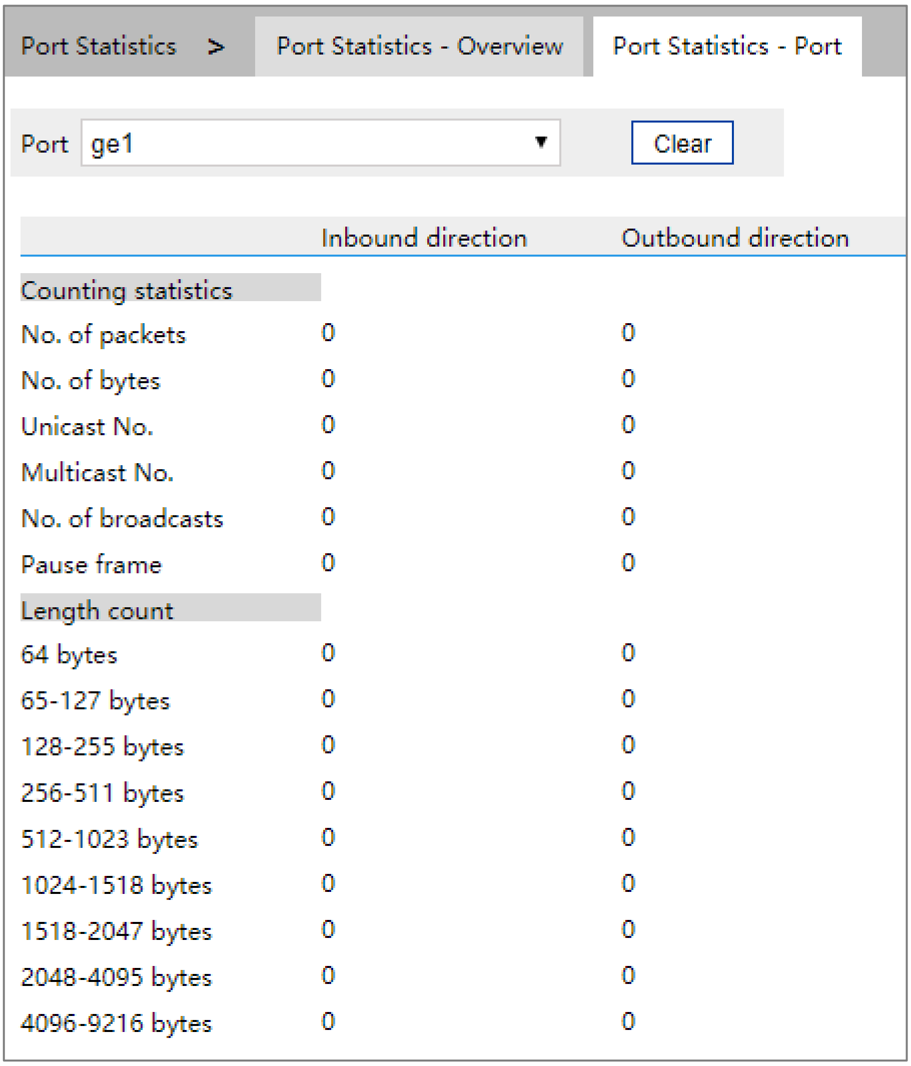
On the "Port Statistics-Port" page, user can check the classified statistic of message sum and the number of message bytes sent and received by specified port.

Operation Path

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

Interface Description

Port Statistics-Port interface as follows:



Port: ge1

	Inbound direction	Outbound direction
Counting statistics		
No. of packets	0	0
No. of bytes	0	0
Unicast No.	0	0
Multicast No.	0	0
No. of broadcasts	0	0
Pause frame	0	0
Length count		
64 bytes	0	0
65-127 bytes	0	0
128-255 bytes	0	0
256-511 bytes	0	0
512-1023 bytes	0	0
1024-1518 bytes	0	0
1518-2047 bytes	0	0
2048-4095 bytes	0	0
4096-9216 bytes	0	0

4.7 Port Isolation

Function Description

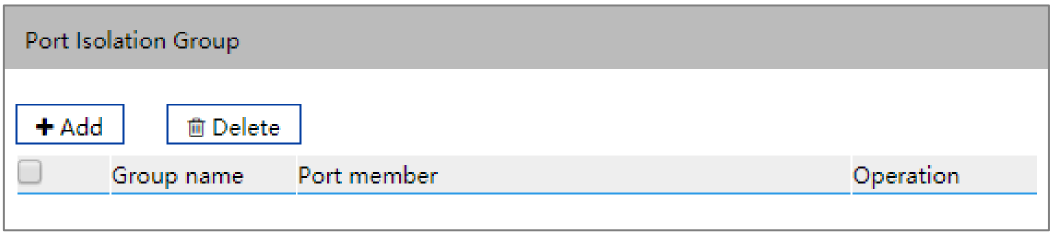
Port isolation is used for the layer 2 isolation between messages. It could add different ports to different VLANs, but waste limited VLAN resources. Adopting isolate-port characteristics can achieve isolation of ports within the same VLAN. After adding the ports to isolation group, user can achieve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

Operation Path

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

Interface Description

Isolate-port configuration interface as follows:



Port Isolation Group

□	Group name	Port member	Operation

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

Interface Element	Description
Group name	The Group ID of the device’s port isolation group. Its value range is 0-8.
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.

5 Layer 2 Configuration

5.1MAC 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

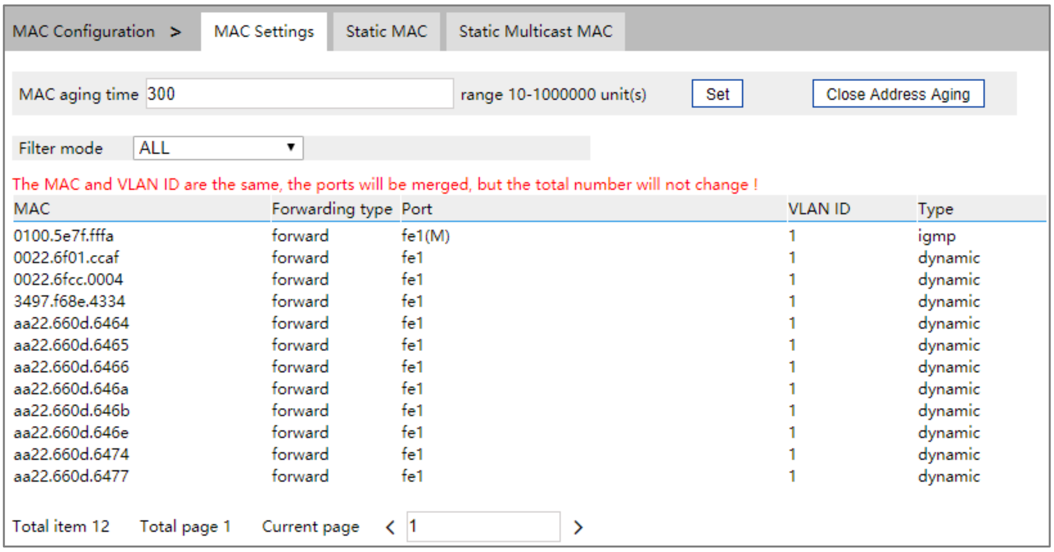
On the "MAC setting" page, user can configure the aging time of dynamic MAC address and check static and dynamic MAC address information.

Operation Path

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

Interface Description

MAC configuration interface as follows:



MAC aging time 300 range 10-1000000 unit(s)

Filter mode ALL

The MAC and VLAN ID are the same, the ports will be merged, but the total number will not change !

MAC	Forwarding type	Port	VLAN ID	Type
0100.5e7f.fffa	forward	fe1(M)	1	igmp
0022.6f01.ccaf	forward	fe1	1	dynamic
0022.6fcc.0004	forward	fe1	1	dynamic
3497.f68e.4334	forward	fe1	1	dynamic
aa22.660d.6464	forward	fe1	1	dynamic
aa22.660d.6465	forward	fe1	1	dynamic
aa22.660d.6466	forward	fe1	1	dynamic
aa22.660d.646a	forward	fe1	1	dynamic
aa22.660d.646b	forward	fe1	1	dynamic
aa22.660d.646e	forward	fe1	1	dynamic
aa22.660d.6474	forward	fe1	1	dynamic
aa22.660d.6477	forward	fe1	1	dynamic

Total item 12 Total page 1 Current page < 1 >

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.
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	The forward type of MAC, discard or transmit, it displays as follows: ● Discard; ● Forward.
Port	Corresponding port number of the MAC address.
VLAN ID	VLAN ID number the data MAC address sending belongs to.
Type	MAC address type, dynamic MAC and static MAC address,

Interface Element	Description
	display as follows: ● dynamic; ● static.

5.1.2 Static MAC

Function Description

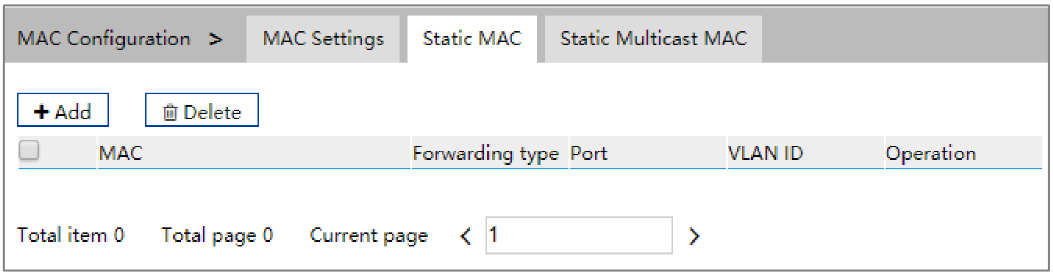
On the "Static Mac" page, user can manually configure the static MAC address and bind the source unicast MAC address without aging.

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
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

Interface Element	Description
	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

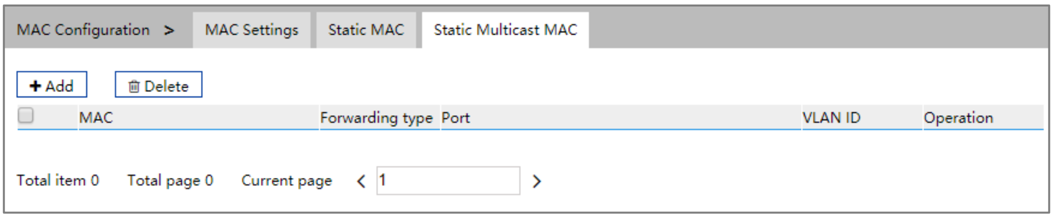
On the "Static Multicast Mac" page, user can manually configure the static MAC address and bind the source multicast MAC address without aging.

Operation Path

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

Interface Description

Static multicast MAC interface as follows:



□	MAC	Forwarding type	Port	VLAN ID	Operation

Total item 0 Total page 0 Current page < 1 >

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.
Interface	The Binding Port

Interface Element	Description
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

5.2VLAN 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

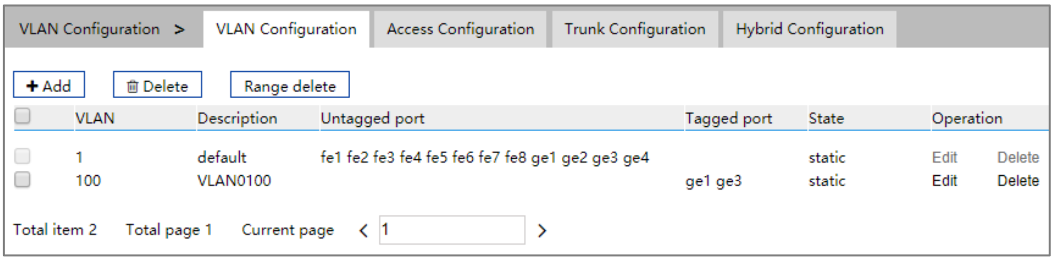
On the "Vlan-config" page, user can create VLAN and edit VLAN description.

Operation Path

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

Interface Description

Vlan configuration interface as follows:



☐	VLAN	Description	Untagged port	Tagged port	State	Operation	
☐	1	default	fe1 fe2 fe3 fe4 fe5 fe6 fe7 fe8 ge1 ge2 ge3 ge4		static	Edit	Delete
☐	100	VLAN0100		ge1 ge3	static	Edit	Delete

Total item 2 Total page 1 Current page < 1 >

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.
Range Delete	Click the "Batch Delete" button to delete range-specified VLAN entry.

5.2.2 Access Configuration

Function Description

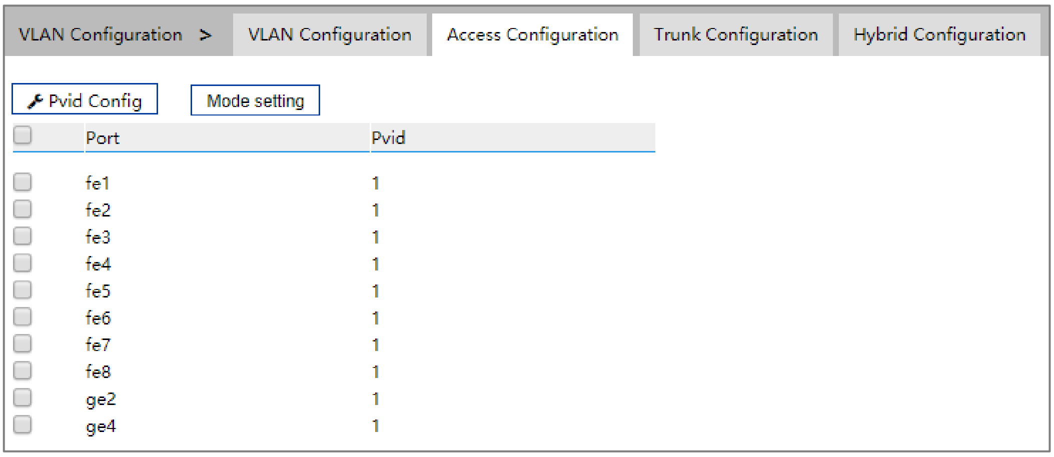
On the "Access Configuration" page, user can configure the port VLAN mode (access, trunk, Hybrid), and port VLAN ID: PVID.

Operation Path

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

Interface Description

Access configuration interface as follow:



□	Port	Pvid
□	fe1	1
□	fe2	1
□	fe3	1
□	fe4	1
□	fe5	1
□	fe6	1
□	fe7	1
□	fe8	1
□	ge2	1
□	ge4	1

The main element configuration description of Access configuration interface.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Pvid	Port Default Vlan ID, which is the default VLAN of the port. Default is 1, value range is 1-4094. Note: Each port has a PVID property, when the port receives Untag messages, it adds Tag mark on them according to PVID. When the port transmits data message with the same Tag mark as PVID, it would erase the Tag mark and then transmit the message. The PVID of all ports default to 1.
Configuration	Check the entries of pvid value that need to be reset, click "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.

5.2.3 Trunk Configuration

Function Description

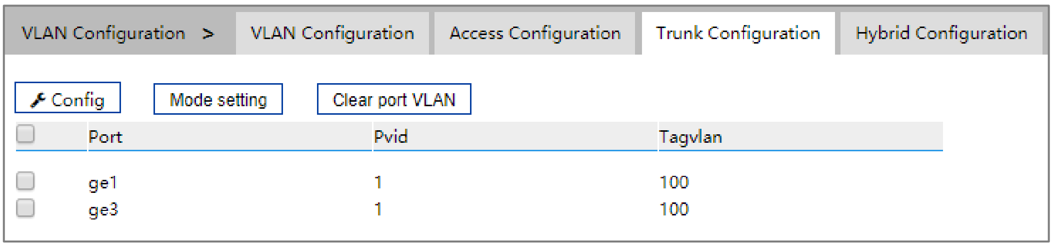
On the “Trunk configuration” page, user can configure port pvid value and tagvlan, as well as transforming the value of Trunk type to Access or Hybrid type.

Operation Path

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

Interface Description

Trunk configuration interface as follows:



□	Port	Pvid	Tagvlan
□	ge1	1	100
□	ge3	1	100

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	The tagged value, an individual number or range (“-” represents range). For example: 9 or 10-15.
Configuration	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 type to access or hybrid
Clear port VLAN	Check the entries that need to be configured, click to clear port VLAN, input tagvlan value to delete tagvlan

5.2.4 Hybrid Configuration

Function Description

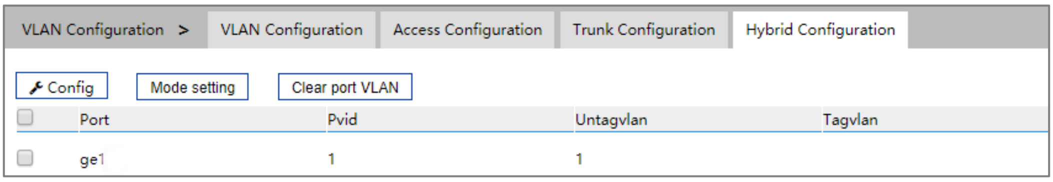
On the "Hybrid Configuration" page, user can configure Hybrid relative parameters.

