8+16+4 Industrial Managed Gigabit Ethernet Fiber Switch

User Guide

Document Version: 01

Issue Date: 09/07/2021

Preface

This Ethernet Switch User Guide introduces the following sections:

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

Note

The reference model for the screenshot in this manual is 8 Gigabit Combo ports, +16 Gigabit copper ports, +4 Gigabit SFP ports and +2 Redundant 100~240VAC power inputs or +2 Redundant 36~72VDC power inputs. In addition to the differences in the supported power supply and port type, the interface functions and operation of other models in this series are similar.

Audience

This document is prepared for the following personnel:

- Network administrators
- Technical support engineers
- Network engineer

Text Format Convention

Format	Description
" "	Words with " " represent the interface words. For example "Port number".
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	Represents clickable words with a hyperlink. These appear in a 'Light Blue' font color.

Symbols

Format	Description
⚠️ *Notice*	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.
⚠️ *Warning*	Pay attention to the notes on the mark, improper operation may cause personal injury.
📄 *Note*	Necessary supplements, descriptions, and explanations for operation.
🔑 *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 guide is only an example, and does not represent the actual port with this number on the device. In actual use, the port number shown on the device shall prevail.

Revision Record

Version No.	Date	Revision note
01	09/07/2021	Product release

CONTENTS

Part One: Operation

1 Login to the Web Interface

1.1 WEB Browsing System Requirement

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

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

1.2 Setting IP Address of PC

The switch default management as follows:

IP Settings	Default Value
IP Address	192.168.1.254
Subnet mask	255.255.255.0

While configuring the switch via Web:

- Before remote configuration, please make sure the route between computer and switch is reachable.

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

Note:

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

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

Operation Steps

Amendment steps as follows:

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

Step 2 Change the selected "5" in red frame of the picture below to "1".
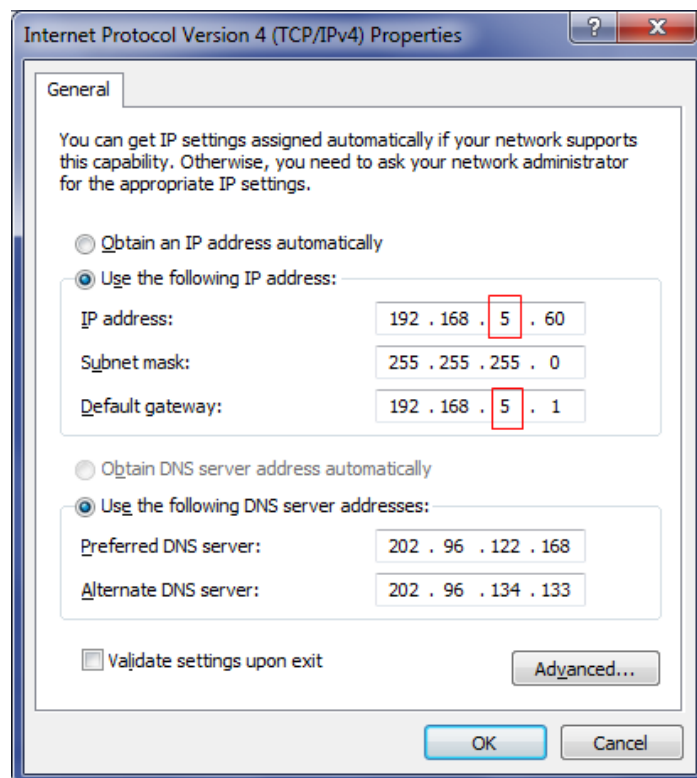
Step 3 Click "OK", IP address is modified successfully.

Step 4 End.

1.3 Log in the Web Configuration Interface

Operation Steps
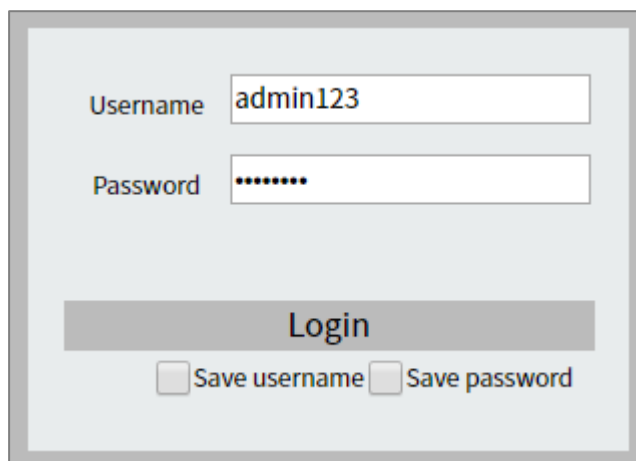
Login in the web configuration interface as follows:

Step 5 Run the computer browser.

Step 6 On the address bar of browser, enter in the IP address of the switch "http://192.168.1.254".

Step 7 Click the "Enter" key.

Step 8 Pop-up dialog box as shown below, enter the Username and Password in the login window.

Note:
- The default username and password are "admin123"; please strictly distinguish capital and small letter while entering.
- Default user account has the administrator privilege.

Step 9 Click "Login".

Step 10 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.

3

2 System Information

Function Description

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

Operation Path

Open: "System Information".

Interface Description

System information interface as follows:
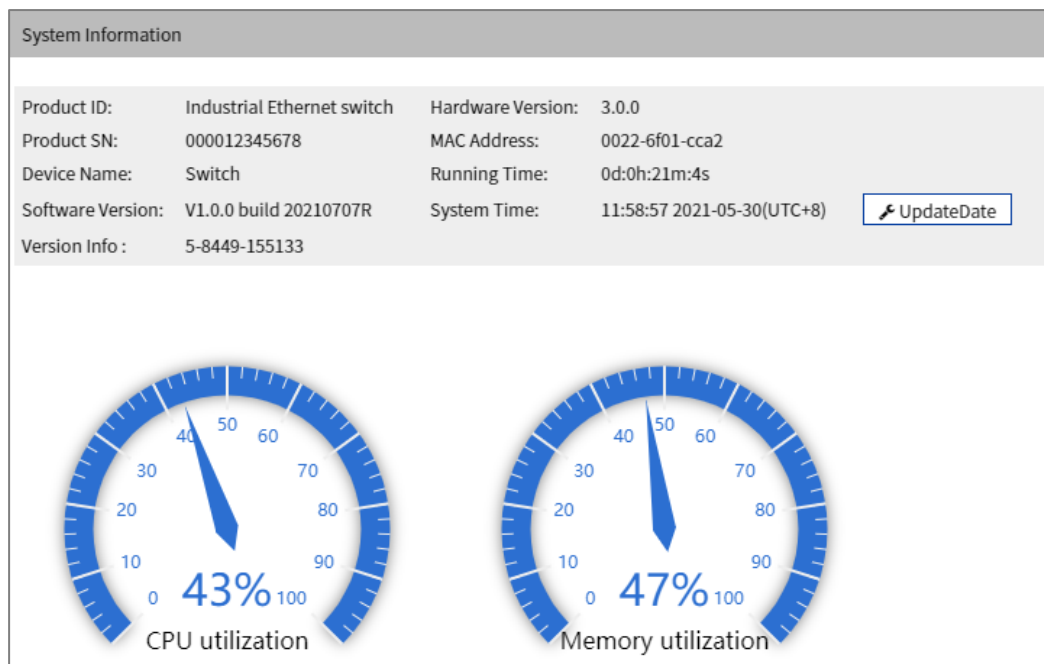
The main element configuration description of state information interface:

Interface Element	Description
Product ID	Model of the device.

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

3 System Configuration

3.1   IP Address Configuration

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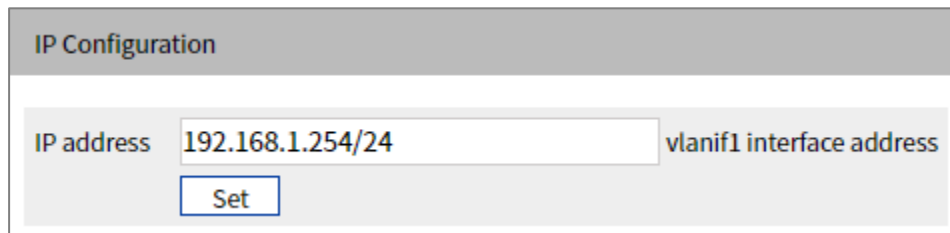
On the "IP Address Configuration" page, users can modify the vlanif1 interface address of the device. The format of IP address is: XXX.XXX.X.XXX/XX. For example, 192.168.1.254/24, 192.168.1.254 represents IP address, and 24 represents subnet mask 255.255.0.

Operation Path

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

Interface Description

IP address configuration interface is as follows:

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 Configuration" page, user can:

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

Operation Path

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

Interface Description

The User Configuration interface is as follows:

The Description of each interface Element of the User Configuration Interface are as follows:

Interface Element	Description
Username	Identification of the visitor. Note: The Username cannot be empty, and the length must be less than 16 characters.
Password	Password used by the visitor. Note: Password cannot be empty and the length must be less than 8 characters.
Protocol	Login protocols supported by user.
Privilege	User permissions are divided into 16 levels from 0 to 15, corresponding to 4 different types of permissions, and the corresponding relationship is as follows.

Interface Element	Description
	• 0: visit level, user can only check system information, device IP address and log information, and cannot modify configuration. • 1: check level, user can check device configuration information without modifying it. • 2: configuration level, user can check and configure device information, but not manage devices. • 3-15: manage level, user has all privileges of the device, including downloading, uploading, rebooting, modifying device information and other other operations.

3.3 Network Diagnosis

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

• Ping
• Traceroute
• Port Loopback
• SFP Digital Diagnosis

3.3.1 Ping

Function Description

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

Operation Path

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

Interface Description

The interface of Ping is as follows:
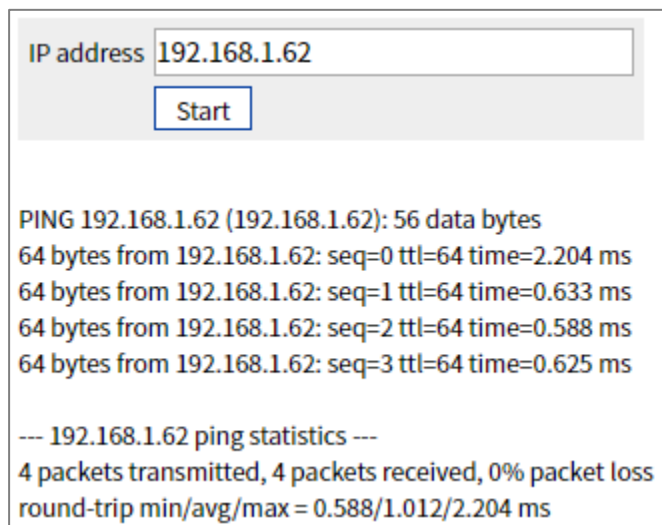
The Description of each Interface Element of the Ping Configuration interface are as follows:

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 Enter the IP address that needs to be pinged in the IP address text box;

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

Step 3 End.

3.3.2 Traceroute

Function Description

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

Operation Path

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

Interface Description

Traceroute interface as follows:

The Description of each Interface Element of the Traceroute interface are as follows:

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

Traceroute Configuration:

Step 4 Fill in the destination IP address in the "IP address" text box;

Step 5 Click the "Start" button to check the results, as the picture below.

Note:

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

Step 6 End.

3.3.3 Port Loopback

Function Description

On the "Port Loopback" page, the 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 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:

Network Diagnosis >	Ping	Traceroute	Port Loopback	SFP Digital Diagnosis

🔧 Config

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
☐	ge1	down	disable
☐	ge2	down	disable
☐	ge3	down	disable
☐	ge4	down	disable
☐	ge5	down	disable
☐	ge6	down	disable
☐	ge7	down	disable
☐	ge8	down	disable
☐	ge9	down	disable
☐	ge10	down	disable
☐	ge11	down	disable
☐	ge12	down	disable
☐	ge13	down	disable
☐	ge14	down	disable
☐	ge15	down	disable
☐	ge16	down	disable
☐	ge17	down	disable
☐	ge18	down	disable
☐	ge19	down	disable
☐	ge20	down	disable
☐	ge21	down	disable
☐	ge22	down	disable
☐	ge23	up	disable
☐	ge24	down	disable
☐	ge25	down	disable
☐	ge26	down	disable
☐	ge27	down	disable
☐	ge28	down	disable

The Description of each Interface Element of the Port Loopback Interface is as follows:

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

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
	• PHY: Data is looped back after transmitted to the physical layer of Ethernet.

3.3.4 SFP Digital Diagnosis

Function Description

On the "SFP Digital Diagnostics" page, user can monitor SFP parameter in real time. This function has greatly facilitated the troubleshooting process of optical fiber link and the cost of on-site debugging.

Operation Path

Open in order: "Main Menu > System Configuration > Network Diagnosis > SFP Digital Diagnosis".