Operation Path

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

Interface Description

Hybrid configuration interface as follow:



□	Port	Pvid	Untagvlan	Tagvlan
□	ge1	1	1	

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	The untagged value, an individual number or range ("-" represents range). For example: 9 or 10-15.
Tagvlan	The tagged value, an individual number or range ("-" represents range). For example: 9 or 10-15.
Configuration	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 type to access or trunk

Process for Port Receiving Message

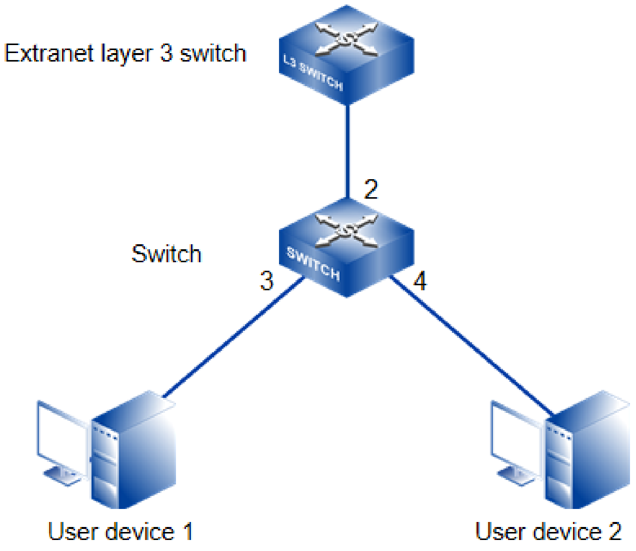
Interface type	Process for Receiving Untagged Message	Process for Receiving Tagged Message
Access	Receive this message and tag it with default VLAN ID.	• Receive the message when the VLAN ID is the same as default VLAN ID. • Discard the message when the VLAN ID is different from the default VLAN ID.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

Process for Sending Message

Interface type	The process of transmit frame
Access	Strip the PVID Tag of the message first, then transmit it.
Trunk	• When the VLAN ID is the same as the default VLAN ID, and it is the VLAN ID allowed to pass through the interface, it would strip the Tag and send this message. • 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. The PVID value of Port3 is set to 3.
- Port 4

  Port4 is downward interface, set Ports to Access type. The PVID value of Port4 is set to 4.
- Port2

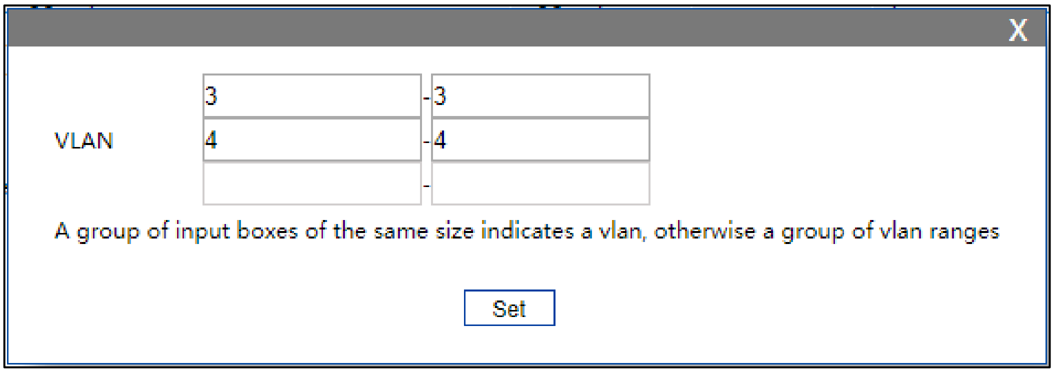
  Port2 is upper interface, set Port2 to Trunk type. Add Port2 into VLAN3 and VLAN4. Port2 can communicate with Port3 and Port4.

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:



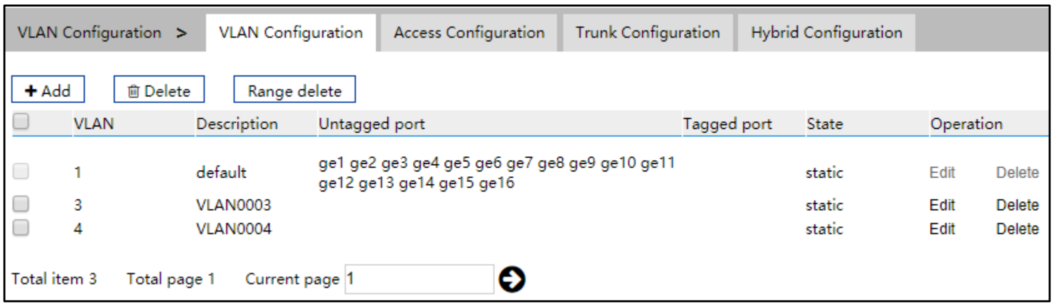
VLAN 3 - 3

4 - 4

-

A group of input boxes of the same size indicates a vlan, otherwise a group of vlan ranges

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

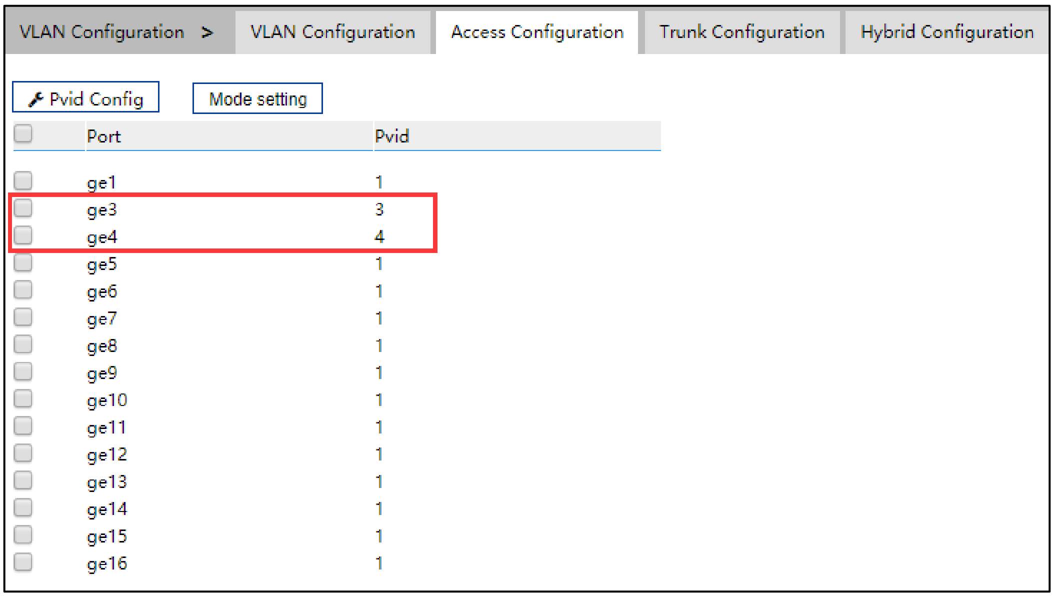


□	VLAN	Description	Untagged port	Tagged port	State	Operation	
□	1	default	ge1 ge2 ge3 ge4 ge5 ge6 ge7 ge8 ge9 ge10 ge11 ge12 ge13 ge14 ge15 ge16		static	Edit	Delete
□	3	VLAN0003			static	Edit	Delete
□	4	VLAN0004			static	Edit	Delete

Total item 3 Total page 1 Current page 1

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

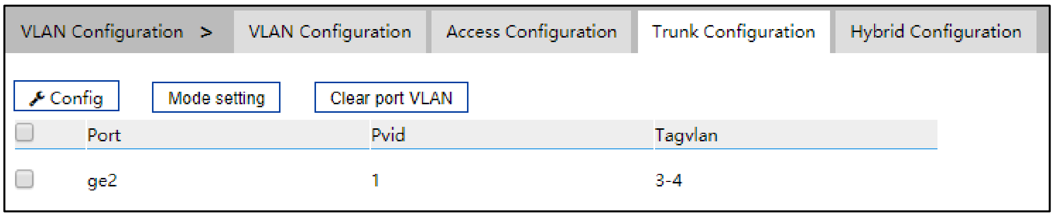
1. Access "Layer 2 Configuration > VLAN Configuration > Access Configuration".
2. Check port ge3, click “configure”, enter “pvid” as “3”, and click “set”.
3. Check port ge4, click “configure”, enter “pvid” as “4”, and click “set”.
4. Check port ge2, click “mode setting”, select “trunk” as “type”, and click “set”.



□	Port	Pvid
□	ge1	1
□	ge3	3
□	ge4	4
□	ge5	1
□	ge6	1
□	ge7	1
□	ge8	1
□	ge9	1
□	ge10	1
□	ge11	1
□	ge12	1
□	ge13	1
□	ge14	1
□	ge15	1
□	ge16	1

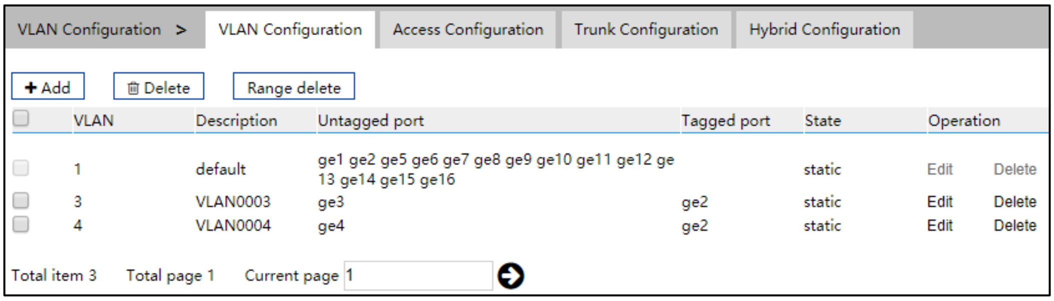
Step 4 Set the tagvlan value of port 2.

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.



□	Port	Pvid	Tagvlan
□	ge2	1	3-4

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



□	VLAN	Description	Untagged port	Tagged port	State	Operation	
□	1	default	ge1 ge2 ge5 ge6 ge7 ge8 ge9 ge10 ge11 ge12 ge13 ge14 ge15 ge16		static	Edit	Delete
□	3	VLAN0003	ge3	ge2	static	Edit	Delete
□	4	VLAN0004	ge4	ge2	static	Edit	Delete

Total item 3 Total page 1 Current page 1

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

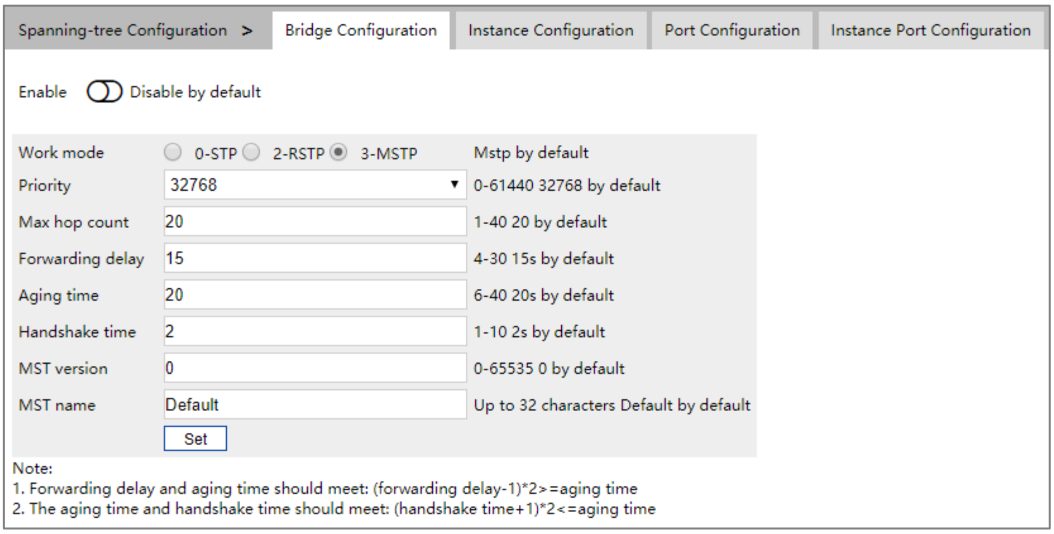
On the "Bridge Configuration" page, user can configure relative parameters of spanning-tree.

Operation Path

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

Interface Description

Bridge configuration interface as follows:



Enable Disable by default

Work mode	○ 0-STP ○ 2-RSTP ● 3-MSTP	Mstp by default
Priority	32768	0-61440 32768 by default
Max hop count	20	1-40 20 by default
Forwarding delay	15	4-30 15s by default
Aging time	20	6-40 20s by default
Handshake time	2	1-10 2s by default
MST version	0	0-65535 0 by default
MST name	Default	Up to 32 characters Default by default

Note:
1. Forwarding delay and aging time should meet: (forwarding delay-1)*2>=aging time
2. The aging time and handshake time should meet: (handshake time+1)*2<=aging time

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.
FWD 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: 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

Interface Element	Description
	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).

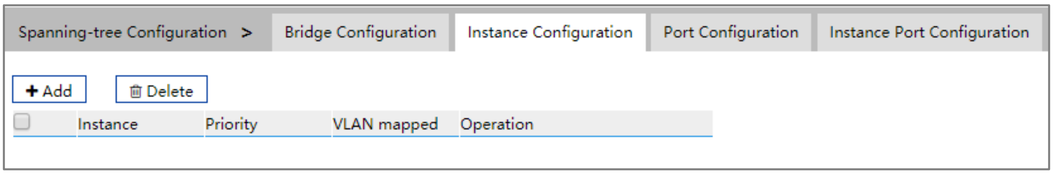
VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI.

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. Note: The priority of a device participates in spanning tree calculation. Its

Interface Element	Description
	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

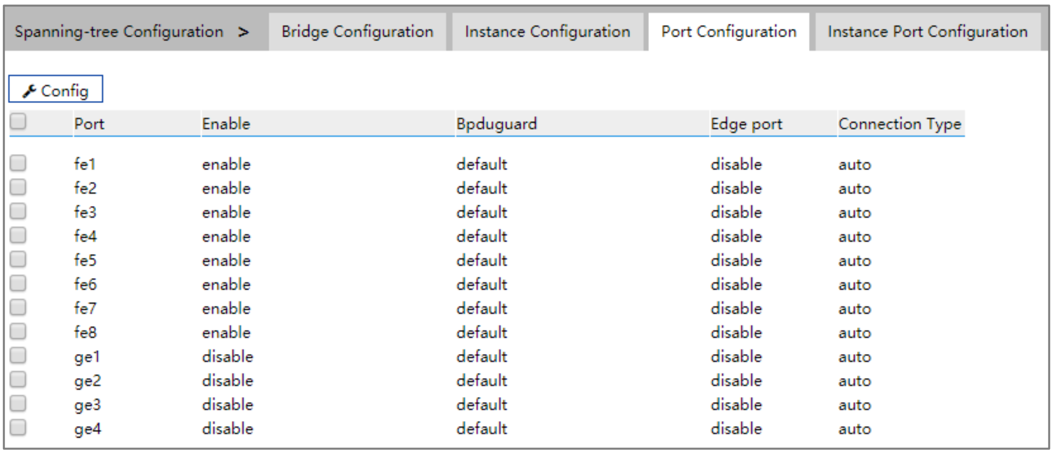
On the "Port Configuration" page, user can enable port to participate in spanning-tree and configure port type, link type and BPDU protection function.

Operation Path

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

Interface Description

Check port configuration interface as below:



□	Port	Enable	Bpduguard	Edge port	Connection Type
□	fe1	enable	default	disable	auto
□	fe2	enable	default	disable	auto
□	fe3	enable	default	disable	auto
□	fe4	enable	default	disable	auto
□	fe5	enable	default	disable	auto
□	fe6	enable	default	disable	auto
□	fe7	enable	default	disable	auto
□	fe8	enable	default	disable	auto
□	ge1	disable	default	disable	auto
□	ge2	disable	default	disable	auto
□	ge3	disable	default	disable	auto
□	ge4	disable	default	disable	auto

The main element configuration description of global 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	Enable checkbox to participate in spanning-tree.
BPDU Guard	BPDU (Bridge Protocol Data Unit) protection function.
Edge port	Configure port type:

Interface Element	Description (check the checkbox of the port, click “config” to configure it.)
	● Enable; ● Disable.
Line 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

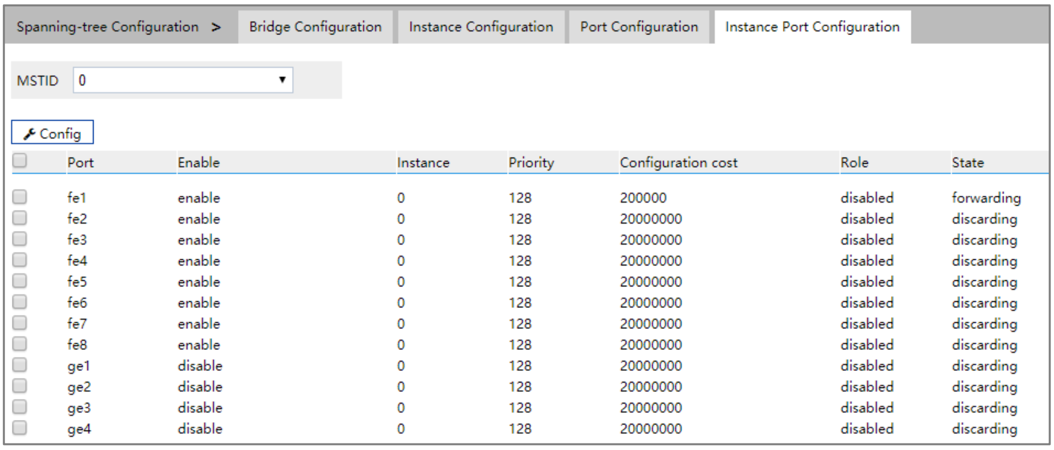
On the "Inst Port Config" page, user can configure port priority level and cost.