Interface Description

The SFP digital diagnosis interface is as follows:

| Network Diagnosis > | Ping | Traceroute | Port Loopback | SFP Digital Diagnosis |

Port xe1 (SFP/SFP+) ▬

Parameter	Mark	Actual Value	Unit	Reference Range
Temperature		44.00	°C	-40.00 - 95.00
Voltage		3.32	V	3.00 - 3.60
Bias Current		12.73	mA	0.00 - 55.00
Rx Power(dBM)		0.00	mW	-27.96 - 0.00
Tx Power(dBM)		-6.39	mW	-10.00 - -2.01

Port xe2(SFP/SFP+) ▬

Parameter	Mark	Actual Value	Unit	Reference Range
Temperature		44.00	°C	0.00 - 100.00
Voltage		3.37	V	2.90 - 3.60
Bias Current		39.89	mA	3.00 - 85.00
Rx Power(dBM)	↓	-40.00	mW	-18.00 - 2.00
Tx Power(dBM)		-3.06	mW	-6.99 - 1.00

The Description of each Interface Element of the SFP Digital Diagnosis interface are as follows:

Interface Element	Description
Port	The corresponding port name of the device's Ethernet port.
Parameters	Parameter information of optical module: ● Temperature: This device's SFP temperature. Its unit is °C. The operating temperature of this SFP module should be within the normal operating temperature range. ● Voltage: The voltage of this device's SFP. Its unit is V. Overvoltage could lead to the breakdown of CMOS device; under voltage would disable the normal operation of lasers. ● Bias current: laser bias current. ● Receiving power: Optical input power, referring to the lowest optical power of receiving in certain rate and bit error rate.

Interface Element	Description
	• Transmission power: Optical output power, referring to the output power of optical source in the sending end of optical module.
Mark	Identification of whether the parameter value is normal: • ↓: The parameter value is less than the normal reference range; • ↑: The parameter value is greater than the normal reference range; • No ID: the parameter value is normal.
Actual value	Current values of parameters of optical module
Unit	Units of each parameter of optical module: • Temperature: ℃. • Voltage: V. • Bias current: mA. • Receiving power: dBm. • Transmission power: dBm.
Reference Range	Reference range of optical module parameters

3.4   Login Mode Configuration

Function Description

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

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

Operation Path

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

Interface Description

Login mode configuration interface as follows:
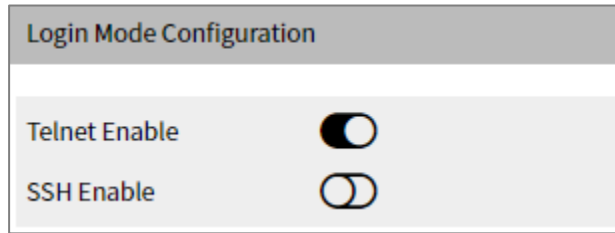
The Description of each Interface Element of the Login Mode Configuration interface are as follows:

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

4 Port Configuration

4.1 Port Settings

Function Description

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

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

Operation Path

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

Interface Description

Port setting interface as follows:

Port Setting

Config

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

Port type selection: ⦿ ge

	Port	State	Medium	Rate	Duplex mode	Flow control	Max frame	Enable	Description
☐	ge1	down	auto ▾	auto	auto	disable	1518	enable	
☐	ge2	down	auto ▾	auto	auto	disable	1518	enable	
☐	ge3	down	auto ▾	auto	auto	disable	1518	enable	
☐	ge4	down	auto ▾	auto	auto	disable	1518	enable	
☐	ge5	down	auto ▾	auto	auto	disable	1518	enable	
☐	ge6	down	auto ▾	auto	auto	disable	1518	enable	
☐	ge7	down	auto ▾	auto	auto	disable	1518	enable	
☐	ge8	down	auto ▾	auto	auto	disable	1518	enable	
☐	ge9	down	copper	auto	auto	disable	1518	enable	
☐	ge10	down	copper	auto	auto	disable	1518	enable	
☐	ge11	down	copper	auto	auto	disable	1518	enable	
☐	ge12	down	copper	auto	auto	disable	1518	enable	
☐	ge13	down	copper	auto	auto	disable	1518	enable	
☐	ge14	down	copper	auto	auto	disable	1518	enable	
☐	ge15	down	copper	auto	auto	disable	1518	enable	
☐	ge16	down	copper	auto	auto	disable	1518	enable	
☐	ge17	down	copper	auto	auto	disable	1518	enable	
☐	ge18	down	copper	auto	auto	disable	1518	enable	
☐	ge19	down	copper	auto	auto	disable	1518	enable	
☐	ge20	down	copper	auto	auto	disable	1518	enable	
☐	ge21	down	copper	auto	auto	disable	1518	enable	
☐	ge22	down	copper	auto	auto	disable	1518	enable	
☐	ge23	up	copper	100m(auto)	full(auto)	disable	1518	enable	
☐	ge24	down	copper	auto	auto	disable	1518	enable	
☐	ge25	down	fiber	auto	auto	disable	1518	enable	
☐	ge26	down	fiber	auto	auto	disable	1518	enable	
☐	ge27	down	fiber	auto	auto	disable	1518	enable	
☐	ge28	down	fiber	auto	auto	disable	1518	enable	

The Descriptions of each Interface Element of the Port Settings interface are as follows:

Interface Element	Description (check the checkbox of the port and click "config" to configure it.)
Port type selection	Select the port type, and check the ports of the same type in batches: ● 100M port (Fe); ● Gigabit port (ge); ● 10Gigabit port (xe) ; ● Static aggregation port (sa); ● Dynamic Aggregation Port (po) .

18

Interface Element	Description (check the checkbox of the port and click "config" to configure it.)
	Note: The port type shall be determined by the port supported by the device, and the aggregation port shall be reflected after configuration.
Port	The corresponding port name of the device's Ethernet port.
State	Ethernet port connection status, display status as follows: ● down: represent the port is disconnected; ● up: represent the port is connected.
Medium	The connection types of Ethernet ports, the status are shown as follows: ● copper: copper port medium. ● fiber: fiber port medium. Note: When the device has a Combo port, the medium of Combo port is "auto", "copper" or "fiber".
Rate	The default is self-adaption mode, and the display status is as follows: ● auto: self-adaption; ● 10m: 10M; ● 100m: 100M; ● 1g: Gigabit. ● 10g: 10 Gigabit. Note: The selected maximum rate is different for different bandwidth ports.
Duplex Mode	The default is self-adaption mode, and the display status is as follows: ● auto: self-adaption; ● half: half-duplex; ● full: full duplex.
Flow Control	Port flow control status, the display status is as follows: ● disable ● tx: enable the port to send data flow control; ● rx: enable flow control of port data receiving;

Interface Element	Description (check the checkbox of the port and click "config" to configure it.)
	• 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 the port "disable" is selected, the port will not be used.
Description	Port information description, supporting 24 valid characters.