Operation Path

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

Interface Description

Instance port configuration interface as follows:



MSTID: 0

□	Port	Enable	Instance	Priority	Configuration cost	Role	State
□	fe1	enable	0	128	200000	disabled	forwarding
□	fe2	enable	0	128	20000000	disabled	discarding
□	fe3	enable	0	128	20000000	disabled	discarding
□	fe4	enable	0	128	20000000	disabled	discarding
□	fe5	enable	0	128	20000000	disabled	discarding
□	fe6	enable	0	128	20000000	disabled	discarding
□	fe7	enable	0	128	20000000	disabled	discarding
□	fe8	enable	0	128	20000000	disabled	discarding
□	ge1	disable	0	128	20000000	disabled	discarding
□	ge2	disable	0	128	20000000	disabled	discarding
□	ge3	disable	0	128	20000000	disabled	discarding
□	ge4	disable	0	128	20000000	disabled	discarding

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.
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.

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
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.

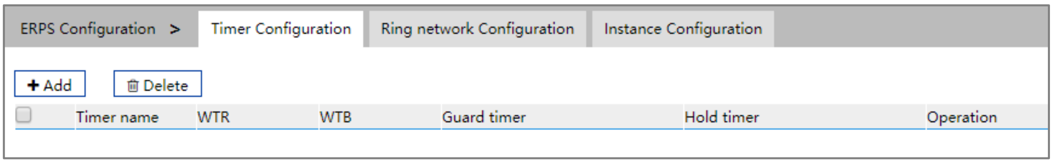
An Ethernet network topology connected in ring is called a ERPS Ring. It could be divided into main ring and subring. Each device in ERPS ring is called a node. The main node is in charge of blocking and opening ports on this node, preventing loops from forming.

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.
GuardTimer	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.
HoldTimer	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 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.

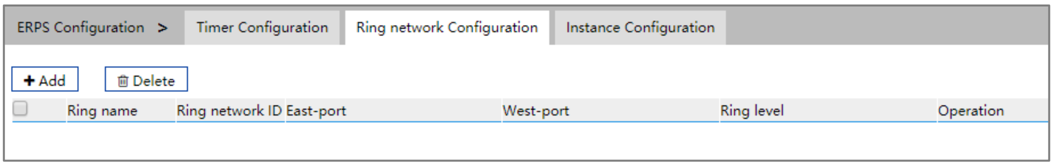
An Ethernet network topology connected in ring is called a ERPS Ring. It could be divided into main ring and subring. Each device in ERPS ring is called a node. The main node is in charge of blocking and opening ports on this node, preventing loops from forming.

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 ID	The ID of ring network, its value range is 1-255
East Interface	Ring network 1, its value range is 1-port number
West Interface	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

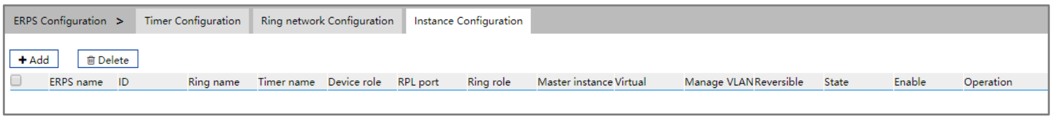
On the "Instance configuration” page, user could configure instance.

Operation Path

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

Interface Description

Instance configuration interface as follows:



□	ERPS name	ID	Ring name	Timer name	Device role	RPL port	Ring role	Master instance	Virtual	Manage VLAN	Reversible	State	Enable	Operation

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. • 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.

Interface Element	Description
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.
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.

Interface Element	Description
Delete	Check the radio box of instance configuration entry, click “delete” button to delete instance configuration.

5.5Ring 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 adopts 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

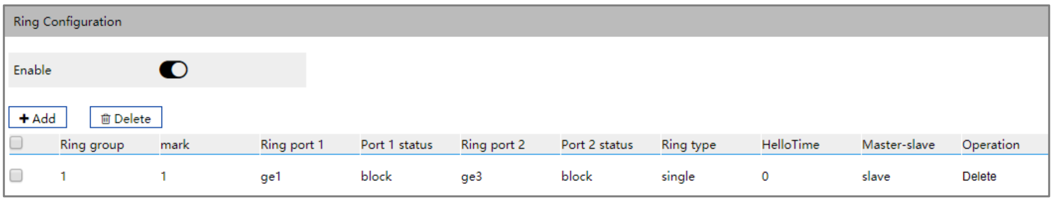
On the "Ring Configuration" page, user can enable/disable the ring network.

Operation Path

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

Interface Description

Ring configuration interface as follow:



Ring Configuration

Enable ●

□	Ring group	mark	Ring port 1	Port 1 status	Ring port 2	Port 2 status	Ring type	HelloTime	Master-slave	Operation
□	1	1	ge1	block	ge3	block	single	0	slave	Delete

The main element configuration description of Ring configuration interface.

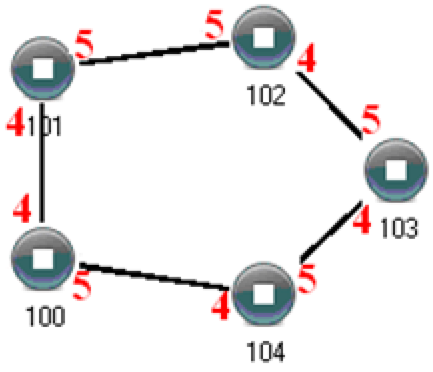
Interface Element	Description
Enable	Enable switch, which can enable the Ring network function after being enabled.
Ring group	Support ring group 1-4, it can create 4 ring networks at the same time.
Mark	When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID. Value

Interface Element	Description
	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", it displays "coupling port". Coupling port is the port that connects different network identities.
Port 1 status	Conduction state of ring port 1.
Ring port 2	The network port 2 on the switch used to form a ring. Note: • When the ring network type is "Couple", it displays "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;
Port 2 status	Conduction state of port 1 of ring network.
Ring Type	According to the requirement in the scene, user can choose different ring type. • Single: single ring, using a continuous ring to connect all device together. • Couple: couple ring is a redundant structure used for connecting two independent networks. • Chain: chain can enhance user's flexibility in constructing all types of redundant network topology via an advanced software technology. • Dual-homing: two adjacent rings share one switch. User could put one switch in two different networks or two different switching equipments in one network.
Hello Time	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	Master-slave mode option: • Master; • Slave. Note: There is only one Master in one ring network.
Add	Click "Add" button to add ring network configuration.

Interface Element	Description
Delete	Check the radio box of ring network configuration entry and click “delete” button to delete ring network configuration.

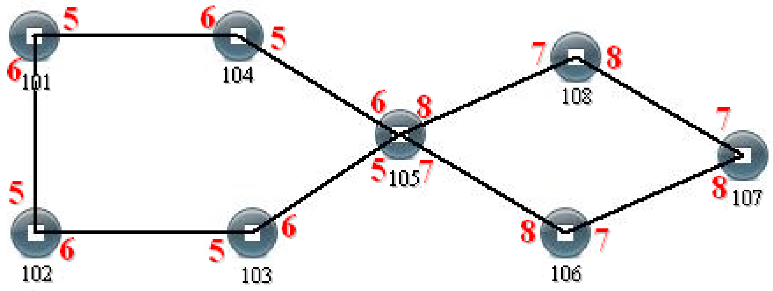
Single Ring Configuration

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;

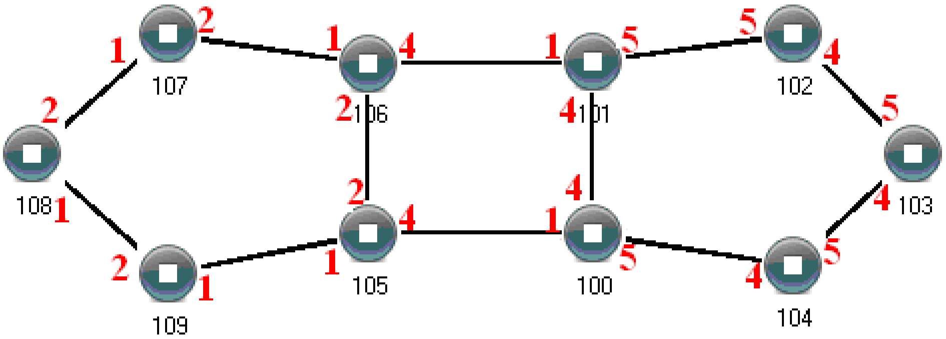
Step 4 Adopt network cable to connect the ring group 2;

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 affect CPU processing speed seriously);

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

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

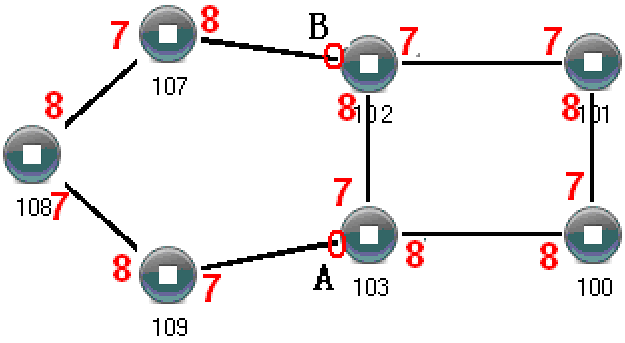
Step 4 Set the ring port of NO. 107, 108 and 109 device ring group 1 to port 1 and port 2, network identification to 1, ring type to Single; Set the ring port of NO. 102, 103 and 104 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single.

Step 5 Connect the port 4 and port 5 of five devices NO. 100-104 to the single ring in turn, adopt network cable to connect the port 1 and port 2 of four devices NO. 105109 to the single ring in turn, then adopt Ethernet cable to connect port 4 of NO. 106 device to port 1 of NO. 101 device, port 4 of NO. 105 device to port 1 of NO. 100 device, coupling ring combination is completed.

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

Chain Configuration

Chain basic framework 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 devices, 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.

5.6IGMP-Snooping Configuration

IP host applies for joining (or leaving) multicast group to nearby routers through the Internet Group Management Protocol (IGMP). IGMP Snooping is a multicast suppression mechanism that manages and controls multicast group by listening and analyzing IGMP messages exchanged between host and multicast devices.

The working process of IGMP Snooping: The switch snoops the messages between user host and router, as well as tracking multicast information and the ports that have been applied for. When the switch intercepts the IGMP Report (request) sent by the host toward router, the switch adds the port to multicast forwarding table. When the switch intercepts the IGMP Leave message sent by the host, the router sends a Group-Specific Query message of the port. If other hosts need the multicast, they will respond with the IGMP Report message. If the router can't receive any response from the host, the switch deletes the port from the multicast forwarding table. The router sends IGMP Query message periodically. When switch receives IGMP Query message, it would delete this port from multicast table if it doesn’t receive IGMP Report message from the host in a given period time.

5.6.1Global Configuration

Function Description

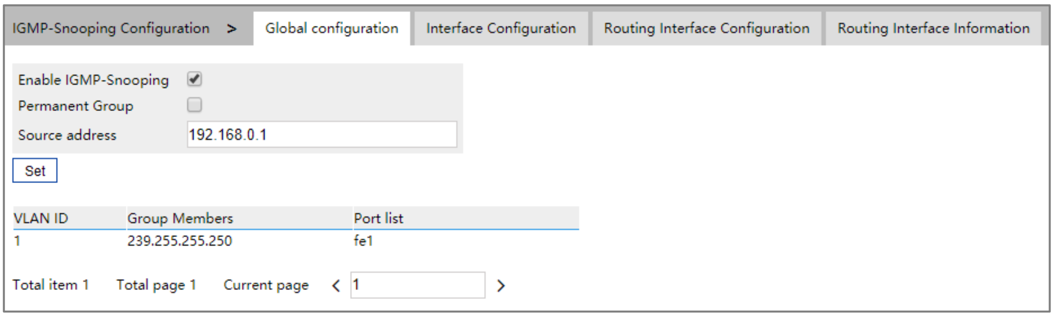
On the "Global Configuration" page, user can enable/disable IGMP monitoring and resident multicast.

Operation Path

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

Interface Description

Global configuration interface is as follows:


IGMP-Snooping Configuration >
Global configuration
Interface Configuration
Routing Interface Configuration
Routing Interface Information
Set

Enable IGMP-Snooping ☑
Permanent Group □
Source address 192.168.0.1

VLAN ID	Group Members	Port list
1	239.255.255.250	fe1

Total item 1 Total page 1 Current page ‹ 1 ›

The main element configuration description of global configuration interface:

Interface Element	Description
Enable IGMP-snooping	Enable IGMP-snooping configuration checkbox.
Permanent group	Configure the multicast group as a resident multicast group without aging or leaving.
Source address	When there is no IP address in VLAN, you can specify the IP address of the sending source, and the default IP address is 192.168.0.1.
VLAN ID	Port number VLAN ID number.
Group members	Multicast IP address.
Port list	The corresponding port name of the device Ethernet port.

5.6.2 Interface Configuration

Function Description

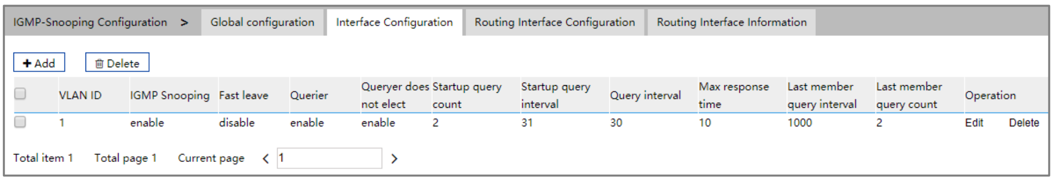
On the "Interface Configuration" page, user can configure the related parameters of interface IGMP Snooping.

Operation Path

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

Interface Description

Interface configuration interface as follows:


IGMP-Snooping Configuration >
Global configuration
Interface Configuration
Routing Interface Configuration
Routing Interface Information
+ Add
Delete

□	VLAN ID	IGMP Snooping	Fast leave	Querier	Queryer does not elect	Startup query count	Startup query interval	Query interval	Max response time	Last member query interval	Last member query count	Operation
□	1	enable	disable	enable	enable	2	31	30	10	1000	2	Edit Delete

Total item 1 Total page 1 Current page ‹ 1 ›

The main element configuration description of interface configuration interface:

Interface Element	Description
VLAN ID	VLAN ID number. Its 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.
Querier	Enable status of IGMP inquirer. IGMP inquirer can send universal group inquiry messages to all hosts and other multicast routers in this network segment.
Querier does not elect	IGMP inquirer does not elect the enabled status. 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 inquiry message. Note: The query interval of universal group must be greater than the maximum response of universal group.
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

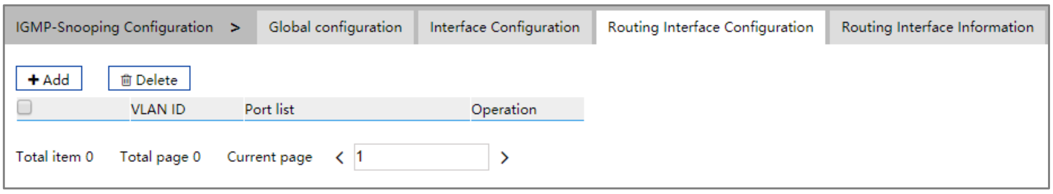
On the "Routing Port Configuration" page, user can configure the port of multicast router.

Operation Path

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

Interface Description

Routing port configuration interface is as below:


IGMP-Snooping Configuration >
Global configuration
Interface Configuration
Routing Interface Configuration
Routing Interface Information
+ Add
Delete

□	VLAN ID	Port list	Operation

Total item 0 Total page 0 Current page < 1 >

Main elements configuration description of routing port configuration interface:

Interface Element	Description
VLAN ID	VLAN ID number. Its 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

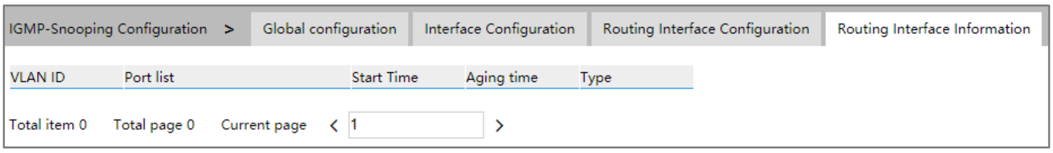
On the Routing Port Information page, you can view the startup time, aging time and port type of the routing port. The startup time starts from the port setting as the routing port.

Operation Path

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

Interface Description

Routing port information interface is as follows:



IGMP-Snooping Configuration >
Global configuration
Interface Configuration
Routing Interface Configuration
Routing Interface Information

VLAN ID	Port list	Start Time	Aging time	Type

Total item 0 Total page 0 Current page < 1 >

5.7 Port Loopback Detection

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

5.7.1 Global Configuration

Function Description

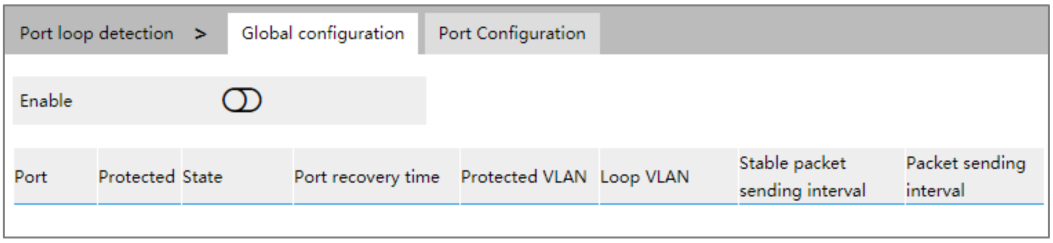
On the "Global Config" page, user can enable loop-detect configuration.

Operation Path

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

Interface Description

Global configuration interface is as follows:



Enable ○

Port	Protected	State	Port recovery time	Protected VLAN	Loop VLAN	Stable packet sending interval	Packet sending interval

The main element configuration description of global configuration interface:

Interface Element	Description
Enable switch	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.
Status	The connection status of this port, values are: ● Down: the port is physically disconnected ● Up: the port is connected

Interface Element	Description
	- Shutdown: the port is closed - No Shutdown: the port is not closed
Port recovery time	Recovery time after detection of loop action.
Protected VLAN	The VLAN ID of the loop protection.
Loop VLAN	The VLAN ID of the currently generated loop.
Stable packet sending interval	The interval between sending loop detection packets normally.
Packet sending interval	After the port is connected, the interval between sending loop detection packets. In this interval, three detection messages will be sent out, and then the packet-sending interval will return to the normal packet-sending interval.

5.7.2 Port Configuration

Function Description

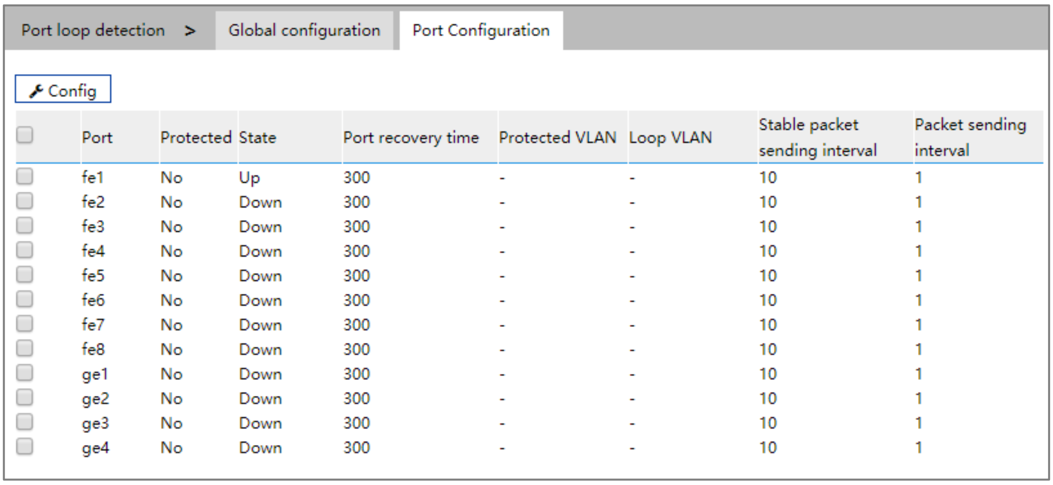
On the "Port config" page, user can implement relevant configuration of port loop detection.

Operation Path

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

Interface Description

Check port configuration interface as below:



□	Port	Protected	State	Port recovery time	Protected VLAN	Loop VLAN	Stable packet sending interval	Packet sending interval
□	fe1	No	Up	300	-	-	10	1
□	fe2	No	Down	300	-	-	10	1
□	fe3	No	Down	300	-	-	10	1
□	fe4	No	Down	300	-	-	10	1
□	fe5	No	Down	300	-	-	10	1
□	fe6	No	Down	300	-	-	10	1
□	fe7	No	Down	300	-	-	10	1
□	fe8	No	Down	300	-	-	10	1
□	ge1	No	Down	300	-	-	10	1
□	ge2	No	Down	300	-	-	10	1
□	ge3	No	Down	300	-	-	10	1
□	ge4	No	Down	300	-	-	10	1

The main element configuration description of global configuration interface:

Interface Element	Description

Interface Element	Description
Port	The corresponding port number of this device's Ethernet port.
Protected	The state of the port protected by a loop.
Status	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: 10-300, its unit is second.
Protect 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	The normal interval time of loop detection data packet sending, value range: 10-300, its unit is second.
Packet sending interval	After the port is connected, the interval between sending loop detection packets. In this interval, three detection messages will be sent out, and then the packet-sending interval will return to the normal packet-sending interval.

6 Layer 3 Configuration

6.1 Interface Configuration

Interface configuration mainly refers to setting the device 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

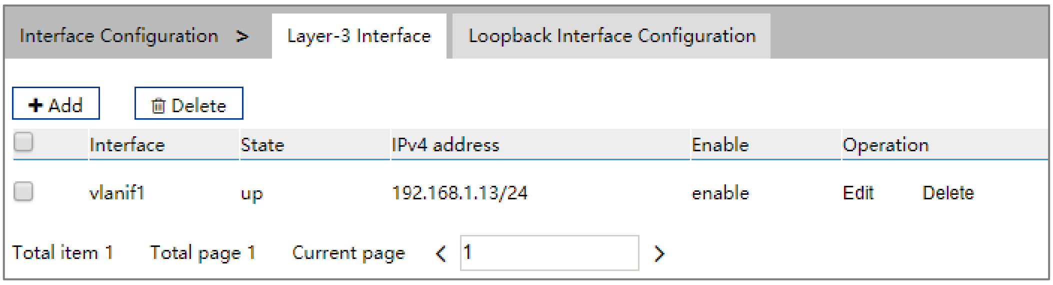
On the "Interface Configuration" page, user can configure the Layer 3 interface IP address.

Operation Path

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

Interface Description

L3 interface configuration interface as follows:



□	Interface	State	IPv4 address	Enable	Operation
□	vlanif1	up	192.168.1.13/24	enable	Edit Delete

Total item 1 Total page 1 Current page < 1 >

The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	Layer 3 interface names, such as, vlanif1, value range: vlanif1-vlanif4094.
Status	Interface state information, options: ● Up; ● Down.
IPv4 address	IPv4 address and subnet mask, such as 192.168.1.1/24.
Interface switch	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

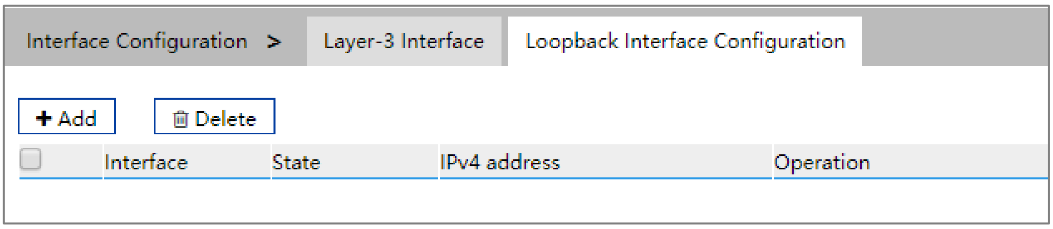
On the "Loopback Interface" page, user can configure the parameter of loopback interface.

Operation Path

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

Interface Description

Loopback interface configuration interface as follows:



□	Interface	State	IPv4 address	Operation

The main element configuration description of loopback interface:

Interface Element	Description
Interface	The name of loopback interface, value range: loopback0 or loopback1.
Status	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

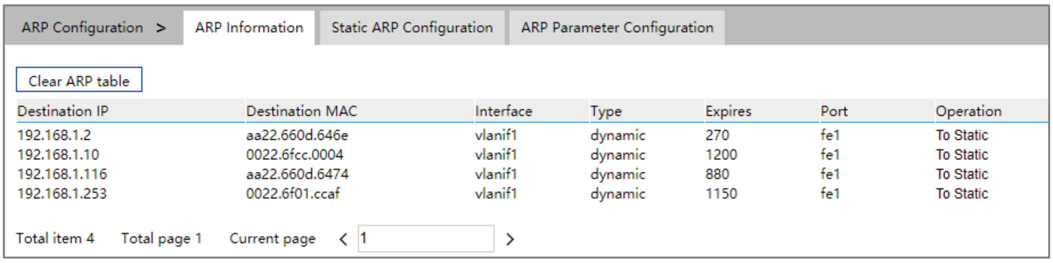
On the "ARP Information" page, user can check the ARP address, MAC, output port and other parameters.

Operation Path

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

Interface Description

ARP Information interface as follow:



Destination IP	Destination MAC	Interface	Type	Expires	Port	Operation
192.168.1.2	aa22.660d.646e	vlanif1	dynamic	270	fe1	To Static
192.168.1.10	0022.6fcc.0004	vlanif1	dynamic	1200	fe1	To Static
192.168.1.116	aa22.660d.6474	vlanif1	dynamic	880	fe1	To Static
192.168.1.253	0022.6f01.ccaf	vlanif1	dynamic	1150	fe1	To Static

The main element configuration description of ARP information interface:

Interface Element	Description
Dest IP	Destination IP address of accessing device.
Dest 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

Interface Element	Description
	address.

6.2.2 Static ARP

Function Description

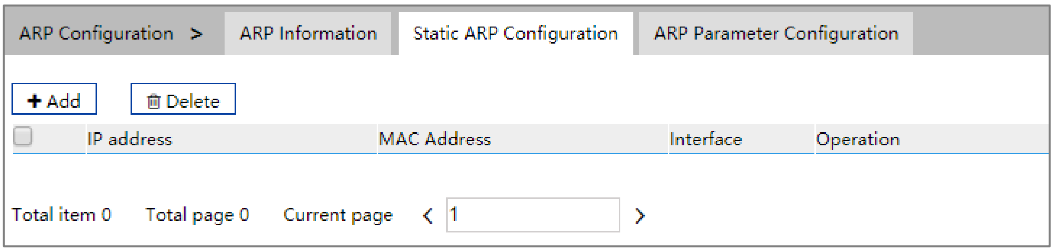
On the "Static ARP" page, user can conduct static ARP configuration.

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

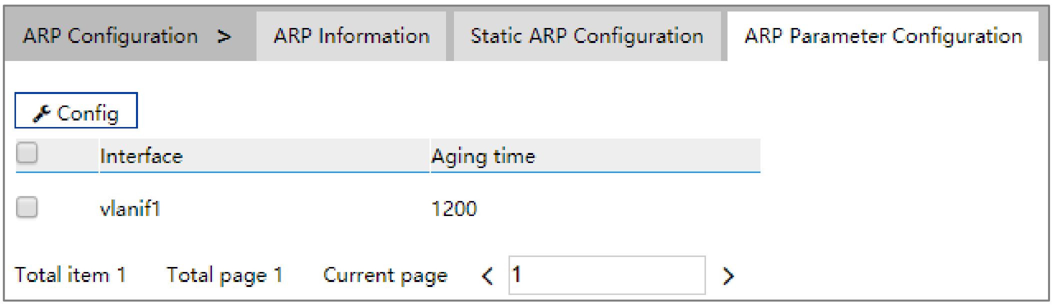
On the "ARP age-time" page, user can conduct ARP age-time configuration.

Operation Path

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

Interface Description

ARP parameter configuration interface as follows:



□	Interface	Aging time
□	vlanif1	1200

Total item 1　Total page 1　Current page < 1 >

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).

6.3VRRP 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

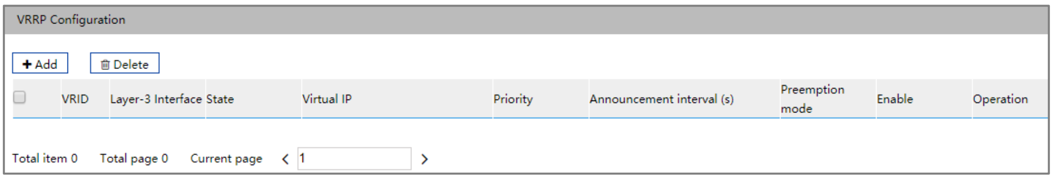
On the "VRRP Configuration" page, user can configure VRRP parameters.

Operation Path

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

Interface Description

VRRP configuration interface as follow:



VRRP Configuration

□	VRID	Layer-3 Interface	State	Virtual IP	Priority	Announcement interval (s)	Preemption mode	Enable	Operation

Total item 0 Total page 0 Current page < 1 >

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.
Status	Current status, options as follows: • Master; • Backup.
Virtual IP	Virtual router IP address, such as 192.168.1.253.
Priority	Priority defaults to 100, valid range is 1-254.
Notice interval (second)	Annunciate time interval, unit: second, default: 1s, valid range is 1-10 seconds.
Preemption mode	Preemption mode, options as follows: • false; • true.
Enable	Enable switch, options are as follows: • Enable; • Disable.
Operation	Click “Edit” under “Operation” to re-edit VRRP configuration

Interface Element	Description
	information; Click “Delete” under “Operation” to delete the entry directly.

6.4NAT Settings

NAT (Network Address Translation) maps private IP address to the legal IP address of external network, which can slow the consumption of IP address space.

6.4.1 NAT Port Binding

Function Description

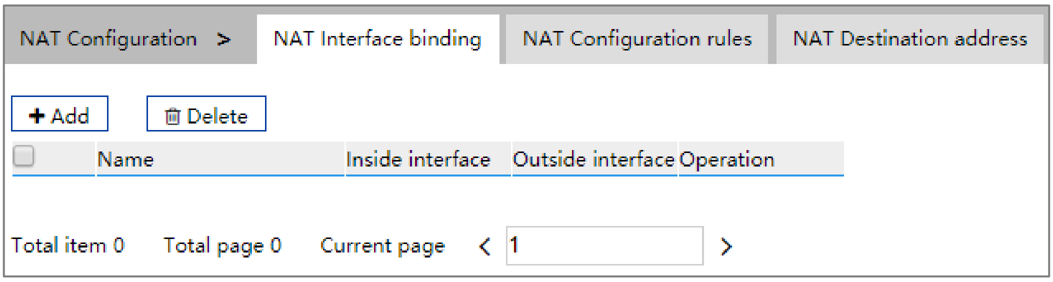
On the “NAT interface binding” page, you can bind NAT layer 3 interfaces.

Operation Path

Open in order: "Layer 3 configuration > NAT Configuration > NAT Interface Binding".

Interface Description

The NAT interface binding interface is as follows:



Configuration description of main elements of NAT interface binding interface.

Interface Element	Description
Add	Click "Add" button to add NAT port binding
Delete	Check NAT port binding information to be deleted, and click “Delete” to delete it
ID	The serial number of NAT port binding
Name	The name of NAT port binding, up to 20 characters
Inside interface	In-car layer 3 interface Note: This parameter can be configured only when the device has set VLAN and bound ports.
Outside interface	Out-car layer 3 interface

Interface Element	Description
	Note: This parameter can be configured only when the device has set VLAN and bound ports.

Instance: typical NAT Port Binding

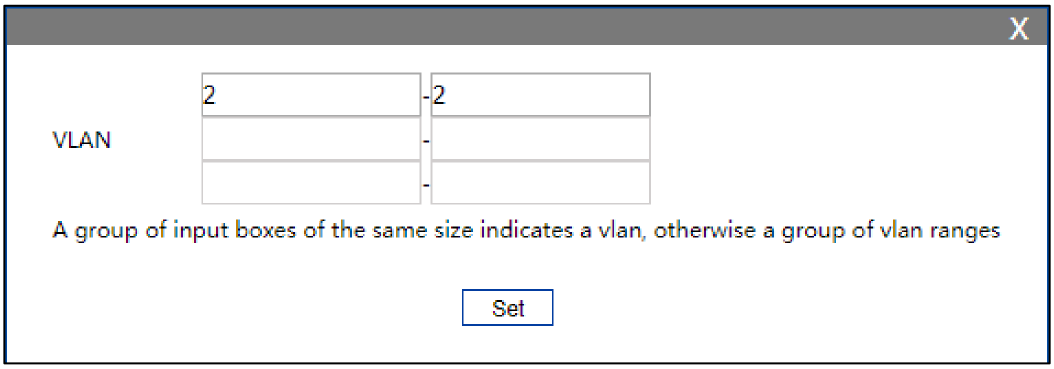
Assume that the switch physical port ge2 that connects external network is out-car interface, the other ports are in-car interfaces. First, port ge2 can be divided into VLAN2 and other ports into VLAN1. Then, VLAN1 and VLAN2 can be configured as the corresponding layer 3 interface, and the IP address and mask of the three-layer interface can be configured. Finally, interface binding can be performed.

Operation Steps

步骤 **1** Divide port ge2 into VLAN2 and other ports into VLAN1.

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

2 Click “Add” and enter 2 in "Vlan " text box as shown below:



VLAN 2 - 2

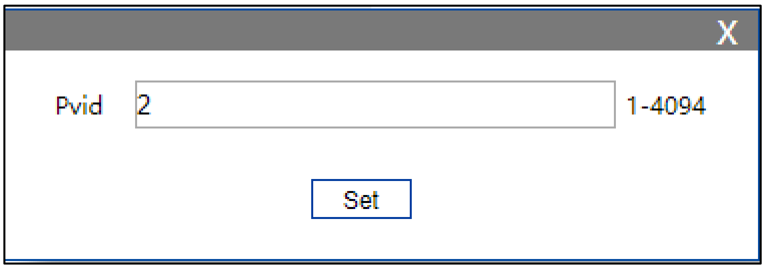
A group of input boxes of the same size indicates a vlan, otherwise a group of vlan ranges

3 Click “Apply” button.

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

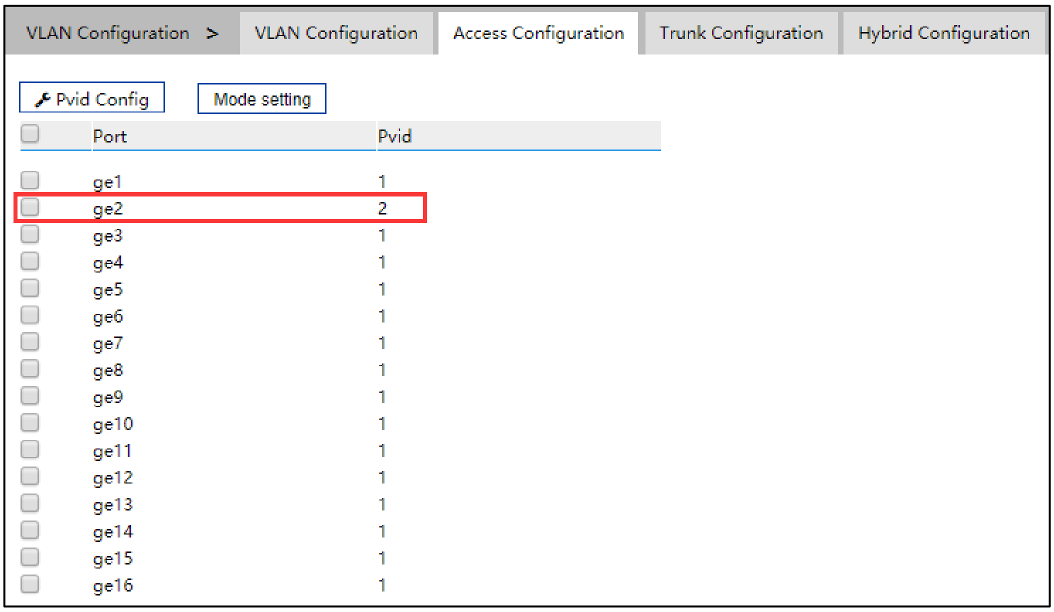
5 Check port 2 and click "Configure".