4.2 Storm Suppression

Function Description

On the "Storm Control" page, user can set the maximum broadcast, multicast, or unknown unicast packet flow that the port allows. When the sum of each port broadcast, unknown multicast or unknown unicast flow exceeds the maximum value set by the user, the system will discard the packets beyond that flow limit, so that the proportion of overall broadcast, unknown multicast or unknown unicast flow can be reduced to a 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:

The Description of each Interface Element of the Storm Suppression interface are as follows:

Interface Element	Description (check the checkbox of the port and click "config" to configure it.)
Port type selection	Select the port type, and check the ports of the same type in batches: • 100M port (Fe);

Interface Element	Description (check the checkbox of the port and click "config" to configure it.)
	• Gigabit port (ge); • 10Gigabit port (xe) ; • Static aggregation port (sa); • Dynamic Aggregation Port (po) . Note: The port type shall be determined by the port supported by the device, and the aggregation port shall be reflected after configuration.
Port	The corresponding port name of the devices's Ethernet port.
Broadcast (bps)	The port control for broadcast packet transmission speed, input value range： • 100M interface: 10-100,000Kbps or 1-100Mbps. • Gigabit interface: 100-1000000Kbps or 1-1000Mbps or 1-1Gbps. • 10Gigabit interface: 100-10,000,000Kbps or 1-10,000Mbps or 1-10Gbps. Note: Broadcast packet, namely, the data frame with the destination address of FF-FF-FF-FF-FF-FF.
Multicast (bps)	The port control for unknown multicast data packet transmission speed, input value range： • 100M interface: 10-100,000Kbps or 1-100Mbps. • Gigabit interface: 100-1000000Kbps or 1-1000Mbps or 1-1Gbps. • 10Gigabit interface: 100-10,000,000Kbps or 1-10,000Mbps or 1-10Gbps. Note: Multicast packet, namely, the destination address is XX-XX-XX-XX-XX-XX data frame, the second X is odd number, such as: 1, 3, 5, 7, 9, B, D, F, other X represents arbitrary number.
Unicast (bps)	The port control for unknown unicast data packet transmission speed, input value range： • 100M interface: 10-100,000Kbps or 1-100Mbps. • Gigabit interface: 100-1000000Kbps or 1-1000Mbps or 1-1Gbps.

Interface Element	Description (check the checkbox of the port and click "config" to configure it.)
	• 10Gigabit interface: 100-10,000,000Kbps or 1-10,000Mbps or 1-10Gbps. Note: Unknown unicast packet, namely, the MAC address of the data frame doesn't exist in the MAC address table of the device, which needs to be forwarded to all ports.

Note

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

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

4.3 Port Rate Limit

Function Description

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

Operation Path

Open in order: "Port Configuration > Port Rate 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: ● ge

	Port	Bandwidth(kbps)	Operation
☐	ge1	-	Clear
☐	ge2	-	Clear
☐	ge3	-	Clear
☐	ge4	-	Clear
☐	ge5	-	Clear
☐	ge6	-	Clear
☐	ge7	-	Clear
☐	ge8	-	Clear
☐	ge9	-	Clear
☐	ge10	-	Clear
☐	ge11	-	Clear
☐	ge12	-	Clear
☐	ge13	-	Clear
☐	ge14	-	Clear
☐	ge15	-	Clear
☐	ge16	-	Clear
☐	ge17	-	Clear
☐	ge18	-	Clear
☐	ge19	-	Clear
☐	ge20	-	Clear
☐	ge21	-	Clear
☐	ge22	-	Clear
☐	ge23	-	Clear
☐	ge24	-	Clear
☐	ge25	-	Clear
☐	ge26	-	Clear
☐	ge27	-	Clear
☐	ge28	-	Clear

The Description of each Interface Element of the Port Rate Limit interface are as follows:

Interface Element	Description (check the checkbox of the port and click "config" to configure it.)
Port type selection	Select the port type, and check the ports of the same type in batches: • 100M port (Fe). • Gigabit port (ge). • 10Gigabit port (xe).

24

Interface Element	Description (check the checkbox of the port and click "config" to configure it.)
	• Static aggregation port (sa). • Dynamic Aggregation Port (po). Note: The port type shall be determined by the port supported by the device, and the aggregation port shall be reflected after configuration.
Port	The corresponding port name of the device Ethernet port.
Bandwidth (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. • 10 Gigabit interface: 64-1000000Kbps or 1-1000Mbps or 1Gbps. • 10 Gigabit interface: 64-10000000Kbps or 1-10000Mbps or 1-10Gbps. Note: Supports unit of K/M/G when configuring the rate. In the WEB display, the unit conversion will be conducted and the simplest values will be displayed according to the input value and the units.
Operation	Click "delete" to delete port rate limit configuration. Port rate restores to no limit by default.

Note

- Flow control should be enabled when using port speed limit, otherwise the speed between devices would not be stable.
- When using the port rate limit, packet loss should not occur unless the flow control is disabled. The representation of packet loss is the fluctuating transmission speed.
- Port speed limit has high requirements on network cable quality, otherwise lots of conflict packets and broken packets would appear.

4.4 Port Mirroring

Function Description

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

Operation Path

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

Interface Description

Port mirror interface as follows:

Port Mirroring			
+ Add **🗑 Delete**			
☐	Session ID	Source port	Destination port Operation

The Description of each Interface Element of the Port Mirroring interface are as follows:

Interface Element	Description (check the checkbox of the port and click "Add" button to configure it.
Session ID	Device mirror ID number, value is 1-4. Note: The device supports maximum 4-way mirror sessions.
Source Port	Monitored ports, from which the device will collect input or output messages. There can be one or more mirror ports.
Destination Port	Monitoring port, copying and analyzing messages from source port.
Operation	Click "Edit" under "Operation" to configure the direction type of source port data to be monitored in this session. Click "Delete" under "operation" to delete the corresponding port mirroring entry directly. Data direction options are as follows: • transmit: egress data, the message sent by the source port will be mirrored to the destination port.

Interface Element	Description (check the checkbox of the port and click "Add" button to configure it.
	• receive: ingress data, the packet received by the source port will be mirrored to the destination port • Both: all data, mirror the source port receiving and sending packets at the same time. Note: Directions can only be superimposed and cannot be deleted.
Add	Click "Add" to increase the port mirror entries.
Delete	Check the checkbox of port mirror entries, click "Delete" button to delete all mirror group entries

Note

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

4.5 Link Aggregation

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

The Link Aggregation Control Protocol (LACP is based on the IEEE 802.3ad standard. It is a protocol for implementing dynamic link aggregation. Devices running this protocol exchange LACPDU (Link Aggregation Control Protocol Data Unit, Link Aggregation Control Protocol Data Unit) to exchange link aggregation related information.

Based on the enabling or disabling of LACP protocol, the link aggregation can be divided into two modes, static aggregation and dynamic aggregation. LACP priority is used to distinguish the priority of different interfaces being selected as active interfaces. The smaller the priority value, the higher the priority.

Function Description

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

Operation Path

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

Interface Description

Link Aggregation interface as below:

The Description of each Interface Element of the Link Aggregation Interface are as follows:

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:

Interface Element	Description
	• 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.
Operation	Click "Edit" under "Operation" to set the working mode for the specified dynamic aggregation group. Click "Delete" under "operation" to delete the corresponding link aggregation group directly.
Add	Click "Add" to add link aggregation entry.
Delete	Check the checkbox of link aggregation entry and click "Delete" button to delete link aggregation entry.

Interface Description: Add

The Link Aggregation-Add interface as follows:

The Description of each Interface Element of the Link Aggregation-Add interface are as follows:

Interface Element	Description
Group ID	The ID number of static aggregation link, support maximum 12 groups, each group can configure 8 ports to join aggregation.
Type	Aggregation group mode: • Static: Static aggregation. • Dynamic: Dynamic aggregation.
Port List	The drop-down box of port member: • Active: the active interface, that is, the interface for forwarding data. • Passive: inactive interface, that is, interface that does not forward data.

Interface Element	Description
	Note: When the type is Static, this function cannot be edited.
Load mode	There are 6 options for the configuration of trunk group load balance mode: • Dst-ip: Load balance mode based on destination IP; • Dst-mac: Load balance mode based on destination MAC. • Src-dst-ip: Load balance mode based on source and destination IP. • Src-dst-mac: Load balance mode based on source and destination MAC. • Src-ip: Load balance mode based on source IP. • Src-mac: Load balance mode based on source MAC.
Port	Port member in the aggregation group.

4.6 Port Statistics

On the Port Statistics page, you can implement the following functions:
- Check the number of messages sent and received by each port and the number of message bytes; number of discarded and erroneous messages.
- Check the classification statistics of the total number of messages sent and received by the designated port and the number of bytes of messages.

4.6.1 Port Statistics-Overview

Function Description

In the "Port Statistics - Overview" page, the following functions can be achieved:
- Check the number of messages sent and received by each port and the number of message bytes; Number of discarded and erroneous messages.
- Click the "Clear" button to clear the overview information of the screen.

Operation Path

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

Interface Description

Port Statistics-Overview interface as follows:

Port Statistics >	Port Statistics - Overview	Port Statistics - Port		
Port ge1 ▼			Clear	
	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		
1519-2047 bytes	0	0		
2048-4095 bytes	0	0		
4096-9216 bytes	0	0		

4.6.2 Port Statistics-Port

Function Description

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

- Check the classification statistics of the total number of messages sent and received by the designated port and the number of bytes of messages.
- Click the "Clear" button to clear the port information from the screen.

Operation Path

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

Interface Description

Port Statistics-Port interface as follows:

Port Statistics >	Port Statistics - Overview	Port Statistics - Port	

Port ge1 ▼   Clear

	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
1519-2047 bytes	0	0
2048-4095 bytes	0	0
4096-9216 bytes	0	0

4.7   Port Isolation

Function Description

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

Operation Path

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

Interface Description

Isolate-port configuration interface as follows:

The Description of each Interface Element of the Port Isolation Configuration interface are as follows:

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

4.8 Link Flapping Protection

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

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

4.8.1 Global Configuration

Function Description

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

Operation Path

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

Interface Description

Global configuration interface is as follows:

Link Shock Protection >	Global configuration	Port Configuration

In the default state, the link oscillates five times within 20s, an alarm log is generated, and the port is set to shutdown state

Detection interval	20	Range: 10-100(s), default: 20(s)
Turbulence hreshold	5	Range: 3-100, default: 5
Automatic recovery	☐	
Recovery time	3600	Range: 30-86400 (s), default: 3600(s)
	Set	

The Description of each Interface Element of the Global Configuration Interface are as follows:

Interface Element	Description
Detection interval	The value range of link detection interval is 10-100s, and the default value is 20s.
Turbulence threshold	The threshold value of oscillation times for link detection, when the oscillation times exceed the threshold value within a certain detection time, an alarm log will be generated, and the port will be set to shutdown state. The range is from 3 to 100, default value is 5.
Automatic recovery	Automatic recovery radio box. After being checked, the port will automatically return to normal within the specified time.
Recovery time	The value range of the time when the port automatically returns to normal is 30-86400s, and the default value is 3600s.

4.8.2 Port Configuration

Function Description

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

Operation Path

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

Interface Description

Check port configuration interface as below:

Link Shock Protection > | Global configuration | Port Configuration

In the default state, the link oscillates five times within 20s, an alarm log is generated, and the port is set to shutdown state

[Enable]   [Cancel]

Port type selection: ⦿ ge   ⦾ all

☐	Port	Enabled state	Port status
☐	ge1	-	down
☐	ge2	-	down
☐	ge3	-	down
☐	ge4	-	down
☐	ge5	-	down
☐	ge6	-	down
☐	ge7	-	down
☐	ge8	-	down
☐	ge9	-	down
☐	ge10	-	down
☐	ge11	-	down
☐	ge12	-	down
☐	ge13	-	down
☐	ge14	-	down
☐	ge15	-	down
☐	ge16	-	down
☐	ge17	-	down
☐	ge18	-	down
☐	ge19	-	down
☐	ge20	-	down
☐	ge21	-	down
☐	ge22	-	down
☐	ge23	-	up
☐	ge24	-	down
☐	ge25	-	down
☐	ge26	-	down
☐	ge27	-	down
☐	ge28	-	down

The Description of each Interface Element of the Port Configuration interface are as follows:

Interface Element	Description
Enable	Select the port and click Enable to enable the link flapping protection function of the port.
Cancel	Select the port and click Disable to disable the link flapping protection function of the port.

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

5 Layer 2 Configuration

5.1 MAC Configuration

MAC (Media Access Control) address is the hardware identity of network device; the switch forwards the message according to MAC address. MAC address has uniqueness, which has guaranteed the correct retransmission of message. Each switch is maintaining a MAC address table. In the table, MAC address is corresponding to the switch port. When the switch receives data frames, it decides whether to filter them or forward them to the corresponding port according to the MAC address table. MAC address is the foundation and premise that switch achieves fast forwarding.