6 Enter 2 in the box that pops up.



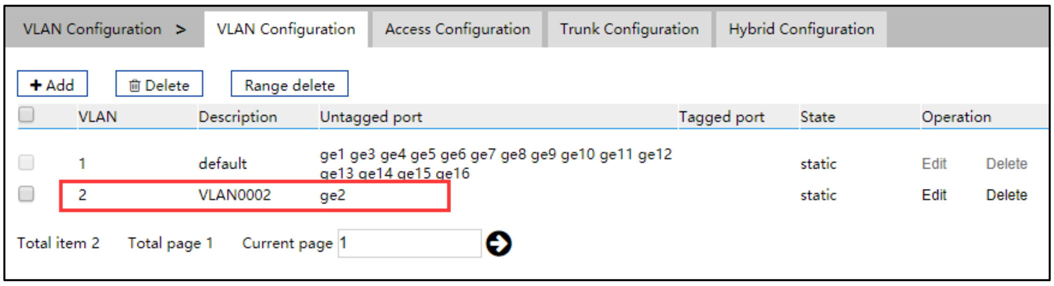
Pvid 2 1-4094

7 Click “Apply” button.



□	Port	Pvid
□	ge1	1
□	ge2	2
□	ge3	1
□	ge4	1
□	ge5	1
□	ge6	1
□	ge7	1
□	ge8	1
□	ge9	1
□	ge10	1
□	ge11	1
□	ge12	1
□	ge13	1
□	ge14	1
□	ge15	1
□	ge16	1

8 Enter “Layer 2 Config > VLAN Config > VLAN Config”, confirm setting.



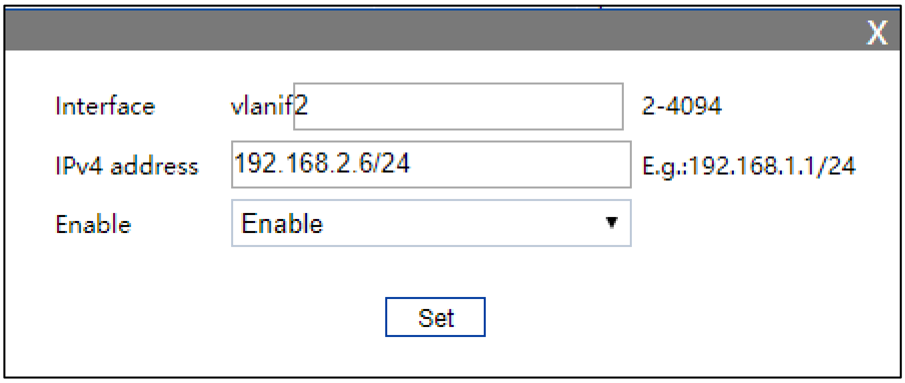
□	VLAN	Description	Untagged port	Tagged port	State	Operation	
□	1	default	ge1 ge3 ge4 ge5 ge6 ge7 ge8 ge9 ge10 ge11 ge12 ge13 ge14 ge15 ge16		static	Edit	Delete
□	2	VLAN0002	ge2		static	Edit	Delete

Total item 2 Total page 1 Current page 1

步骤 **2** Configure VLAN1 and VLAN2 as the corresponding layer 3 interface, and configure the IP address and mask of the layer 3 interface.

1 Enter “Layer 3 Config > Interface Config > Layer 3 Interface”.

2 Click “Add”. Enter “2” in the “Interface”, “192.168.2.6/24” in the “IPv4 address”, select “enable” in the “interface switch”.

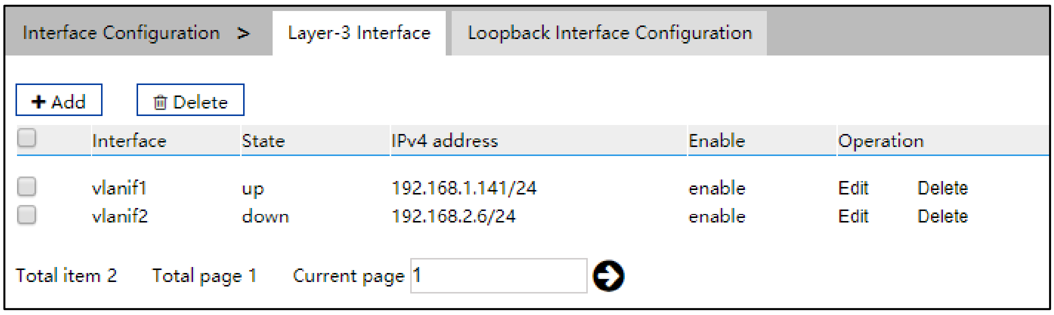


Interface vlanif2 2-4094

IPv4 address 192.168.2.6/24 E.g.:192.168.1.1/24

Enable Enable

3 Click “Apply”.



□	Interface	State	IPv4 address	Enable	Operation	
□	vlanif1	up	192.168.1.141/24	enable	Edit	Delete
□	vlanif2	down	192.168.2.6/24	enable	Edit	Delete

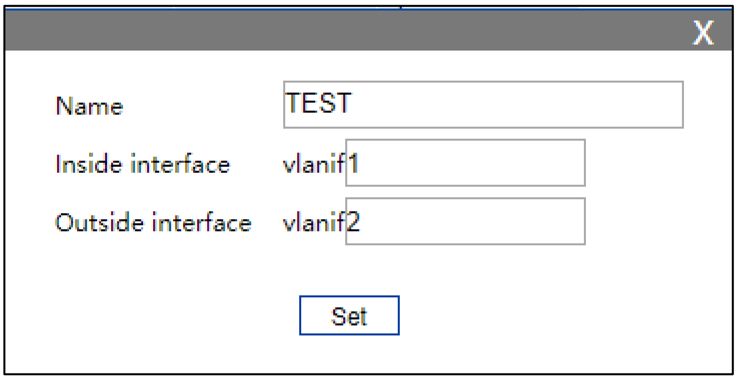
Total item 2 Total page 1 Current page 1

步骤 **3** NAT port binding

1 Enter: "Layer 3 Configuration > NAT Config > NAT Port Binding".

2 Click “Add”.

3 Enter "TEST" in the pop-up window "Name", enter "1" in the "In-car interface" and "2" in the "Out-car interface".

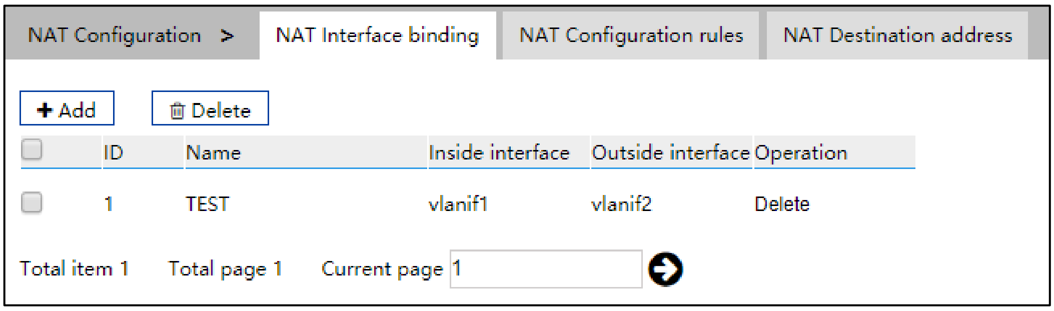


Name TEST

Inside interface vlanif 1

Outside interface vlanif 2

4 Click “Apply”.



□	ID	Name	Inside interface	Outside interface	Operation
□	1	TEST	vlanif1	vlanif2	Delete

Total item 1 Total page 1 Current page 1

步骤 **4** End.

6.4.2 NAT Configuration Rule

Function Description

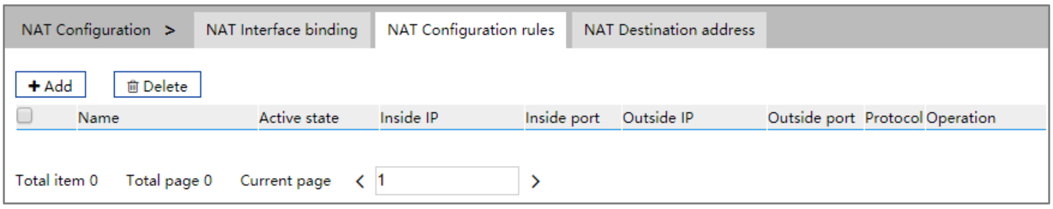
On the "NAT Config Rule" page, user can configure NAT rule.

Operation Path

Open in order: "L3 Config > NAT Config > NAT Config Rule".

Interface Description

NAT configuration rule interface is as follows:



Main elements configuration description of NAT configuration rule interface:

Interface Element	Description
Add	Click "Add" button to add NAT configuration rule
Delete	Check NAT configuration rule to be deleted, and click “Delete” to delete it
ID	NAT rule ID.
Name	The name of NAT rule, up to 20 characters
Active state	Activation state ● Disable ● Enable Note: The out-car IP to be accessed can be activated only when it exists
Inside IP	IP address of intranet device.
Inside Port	Port number of intranet device.
Outside IP	IP address corresponding to external network interface.
Outside Port	The corresponding port number of external network port.
Protocol	Type of protocol, available value: ● TCP ● UDP ● All
DST	The destination IP address and mask for access.
Operation	Click the "Delete" button under the operation to delete this NAT configuration rule.

6.4.3 NAT Destination Address

Function Description

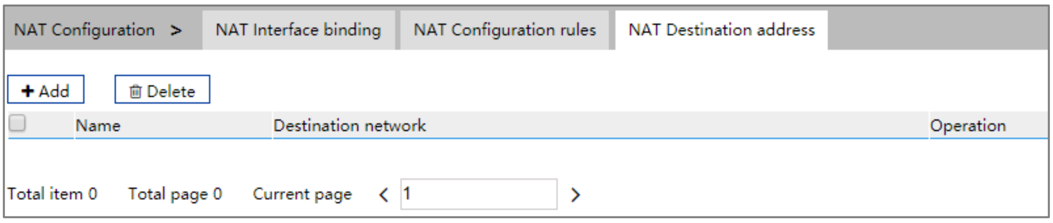
On the “NAT Destination Address” page, you can configure the NAT destination network address.

Operation Path

Open in order: "Layer 3 Configuration > NAT Configuration > NAT Destination Address".

Interface Description

The NAT destination address interface is as follows:



Main elements configuration description of NAT configuration rule interface:

Interface Element	Description
Name	NAT rule name.
Destination network	Destination network address converted from NAT message.
Operation	Click “Delete” under “Operation” to delete the corresponding entry.

6.5IGMP Configuration

6.5.1 Interface Configuration

Function Description

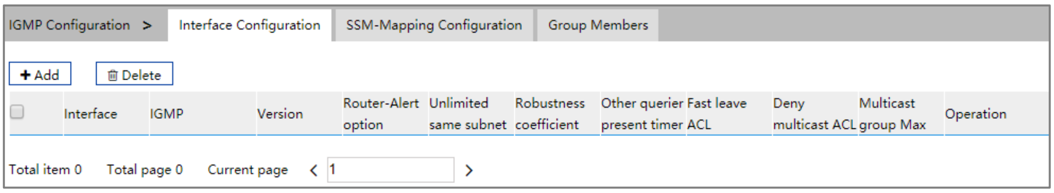
On the interface configuration page, user can add or delete IGMP configuration of Ethernet ports.

Operation Path

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

Interface Description

Interface configuration interface as follows:



□	Interface	IGMP	Version	Router-Alert option	Unlimited same subnet	Robustness coefficient	Other querier present timer	Fast leave ACL	Deny multicast ACL	Multicast group Max	Operation

Total item 0 Total page 0 Current page < 1 >

The main element configuration description of interface configuration interface:

Interface Element	Description
IGMP	IGMP status: • enable; • disable.
Interface	Layer 3 interface, such as vlanif1.
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 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

Interface Element	Description
	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 multicasts supported.
Operation: edit	Modify IGMP entries.
Operation: delete	Delete the current IGMP entry.

6.5.2 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

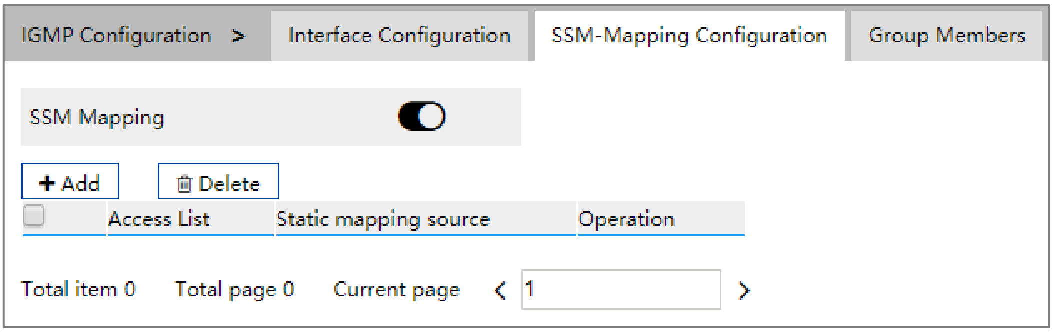
On the interface configuration page, user can add or delete IGMP configuration of Ethernet ports.

Operation Path

Open in order: "L3 Configuration > 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	Note
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	The specified multicast source address in the access list.

Interface Element	Note
source	

6.5.3 Multicast Group Information

Function Description

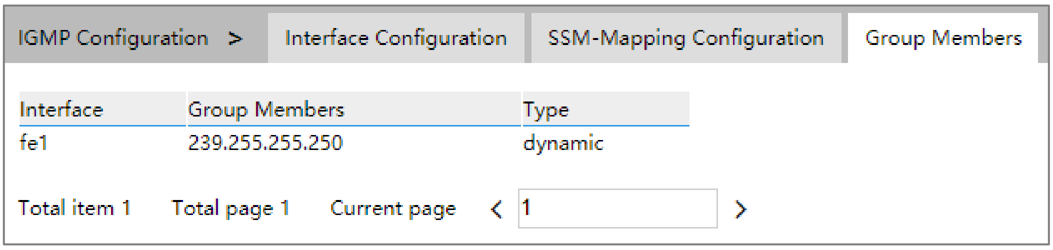
On the "Multicast Group Information" page, display the multicast information received by the device interface.

Operation Path

Open in order: "L3 Configuration > IGMP Configuration > Multicast Group Information".

Interface Description

The multicast group information interface is as follows:



Interface	Group Members	Type
fe1	239.255.255.250	dynamic

Total item 1 Total page 1 Current page < 1 >

Main element configuration description of multicast group information interface:

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

6.6PIM-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

6.6.1 Global Configuration

Function Description

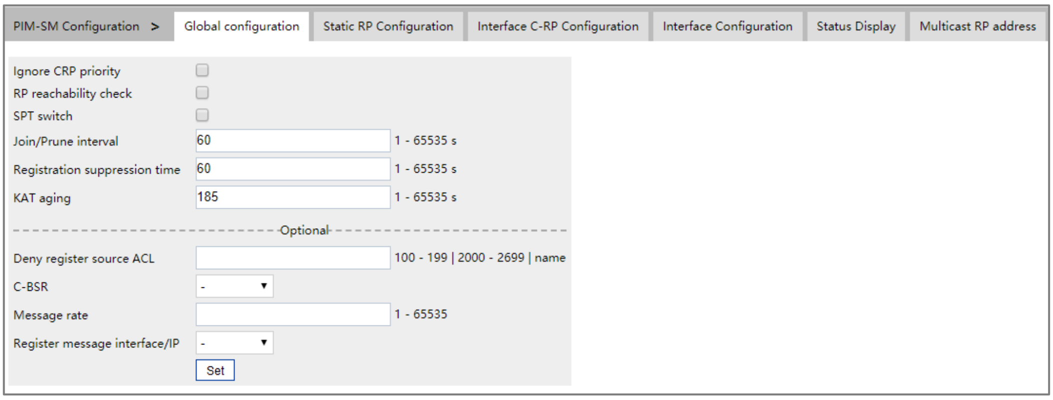
On the global configuration page, user can configure the global parameters of PIM-SM.

Operation Path

Open in order: "L3 Configuration > PIM-SM Configuration > Global Configuration".

Interface Description

Global configuration interface is as follows:



Ignore CRP priority □
RP reachability check □
SPT switch □
Join/Prune interval 60 1 - 65535 s
Registration suppression time 60 1 - 65535 s
KAT aging 185 1 - 65535 s

Optional

Deny register source ACL 100 - 199 | 2000 - 2699 | name
C-BSR -
Message rate 1 - 65535
Register message interface/IP -

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.
Add/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 suppression time	The time interval for sending the registration message again 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.

Interface Element	Description
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.