5.1.1 MAC Settings

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

Function Description

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

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

Operation Path

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

39

Interface Description

MAC Settings interface as follows:

The Description of each Interface Element of the MAC Settings interface are as follows:

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

Interface Element	Description
	• Dynamic: dynamic MAC address. • Static: static MAC address.

5.1.2 Static MAC

Function Description

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

Operation Path

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

Interface Description

Static MAC interface as follows:

The Description of each Interface Element of the Static MAC interface are as follows:

Interface Element	Description
MAC	Fill in the unicast MAC address that needs to bind the interface, such as 0001.0001.0001.
Forwarding Type	The forward type of MAC, discard or transmit, it displays as follows: • Discard. • Forward.
Port	The Binding Port Number.
VLAN ID	The VLAN ID number to which the data sent by this MAC address belongs, for example, 1-4094. Note:

Interface Element	Description
	Input VLAN ID is the existing ID.
Operation	Click "Delete" under "Operation" to delete the corresponding MAC entry directly.
Add	Click "Add" button to add static MAC entry.
Delete	Check the radio box of MAC entries and click "Delete" button to delete MAC entries.

Note

- The function acts as a security mechanism. Carefully confirm the setting, otherwise, part of the devices won't be able to communicate.
- Do not adopt multicast address as the entering address.
- Do not enter reserved MAC address, such as the local MAC address.

5.1.3 Static Multicast MAC

Function Description

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

Operation Path

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

Interface Description

Static Multicast MAC interface as follows:

The Description of each Interface Element of the Static Multicast MAC Interface are as follows:

Interface Element	Description
MAC	Fill in the multicast MAC address that needs to bind the interface, such as 0100.0001.0001.
Forwarding Type	The forward type of MAC, discard or transmit, it displays as follows: • Discard. • Forward.
Port	The Binding Port Number.
VLAN ID	The VLAN ID number to which the data sent by this MAC address belongs, for example, 1-4094. Note: Input VLAN ID is the existing ID.
Operation	Click "Delete" under "operation" to delete the corresponding MAC entry directly.
Add	Click "Add" button to add static MAC entry.
Delete	Check the radio box of MAC entries and click "delete" button to delete MAC entries

5.2   VLAN Configuration

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

VLAN advantages mainly include:
- Port isolation. Ports from different VLANs, even from the same switch, cannot intercommunicate. Such a physical switch can be used as multiple logical switches.
- Network security. Different VLANs cannot directly communicate with each other, which has eradicated the insecurity of broadcast information.
- Flexible management. You would not need to change ports or connection when changing the network user, only the firmware configuration.

43

That is, ports within the same VLAN can intercommunicate; otherwise, ports cannot communicate with each other. A VLAN is identified by VLAN ID. Ports with the same VLAN ID, belong to the same VLAN.

5.2.1 VLAN Configuration

Function Description

On the "VLAN Configuration " page, user can create VLANs and edit VLAN descriptions.

Operation Path

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

Interface Description

VLAN Configuration interface as follows:

The Description of each Interface Element of the VLAN Configuration interface are as follows:

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.

Interface Element	Description
	• 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 "Range Delete" button to delete range-specified VLAN entry.

5.2.2 Access Configuration

Function Description

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

Operation Path

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

Interface Description

Access configuration interface as follows:

The Description of each Interface Element of the Access Configuration interface are as follows:

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 Untagged messages, it adds a Tag mark on them according to the PVID. When the port transmits the data message with

Interface Element	Description
	the same Tag mark as PVID, it would erase the Tag mark and then transmit the message. The PVID of all ports default to 1.
Pvid Configuration	Check the entries of PVID value that need to be reset, click "Pvid Config" button to reset pvid value.
Mode setting	There are three port link types that the switch supports: • Access: port only belongs to 1 VLAN (which is the default VLAN), all ports of the switch are Access mode by default and all PVID are 1. • Trunk: port can belong to multiple VLANs, Trunk port can allow the messages of multiple VLANs to pass with Tag, but only allow the messages of one VLAN to transmit without tag (strip Tag) from this kind of interface. Commonly used in the connection between network devices. • Hybrid: port can belong to multiple VLANs. Hybrid port allows messages of multiple VLANs to pass with tag, and allows the messages sent from this kind of interface to configure whether the messages of some VLANs is with tag (not strip Tag) or not (strip Tag). It could be used in the connection between network devices, as well as user devices. Note: If the port mode is set to Trunk or Hybrid, the port display will be updated to the tab corresponding to "Trunk Configuration" or "Hybrid Configuration".

5.2.3 Trunk Configuration

Function Description

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

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

Operation Path

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

Interface Description

Trunk configuration interface as follows:

The Description of each Interface Element of the Trunk Configuration Interface are as follows:

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

5.2.4 Hybrid Configuration

Function Description

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

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

Operation Path

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

Interface Description

Hybrid configuration interface as follows:

The Description of each Interface Element of the Hybrid Configuration interface are as follows:

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

Process for Port Receiving Message

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

Process for Sending Message

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

Instance: typical VLAN configuration

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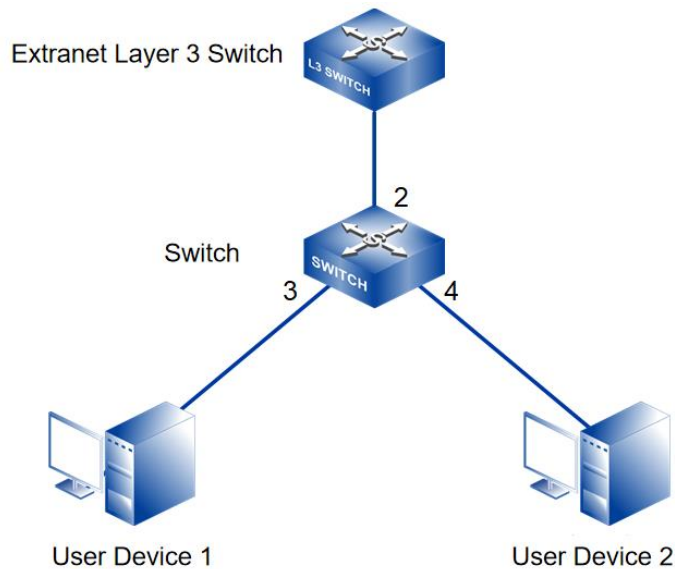
Instance analysis

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

- Port3

Port3 is upper interface, set Ports to Access type.