6.6.2 Static RP Configuration

Function Description

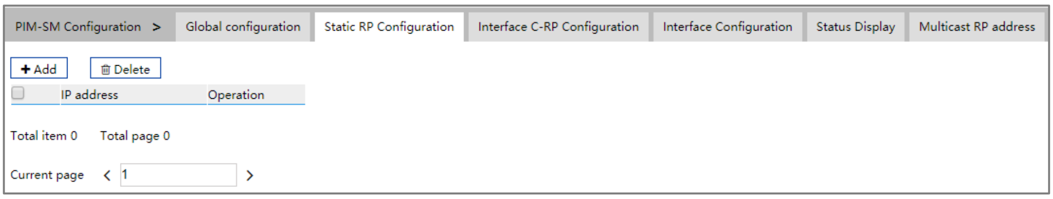
On the static RP configuration page, you can set up the static RP manually.

Operation Path

Open in order: "L3 Configuration > PIM-SM Configuration > Static RP Configuration".

Interface Description

Static RP configuration interface as follow:



□	IP address	Operation

Total item 0 Total page 0

Current page < 1 >

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.

6.6.3 C-RP Configuration of Interface

Function Description

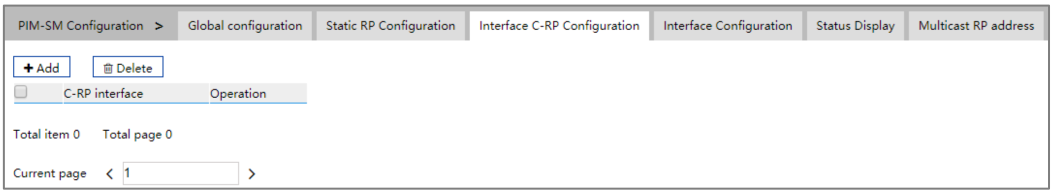
On the interface C-RP configuration page, you can add or delete C-RP interfaces.

Operation Path

Open in order: "L3 Configuration > PIM-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.

6.6.4 Interface Configuration

Function Description

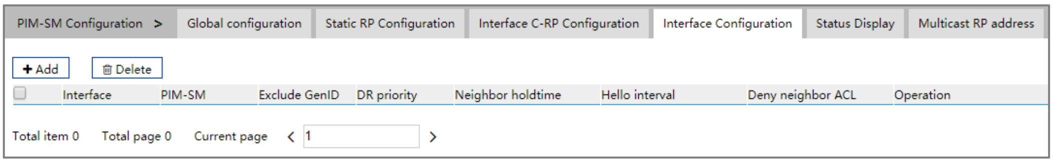
On the "Interface Configuration" page, user can set interface PIM- SM parameters.

Operation Path

Open in order: "L3 Configuration > PIM-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.

6.6.5 Status Display

Function Description

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

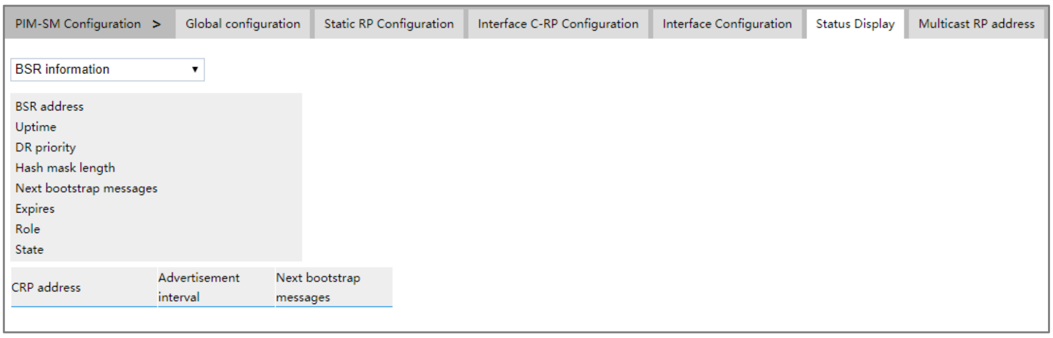
- BSR information
- Interface information
- Local multicast
- Multicast routing table
- Neighbor
- Next hop information
- RP-Set information

Operation Path

Open in order: "L3 Configuration > PIM-SM Configuration > Status Display".

Interface Description

The status display interface is as follows:



BSR address
Uptime
DR priority
Hash mask length
Next bootstrap messages
Expires
Role
State

CRP address	Advertisement interval	Next bootstrap messages

6.6.6 Multicast PR Address

Function Description

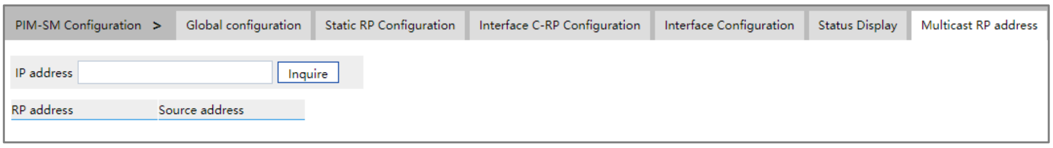
In multicast RP address, user can query the multicast RP address.

Operation Path

Open in order: "L3 Configuration > PIM-SM Configuration > Multicast RP Address".

Interface Description

The multicast RP address interface is as follows:



IP address

RP address	Source address

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.

6.7 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

6.7.1 Global Configuration

Function Description

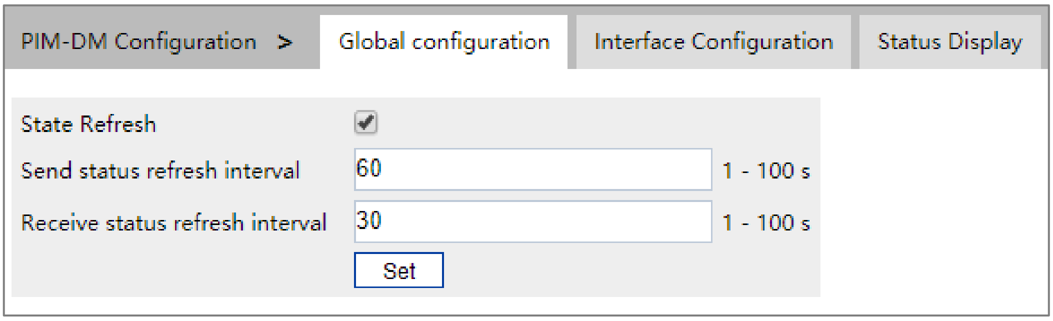
On the Global Configuration page, user can refresh the pruning timer status and set the time interval between sending status and receiving status.

Operation Path

Open in order: "L3 Configuration > PIM-DM Configuration > Global Configuration".

Interface Description

Global configuration interface is as follows:



State Refresh ☑

Send status refresh interval 60 1 - 100 s

Receive status refresh interval 30 1 - 100 s

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.

6.7.2 Interface Configuration

Function Description

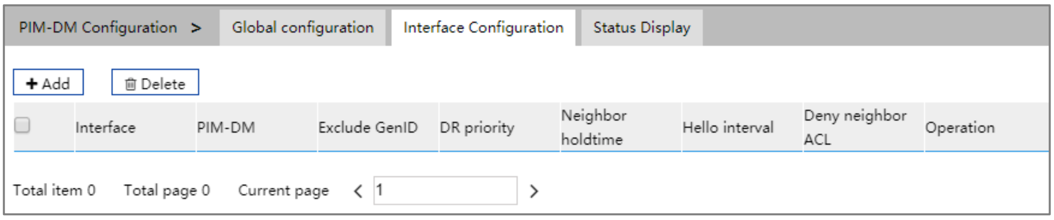
On the "Interface Configuration” page, user can configure interface PIM-DM parameters.

Operation Path

Open in order: "L3 Configuration > PIM-DM Configuration > Interface Configuration".

Interface Description

Interface configuration interface as follows:



□	Interface	PIM-DM	Exclude GenID	DR priority	Neighbor holdtime	Hello interval	Deny neighbor ACL	Operation

Total item 0 Total page 0 Current page < 1 >

The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	Configure interface:

Interface Element	Description
	● vlanif: vlanif interface; ● Loopback：loopback interface.
Operation: delete	Delete the candidate convergence point entry in the current line.
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.

6.7.3 Status Display

Function Description

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

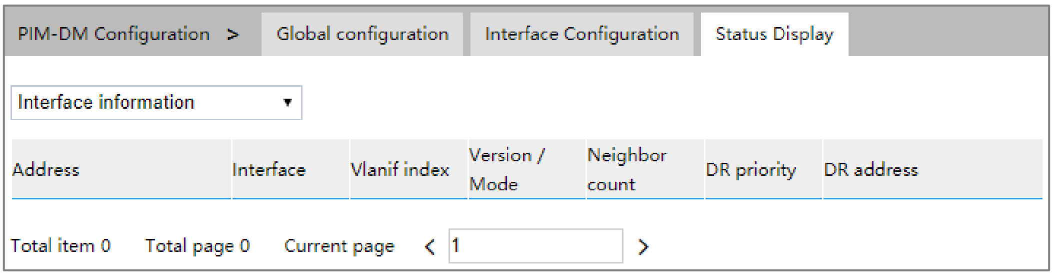
- BSR information
- Interface information
- Local multicast
- Multicast routing table
- Neighbor
- Next hop information
- RP-Set information

Operation Path

Open in order: "L3 Configuration > PIM-DM Configuration > Status Display".

Interface Description

The status display interface is as follows:



Interface information ▼

Address	Interface	Vlanif index	Version / Mode	Neighbor count	DR priority	DR address

Total item 0 Total page 0 Current page < 1 >

7 Router Configuration

7.1 IPv4 Configuration

7.2 IPv4 Routing Table

Function Description

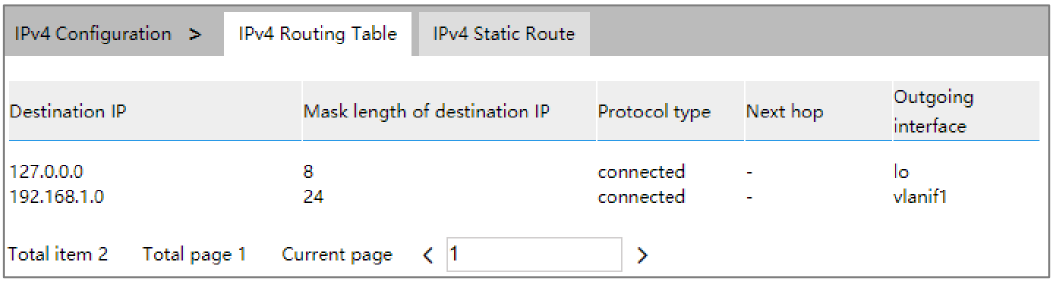
On the "IPv4 Routing Table" page, user can check various router configuration methods.

Operation Path

Open in order: "Main Menu > IPv4 Configuration > IPv4 Routing Table".

Interface Description

The IPv4 routing table interface as follows:



Destination IP	Mask length of destination IP	Protocol type	Next hop	Outgoing interface
127.0.0.0	8	connected	-	lo
192.168.1.0	24	connected	-	vlanif1

Total item 2 Total page 1 Current page < 1 >

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;C - connected;S – static;R – RIP;O – OSPF;I -

Interface Element	Description
	IS-IS;B – BGP;A – Babel;> - selected route;* - FIB route.
Next hop	Gateway address information of next hop.
Outgoing port	Interface Name.

7.3 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

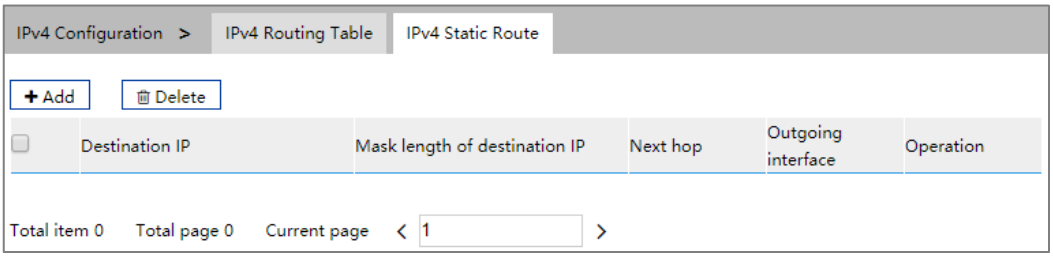
On the "IPv4 Static Route" page, user can configure static route.

Operation Path

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

Interface Description

The IPv4 Static Route interface as follows:



□	Destination IP	Mask length of destination IP	Next hop	Outgoing interface	Operation

Total item 0 Total page 0 Current page < 1 >

The main element configuration description of IPv4 Static Route interface:

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

7.4RIP 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.

7.4.1 RIP Global Configuration

Function Description

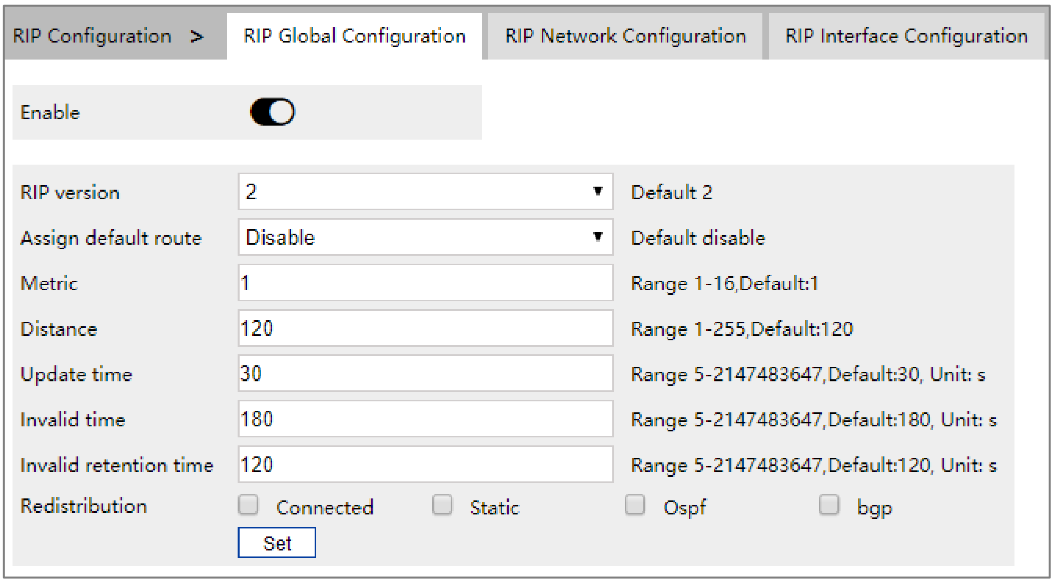
On the "RIP Global Config" page, user can conduct RIP global relative parameters configuration.

Operation Path

Open in order: "Route Configuration > RIP Configuration > RIP Global Configuration".

Interface Description

RIP global configuration interface as follows:



Enable	●	
RIP version	2 ▾	Default 2
Assign default route	Disable ▾	Default disable
Metric	1	Range 1-16,Default:1
Distance	120	Range 1-255,Default:120
Update time	30	Range 5-2147483647,Default:30, Unit: s
Invalid time	180	Range 5-2147483647,Default:180, Unit: s
Invalid retention time	120	Range 5-2147483647,Default:120, Unit: s
Redistribution	□ Connected □ Static □ Ospf □ bgp	

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:

Interface Element	Description
	• 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 router.	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 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:

Interface Element	Description
	● 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.
Network Configuration	**Network Configuration Bar**
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.

7.4.2 RIP Network Setting

Function Description

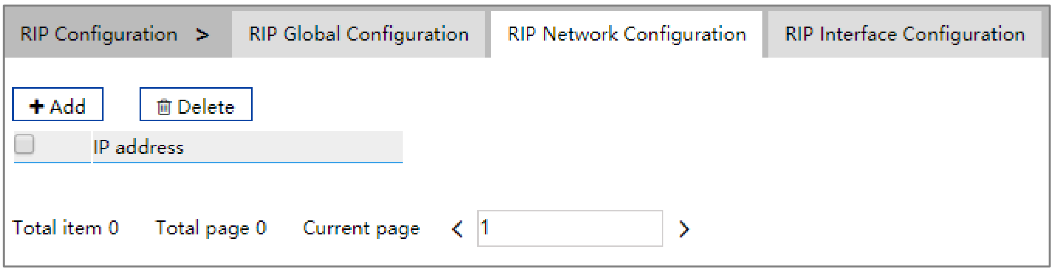
On the “RIP Network Configuration” page, user can configure the RIP network address.

Operation Path

Open in order: "Route Config > RIP Config > RIP Network Setting".

Interface Description

RIP network setting interface as follows:



The main element configuration description of RIP global configuration interface:

Interface Element	Description
IP Address	IP address of the network interface of RIP protocol.

7.4.3 RIP Interface Configuration

Function Description

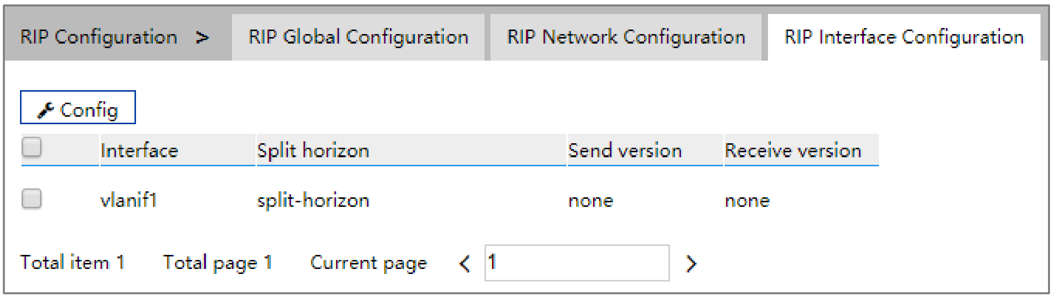
On the "RIP Interface Configuration" page, user can conduct RIP network parameter configuration.