Configure the PVID value ofPort3 to 3.

- Port 4

Port4 is downward interface, set Ports to Access type.

The PVID value of Port4 is set to 4.

- Port2

Port2 is upper interface, set Port2 to Trunk type. Add Port2 into VLAN3 and VLAN4.

Port2 can communicate with Port3 and Port4.

Operation Steps

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

Step 2 Set VLAN value: VLAN3 and VLAN4.

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

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

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

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

2 Check port ge3, click "configure", enter "Pvid" as "3", and click "set".

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

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

52

Step 4 Set the tagvlan value of port 2.

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

2　　Check the item and click "Apply".

3　　Enter "1" in "Pvid" and "3-4" in "Tagvlan".

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

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

Step 5 End.

5.3 Spanning-Tree Configuration

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

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

Spanning-tree protocol has two main functions:

- The 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.
- The second function is achieving the convergence protection purpose via spanning-tree protocol when Ethernet topology changes.

Compared to STP and RSTP, MSTP can converge the network more quickly when the network structure changes; MSTP is compatible with STP and RSTP and is better than STP and RSTP. It can quickly converge but also send different VLANs along each path to provide better load sharing system for redundant links.

5.3.1 Bridge Configuration

Function Description

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

Operation Path

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

Interface Description

Bridge configuration interface as follows:

The Description of each Interface Element of the Bridge Configuration interface are as follows:

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, the higher the priority level is.
Max hop count	The maximum hop in MST region, defaults to 20, the value range is 1-40. Note: The maximum hop in MST region has limited the size of MST region. The maximum hop configured on a domain root will be used as the maximum hop in MST region.
Forwarding delay	Port state transition delay, defaults to 15S, the value range is 4-30.

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

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

Operation Path

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

Interface Description

Instance configuration interface as follows:

The main element configuration description of instance configuration interface:

Interface Element	Description
Instance	Instance ID number of Multiple Spanning-tree. The value range is 1-16.
Priority	Device priority level, value range is 0-61440, default to 32769, step is 4096. During adding, choose a priority based on 0-15 times the value on the 4096. Note: The priority of a device participates in spanning tree calculation. Its size determines whether the device can be selected as the root bridge of a spanning tree.
Vlan 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 the 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 shown below:

	Spanning-tree Configuration >	Bridge Configuration	Instance Configuration	Port Configuration	Instance Port Configuration

🔧 Config

	Port	Enable	Bpduguard	Edge port	Connection Type
☐	ge1	enable	default	disable	auto
☐	ge2	enable	default	disable	auto
☐	ge3	enable	default	disable	auto
☐	ge4	enable	default	disable	auto
☐	ge5	enable	default	disable	auto
☐	ge6	enable	default	disable	auto
☐	ge7	enable	default	disable	auto
☐	ge8	enable	default	disable	auto
☐	ge9	enable	default	disable	auto
☐	ge10	enable	default	disable	auto
☐	ge11	enable	default	disable	auto
☐	ge12	enable	default	disable	auto
☐	ge13	enable	default	disable	auto
☐	ge14	enable	default	disable	auto
☐	ge15	enable	default	disable	auto
☐	ge16	enable	default	disable	auto
☐	ge17	enable	default	disable	auto
☐	ge18	enable	default	disable	auto
☐	ge19	enable	default	disable	auto
☐	ge20	enable	default	disable	auto
☐	ge21	enable	default	disable	auto
☐	ge22	enable	default	disable	auto
☐	ge23	enable	default	disable	auto
☐	ge24	enable	default	disable	auto
☐	ge25	enable	default	disable	auto
☐	ge26	enable	default	disable	auto
☐	ge27	enable	default	disable	auto
☐	ge28	enable	default	disable	auto

The Description of each Interface Element of the Port Configuration interface are as follows:

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
Port	The corresponding port name of the device Ethernet port.
Enable	Status of participating in spanning tree enable switch.
BPDU Guard	BPDU (Bridge Protocol Data Unit) protection function status: • Enable • Disable • Default
Edge port	Configure port type: • Enable • Disable
Connection Type	Port link type: • Auto: Automatic system detection • Point-to-point: point-to-point link; • Shared: Non point-to-point link.

5.3.4 Instance Port Configuration

Function Description

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

Operation Path

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

Interface Description

Instance port configuration interface as follows:

The Description of each Interface Element of the Instance Port Configuration interface are as follows:

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.
Instance	Instance ID number port belongs to.

Interface Element	Description (check the checkbox of the port, click "config" to configure it.)
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
State	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 a ring configuration is called an ERPS Ring. It could be divided into main ring and subring. Each device in the 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:

The Description of each Interface Element of the Timer Configuration interface are as follows:

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 a clean command on the owner node. After the timer expires, the owner node will block the RPL port and unblock the temporary blocking port.

Interface Element	Description
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 the "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 network Configuration" page, user could configure the ring network.

An Ethernet network topology connected in a ring is called an ERPS Ring. It could be divided into the main ring and subring. Each device in the 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 network Configuration interface as follows:

The Description of each Interface Element of the Ring network Configuration interface are as follows:

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

5.4.3 Instance Configuration

Function Description

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

Operation Path

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

Interface Description

Instance configuration interface as follows:

The Description of each Interface Element of the Instance Configuration interface are as follows:

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

Interface Element	Description
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.
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:

65

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

5.5 Ring Configuration

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

The core of Ring technology 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 follows:

The Description of each Interface Element of the Ring Configuration interface are as follows:

Interface Element	Description
Enable	Enable switch, slide to the right to enable the Ring ring network function.
Ring group	Support ring group 1-12, it can create 12 ring networks at the same time.

Interface Element	Description
Mark	When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID. Value range is 1-255. Note: The ring network identification must remain the same in one ring network.
Ring Port 1	The network port 1 on the switch device used to form a ring. Note: When the ring network type is "Couple", port 1 is the "Coupled Port". Coupling port is the port that connects different network identities.
Port1 Status	The current state of port 2. ● block. ● forward.
Ring Port 2	The network port 2 on the switch used to form a ring. Note: ● When the ring network type is "Couple", port 2 is the "console port". Console port is the port in the chain where two rings intersect. ● "Port 1" and "Port 2" cannot be set to the same port, and the port number it sets must be the same as it actually connects without sequential order.
Port 2 Status	The current state of the port 2. ● block. ● forward.
Ring Type	According to the requirement in the scene, user can choose different ring type. ● Single: single ring, using a continuous ring to connect all devices 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.