Operation Path

Open in order: "Route Configuration > RIP Configuration > RIP Interface Configuration".

Interface Description

RIP interface configuration interface as follows:



□	Interface	Split horizon	Send version	Receive version
□	vlanif1	split-horizon	none	none

Total item 1 Total page 1 Current page < 1 >

The main element configuration description of interface configuration interface:

Interface Element	Description
Interface	RIP interface information
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 Advanced Configuration

8.1 DHCP 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.

8.1.1 DHCP Switch

Function Description

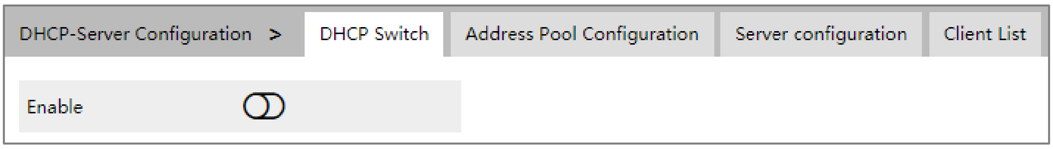
On the "DHCP Switch" page, user can enable/disable DHCP.

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.

8.1.2 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-side 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. Same level address pool order 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

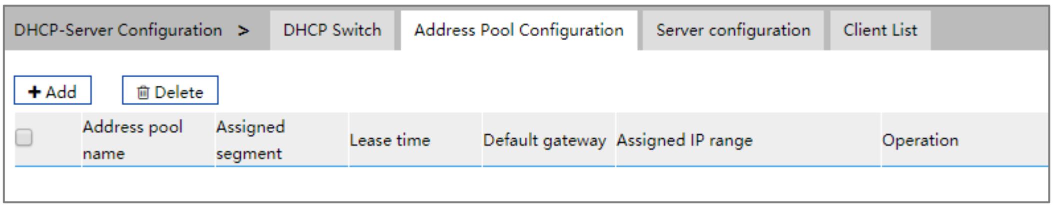
On the "DHCP Pool Config" page, user can add, delete the address pool and look over the configuration information of address pool.

Operation Path

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

Interface Description

DHCP address pool configuration interface as follows:



DHCP-Server Configuration >	DHCP Switch	Address Pool Configuration	Server configuration	Client List	

□	Address pool name	Assigned segment	Lease time	Default gateway	Assigned IP range	Operation

The main element configuration description of DHCP pool configuration interface:

Interface Element	Description
Address pool	The name of address pool, up to 32 characters.
Assigned segment	Address pool distributes the IP address network segment of client-side, 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.

8.1.3 Server Configuration

Function Description

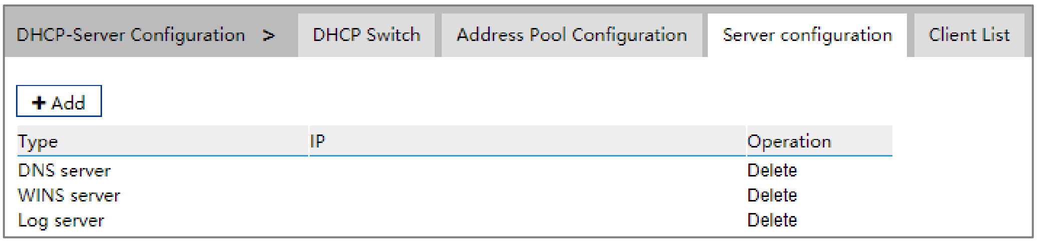
On the "Address Pool Server Config" page, user can add, delete DNS/WINS/Log Server Address Pool.

Operation Path

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

Interface Description

Server configuration interface as follows:



Type	IP	Operation
DNS server		Delete
WINS server		Delete
Log server		Delete

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.

8.1.4 Client List

Function Description

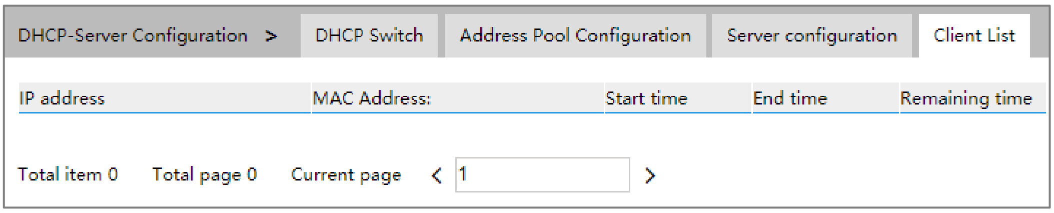
On the "Client List" page, user can look over the information of DHCP client-side.

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.
MAC Address	MAC address of DHCP client-side device.
Start time	Valid start time of DHCP client.
End time	Valid end time of DHCP client.
End time	Valid remaining time of DHCP client.

8.2 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).

8.2.1 Global Configuration

Function Description

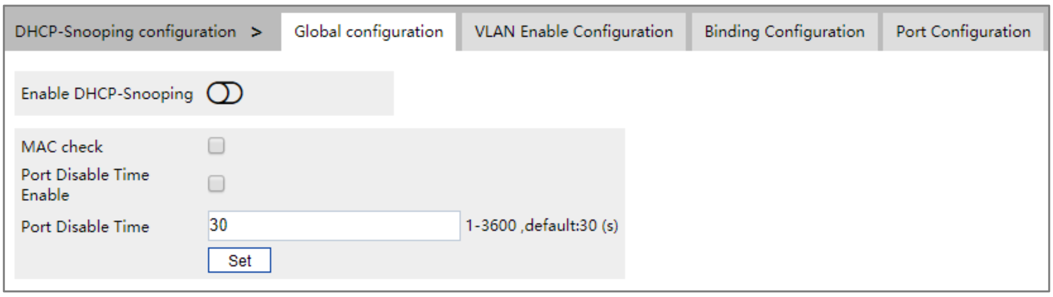
On the “Global Configuration” page, user can enable/disable DHCP Snooping.

Operation Path

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

Interface Description

Global configuration interface is as follows:



DHCP-Snooping configuration > Global configuration | VLAN Enable Configuration | Binding Configuration | Port Configuration

Enable DHCP-Snooping ○

MAC check □

Port Disable Time Enable □

Port Disable Time 30 1-3600 ,default:30 (s)

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. 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.

8.2.2 VLAN Enable Configuration

Function Description

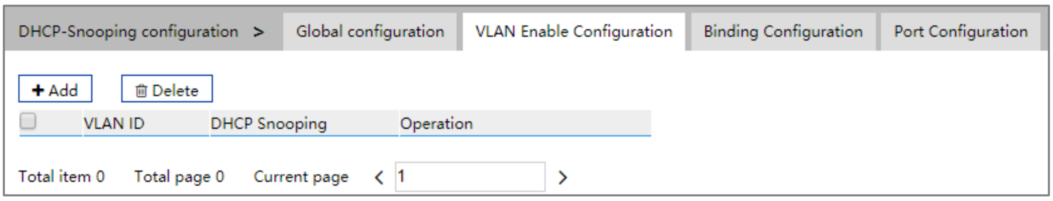
On the "VLAN Enable Configuration" page, user can specify that the VLAN to enable DHCP Snooping.

Operation Path

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

Interface Description

The Vlan enable configuration interface is as follows:



DHCP-Snooping configuration > Global configuration | VLAN Enable Configuration | Binding Configuration | Port Configuration

□	VLAN ID	DHCP Snooping	Operation

Total item 0 Total page 0 Current page < 1 >

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 ● disable
Operation: delete	Delete the current VLAN enable entry

8.2.3 Binding Configuration

Function Description

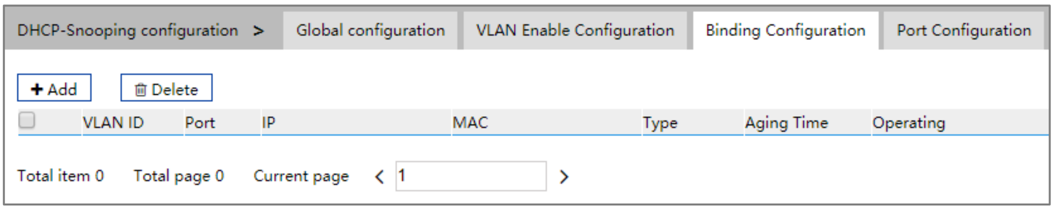
On the Binding Configuration page, user can bind ports, IP addresses and MAC addresses.

Operation Path

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

Interface Description

The binding configuration interface is as follows:



□	VLAN ID	Port	IP	MAC	Type	Aging Time	Operating

Total item 0 Total page 0 Current page < 1 >

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.

8.2.4 Port Configuration

Function Description

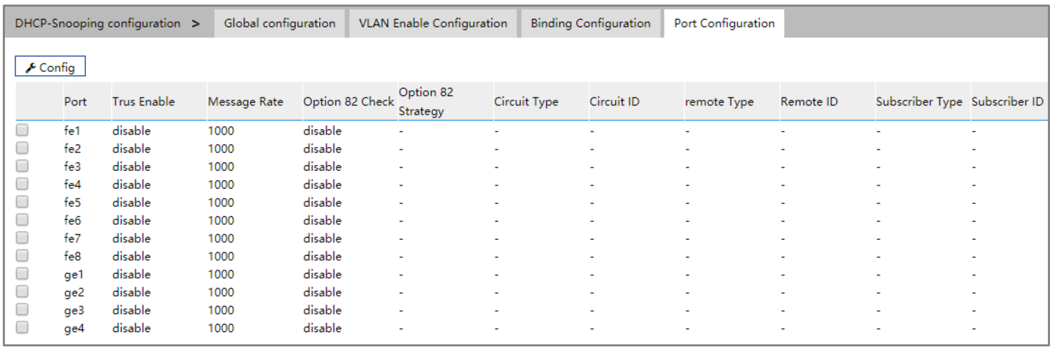
On the port configuration page, user can configure DHCP Snooping port information.

Operation Path

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

Interface Description

Check port configuration interface as below:



	Port	Trus Enable	Message Rate	Option 82 Check	Option 82 Strategy	Circuit Type	Circuit ID	remote Type	Remote ID	Subscriber Type	Subscriber ID
□	fe1	disable	1000	disable	-	-	-	-	-	-	-
□	fe2	disable	1000	disable	-	-	-	-	-	-	-
□	fe3	disable	1000	disable	-	-	-	-	-	-	-
□	fe4	disable	1000	disable	-	-	-	-	-	-	-
□	fe5	disable	1000	disable	-	-	-	-	-	-	-
□	fe6	disable	1000	disable	-	-	-	-	-	-	-
□	fe7	disable	1000	disable	-	-	-	-	-	-	-
□	fe8	disable	1000	disable	-	-	-	-	-	-	-
□	ge1	disable	1000	disable	-	-	-	-	-	-	-
□	ge2	disable	1000	disable	-	-	-	-	-	-	-
□	ge3	disable	1000	disable	-	-	-	-	-	-	-
□	ge4	disable	1000	disable	-	-	-	-	-	-	-

The main element configuration description of global configuration interface:

Interface Element	Description
Port	The port name corresponding to the Ethernet port of this device.
Trust enable	Port trust enable, and the trust port forwards the received DHCP message normally.
Message rate	Message transmission rate of the port, the input range is 10-1000 (s), and the default value is 1000s.
Option 82 check	When Option 82 check is enabled, the location information of DHCP client can be obtained from Option 82, so as to locate DHCP client.
Option 82 strategy	Option 82 processing strategy, options are as follows: ● Drop: drop the message. ● Keep: fill Option 82 with different modes, replace the original Option 82 in the message and forward it. The filling mode will be described below. ● Replace: keep Option 82 in the message unchanged and forward it.

Interface Element	Description
Circuit type	Circuit ID sub-option fill type, with the following options: • Normal: normal mode; • String: string mode.
Circuit ID	The filling content of circuit 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.
Remote type	The remote ID sub-option fill type is as follows: • Normal: normal mode; • Sysname: directly use the device system name to fill Option 82; • String: string 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	Subscriber option fill type 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.

8.3 DHCP-Relay Configuration

Function Description

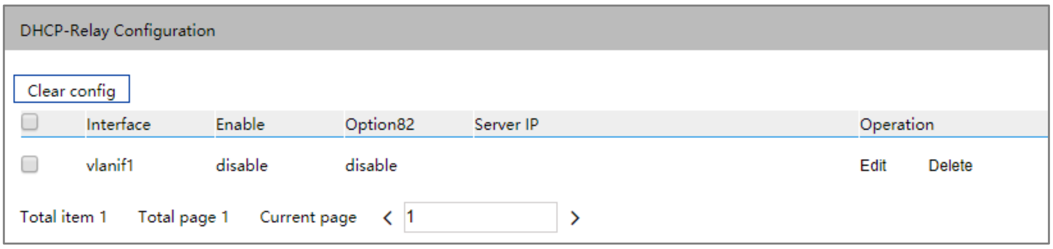
On the "DHCP-Relay Configuration" page, user can configure the relevant parameters of Relay port.

Operation Path

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

Interface Description

DHCP-Relay configuration interface is as follows:



DHCP-Relay Configuration

Clear config

□	Interface	Enable	Option82	Server IP	Operation
□	vlanif1	disable	disable		Edit Delete

Total item 1 Total page 1 Current page < 1 >

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.
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.

8.4 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 described that LLDP is only a remote device status information discovery protocol, which cannot complete the network device configuration, port control and other functions.

8.4.1 Current configuration

Function Description

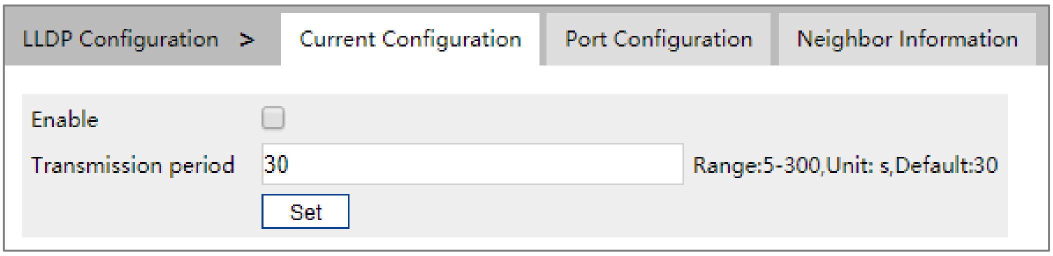
On the "Current Config" page, user can configure the relevant parameters of LLDP.

Operation Path

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

Interface Description

The current configuration interface is as follows:



Enable □

Transmission period 30 Range:5-300,Unit: s,Default:30

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.

8.4.2 Port Configuration

Function Description

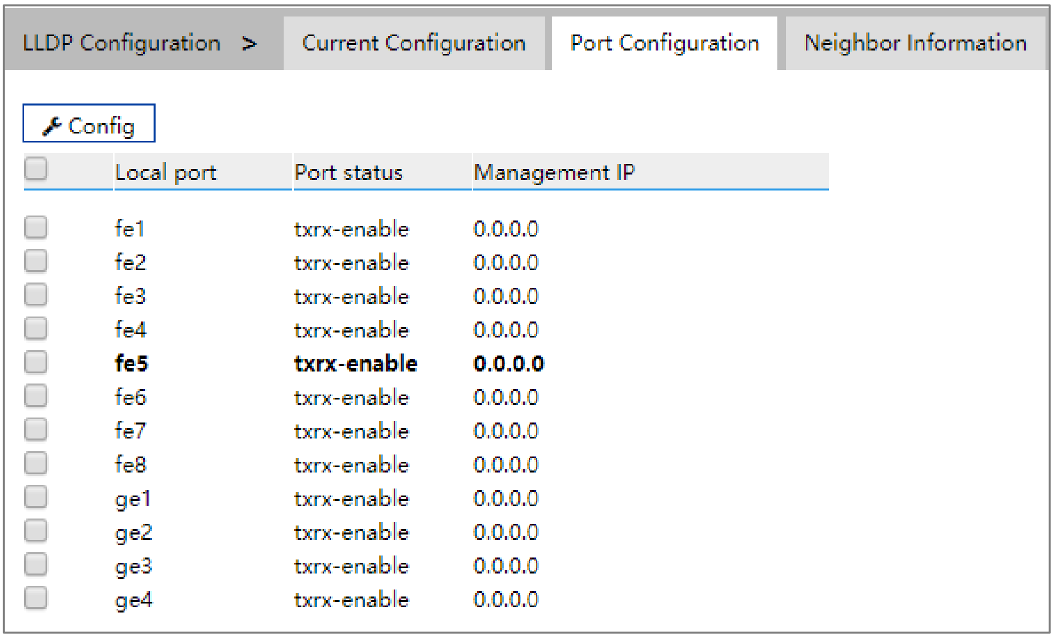
On the "Port Config" page, user can configure the sending and receiving mode and management address of the port.

Operation Path

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

Interface Description

Check port configuration interface as below:



□	Local port	Port status	Management IP
□	fe1	txrx-enable	0.0.0.0
□	fe2	txrx-enable	0.0.0.0
□	fe3	txrx-enable	0.0.0.0
□	fe4	txrx-enable	0.0.0.0
□	**fe5**	**txrx-enable**	**0.0.0.0**
□	fe6	txrx-enable	0.0.0.0
□	fe7	txrx-enable	0.0.0.0
□	fe8	txrx-enable	0.0.0.0
□	ge1	txrx-enable	0.0.0.0
□	ge2	txrx-enable	0.0.0.0
□	ge3	txrx-enable	0.0.0.0
□	ge4	txrx-enable	0.0.0.0

The main element configuration description of global 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 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

Interface Element	Description
	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.

8.4.3 Neighbor Information

Function Description

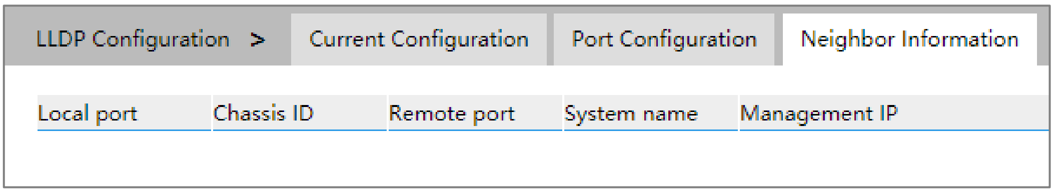
On the "Neighbors Information" page, user can look over the relative information of neighbors.

Operation Path

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

Interface Description

Neighbor information interface as follows:



Local port	Chassis ID	Remote port	System name	Management IP

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.

8.5NTP 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

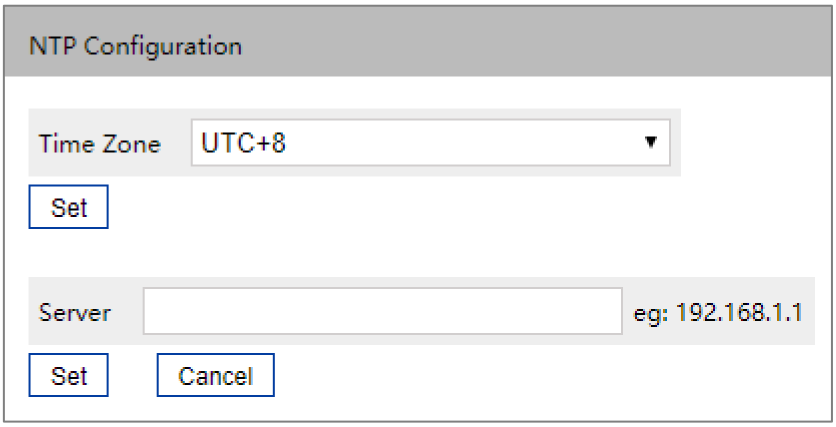
On the "NTP Config" page, user can configure the device time and NTP server information.

Operation Path

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

Interface Description

NTP configuration interface as follows:



NTP Configuration

Time Zone: UTC+8

Server: eg: 192.168.1.1

The main element configuration description of NTP configuration interface:

Interface Element	Description
Timezone	UTC(Universal Time Coordinated) time zone.
Server	IP address of NTP server, for example: 192.168.1.1.

9 System Maintenance

9.1 Configure File Management

9.1.1 Global Configuration

Function Description

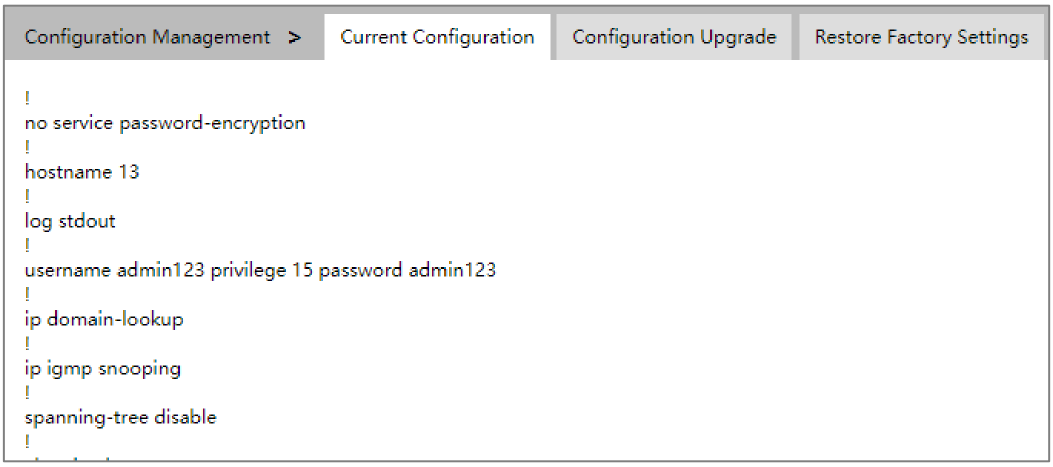
On the "Current Configuration" page, user can view current configuration information.

Operation Path

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

Interface Description

Global configuration interface is as follows:



```
!
no service password-encryption
!
hostname 13
!
log stdout
!
username admin123 privilege 15 password admin123
!
ip domain-lookup
!
ip igmp snooping
!
spanning-tree disable
!
```

9.1.2 Configuration File Update

Function Description

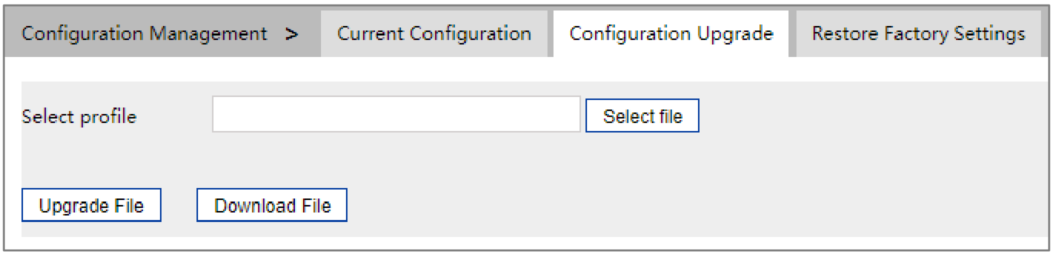
On the "Management File" page, user can download and upload configuration file.

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
Select 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.

9.1.3 Restore Factory Settings

Function Description

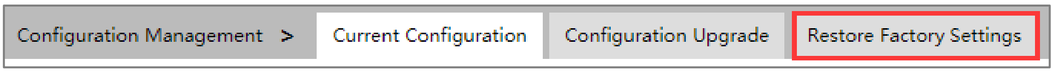
On the "Restore Factory Settings" page, user can restore the device to default setting.

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 interface:

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

9.2 Alarm Configuration

9.2.1 Port Alarm

Function Description

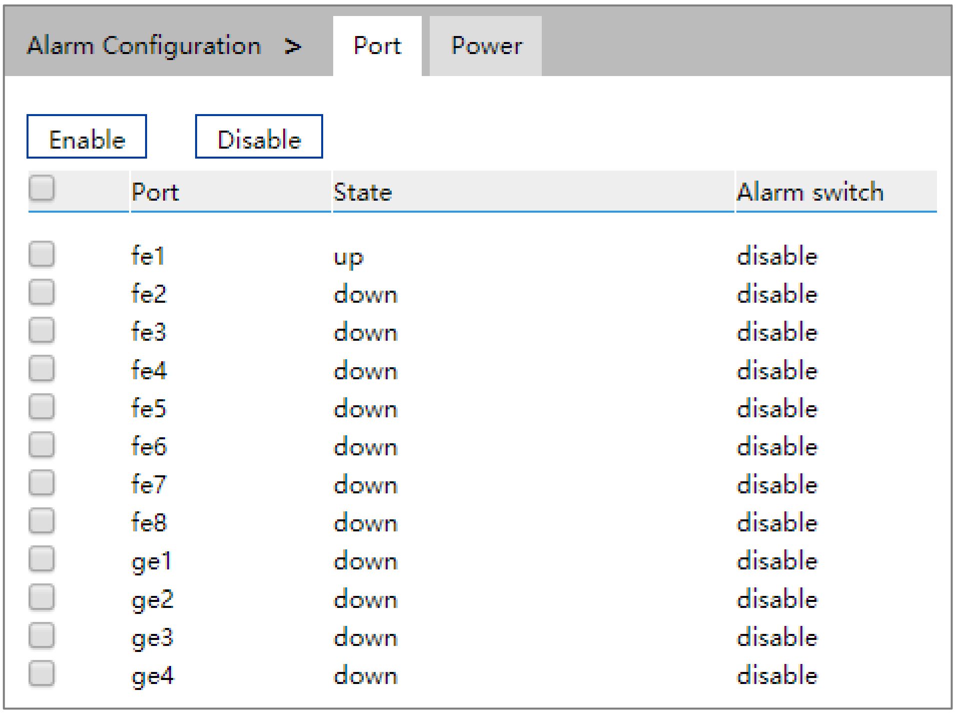
On the "Port Configuration" page, user can set the port alarm function. When the device port is in an abnormal state, the administrator can be informed in time, and the device state can be quickly repaired to avoid excessive loss.

Operation Path

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

Interface Description

Port alarm interface as below:



□	Port	State	Alarm switch
□	fe1	up	disable
□	fe2	down	disable
□	fe3	down	disable
□	fe4	down	disable
□	fe5	down	disable
□	fe6	down	disable
□	fe7	down	disable
□	fe8	down	disable
□	ge1	down	disable
□	ge2	down	disable
□	ge3	down	disable
□	ge4	down	disable

The main element configuration description of alarm information interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
State	Port link status, display items as follows: • up; • down.
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.
Close	Check the port that needs to disable port alarm, and click disable to disable this function.

9.2.2 Power Alarm

Function Description

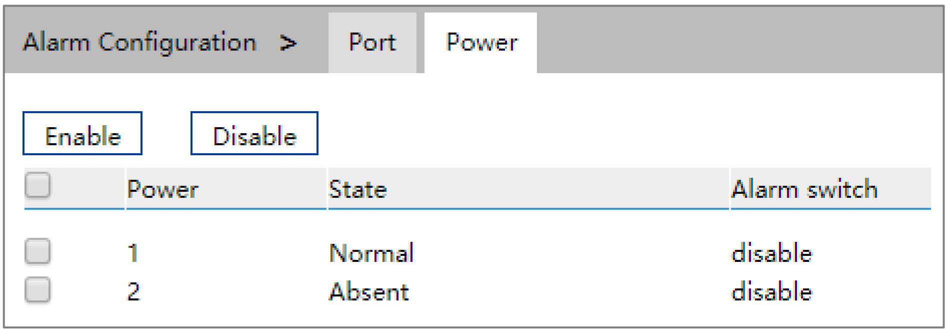
On the "Power Alarm" page, user can configure the alarm functions of the power supply.

Operation Path

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

Interface Description

Power alarm interface as below:



□	Power	State	Alarm switch
□	1	Normal	disable
□	2	Absent	disable

The main element configuration description of port alarm interface:

Interface Element	Description

Interface Element	Description
Power	The corresponding name of this device's power supply
State	Device power link status, display items as follows: • Normal; • Absent.
Alarm switch	The state of power supply alarm function, options: • Enable; • Disable.
Enable	Check the port that needs to enable power alarm, and click enable to enable this function.
Close	Check the port that needs to disable power alarm, and click disable to disable this function.

9.3 Upgrade

Function Description

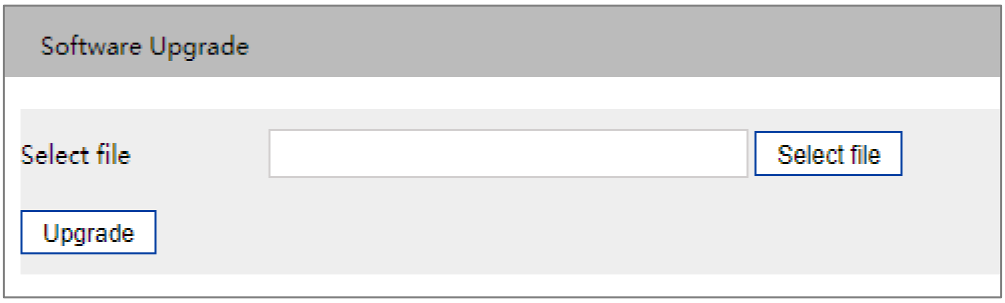
On the "Software Upgrade" page, user can update and upgrade the device procedure via TFTP server.

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.

9.4 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.

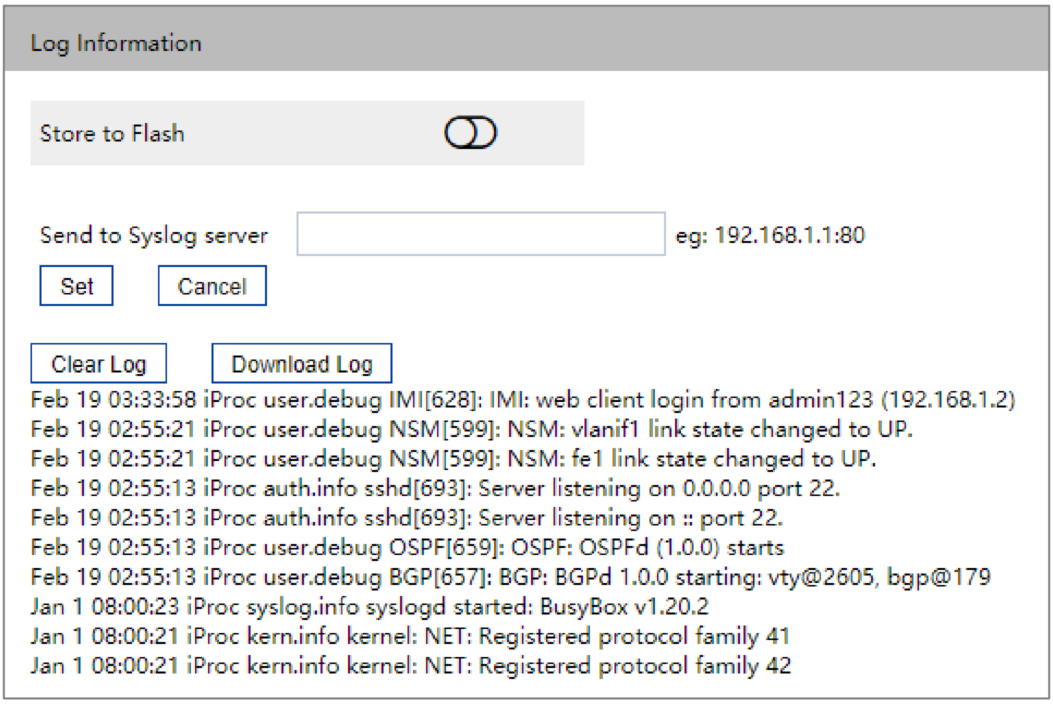
- User log: records user operations and system operation information.
- Security log: records information including account management, protocol, anti-attack and status.
- Diagnostic log: records information that assists in problem identification.

Operation Path

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

Interface Description

Log information interface as follow:



```
Feb 19 03:33:58 iProc user.debug IMI[628]: IMI: web client login from admin123 (192.168.1.2)
Feb 19 02:55:21 iProc user.debug NSM[599]: NSM: vlanif1 link state changed to UP.
Feb 19 02:55:21 iProc user.debug NSM[599]: NSM: fe1 link state changed to UP.
Feb 19 02:55:13 iProc auth.info sshd[693]: Server listening on 0.0.0.0 port 22.
Feb 19 02:55:13 iProc auth.info sshd[693]: Server listening on :: port 22.
Feb 19 02:55:13 iProc user.debug OSPF[659]: OSPF: OSPFd (1.0.0) starts
Feb 19 02:55:13 iProc user.debug BGP[657]: BGP: BGPd 1.0.0 starting: vty@2605, bgp@179
Jan 1 08:00:23 iProc syslog.info syslogd started: BusyBox v1.20.2
Jan 1 08:00:21 iProc kern.info kernel: NET: Registered protocol family 41
Jan 1 08:00:21 iProc kern.info kernel: NET: Registered protocol family 42
```

Main elements configuration description of log information interface:

Interface Element	Description
Store to Flash	Save it to the Flash enable switch, and save the switch log information to the Flash chip after it is enabled.
Send to Syslog server	The IP address of remote server (such as PC) that receives syslog

Interface Element	Description
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 file “messages” locally.

The Second Part: Frequently Asked Questions

10 FAQ

10.1 Sign in Problems

1. **Why the webpage displays abnormally when browsing the configuration via WEB?**
   Before access the WEB, please eliminate IE cache buffer and cookies. Otherwise, the webpage 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 adopting BlueEyes_Ⅱ 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.

10.2 Configuration Problem

1. **Why the bandwidth can't be increased after configure 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 is 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:
   - Connected computer and switch ports keep invariant, change other network cable;
   - Connected network cable and switch port keep invariant, change other computers;
   - Connected network cable and computer keep invariant, 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.

10.3 Alarm Problem

1. **When the device alarms, except BlueEyes_II software nether alarm information display area will display alarm information, is there any other way to notify technical staffs?**
   When the device alarms, the computer buzzer for host monitoring will continue to emit alarm sounds.

10.4 Indicator Problem

1. **Power indicator isn't bright, what's the reason?**

Possible reasons include:

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

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

   Possible reasons include:

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

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

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

4. **Communication crashes after a period of time, that is, 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.

11 Maintenance and Service

Since the date of product delivery, our company provides 5-year product warranty. According to our company's product specification, during the warranty period, if the product exists any failure or functional operation fails, our company will repair or replace the product for users free of charge. However, the commitments above do not cover damage caused by improper usage, accident, natural disaster, incorrect operation or improper installation.

In order to ensure that consumers benefit from our company's managed switch products, consumers can get help and solutions in the following ways:

- Internet Service;
- Service Hotline;
- Product repair or replacement;

11.1 Internet Service

More useful information and tips are available via our company website.

Website: http://www.3onedata.com

11.2 Service Hotline

Users of our company's products could call technical support office for help. Our company has professional technical engineers to answer your questions and help you to solve the product or usage problems ASAP. Free service hotline: +86-4008804496

11.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company's technical staff, and then contact the salesmen to solve the problem.

According to the company's handling procedure, customers should negotiate with our company's technical staff and salesmen to complete the product maintenance, replacement or return.

3onedata

3onedata Co., Ltd.

Headquarter address: 3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China

Technology support: tech-support@3onedata.com

Service hotline: 4008804496

Official Website: http://www.3onedata.com