Interface Element	Description
	• 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.
HelloTime	Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends information packet to adjacent device for confirming the connection is normal or not. Value range is 0-300.
Master-slave	Single loop network supports no-master station structure and one-master multi-slave structure. • When all the single-loop devices are slave stations, the single-loop structure is no-master station. • When a single ring device is a master and multiple slave station, one device can be designated as the master device and the other devices as the slave device. One end of the main device of the ring network is the backup link. When the ring network fails, the backup link is enabled from the master station to ensure the normal operation of the network.
Heartbeat	Heartbeat detection mechanism. When this configuration is enabled, the network association will periodically send heartbeat messages to detect whether the corresponding devices are in live state, thus enhancing the reliability of the network. Swipe the "⬤◯" button to the right to activate the heartbeat function.
Add	Click "Add" button to add ring network configuration.
Delete	Check the radio box of ring network configuration entry and click "delete" button to delete ring network configuration.

Single Ring Configuration

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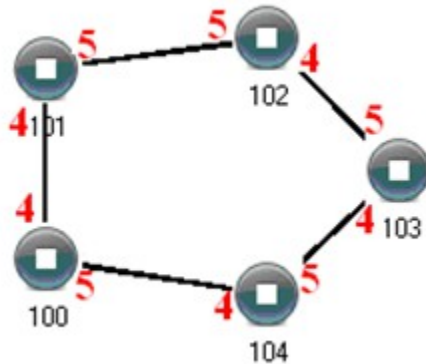
Double Ring Configuration

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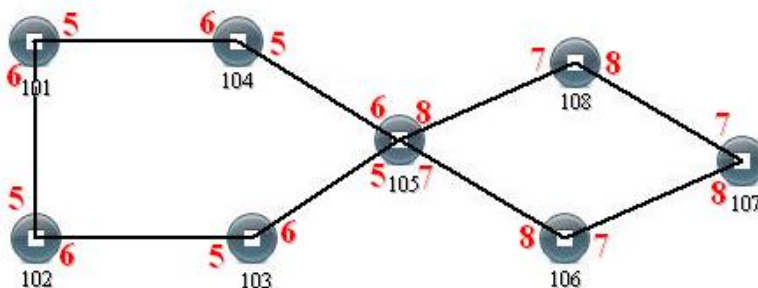
Configuration Method:

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

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

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

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

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

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

Coupling Ring Configuration

Coupling ring basic framework as the picture below:

Operation method:
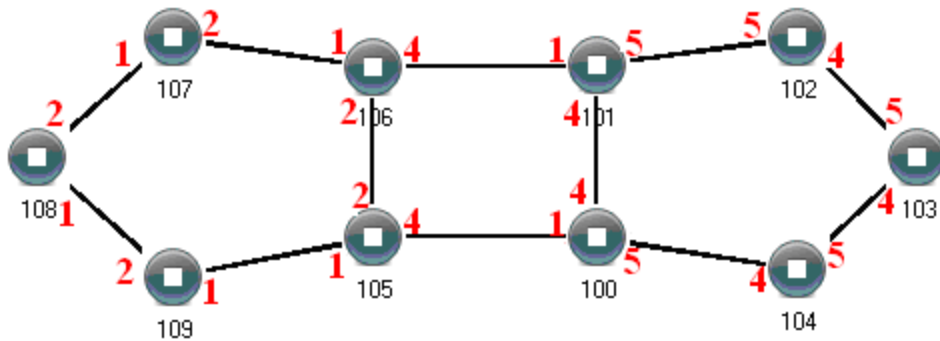
Step 1 Enable ring network group 1 and 2: (Hello_time could be disabled, but the time could not be set to make Hello packet sent too fast.　Otherwise, it would seriously affect the CPU processing speed.　seriously);

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

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

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

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

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

Chain Configuration

Chain basic framework as the picture below:
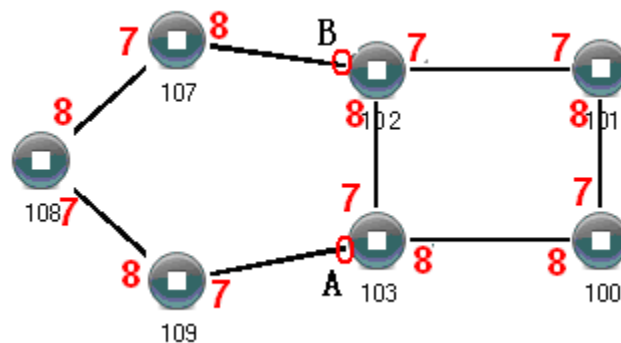
Operation method:

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

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

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

📄*Note*

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

5.6   IGMP-Snooping Configuration

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

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

Various ways IGMP Snooping processes different messages:

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

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

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

– If the forwarding table entry corresponding to the group already exists and the dynamic member port is included in the outgoing port list, will reset its aging timer.

– If the forwarding table entry corresponding to the group already exists, but the port is not included in the out port list, the port is added to the out port list as a dynamic member port and it's aging timer is started.

– If there is no forwarding table entry corresponding to the group, create a forwarding table entry, add the port as a dynamic member port to the out port list, start its aging timer, and then send the report message of the group to all router ports.

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

5.6.1 Global Configuration

Function Description

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

Operation Path

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

Interface Description

Global configuration interface is as follows:

The Description of each Interface Element of the Global Configuration interface are as follows:

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

5.6.2 Interface Configuration

Function Description

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

Operation Path

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

Interface Description

Interface configuration interface as follows:

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

+Add   🗑 Delete

☐	VLAN ID	IGMP Snooping	Fast leave	Querier	Querier election disable	Startup query count	Startup query interval	Query interval	Query max response time	Last member query interval	Last member query count	Operation

Total item 0   Total page 0   Current page < 1 >

The Description of each Interface Element of the Interface Configuration interface are as follows:

Interface Element	Description
VLAN ID	VLAN ID number, value range is 1-4094.
IGMP Snooping	IGMP Snooping status, enabling IGMP snooping on global or VLAN interface. Note: Only when IGMP snooping is enabled on the global and VLAN interfaces can the configuration of the other IGMP snooping properties on that interface take effect.
Fast Leave	The enabled state of the multicast group Fast Leave. After fast leaving is enabled, when the switch receives the IGMP leaving group message sent by the host from a port, it directly deletes the port from the outgoing port list of the corresponding forwarding table entry. • Enable: enable the multicast fast leave function. • Disable: disable the multicast fast leave function.
Querier	Enable status of IGMP inquirer. IGMP querier can send general query messages to all hosts and other multicast routers in this network segment.
Querier election disable	Enable non-election status of IGMP-Querier. IGMPv2 uses an independent inquirer election mechanism. When there are multiple multicast routers on the shared network segment, the router with the smallest IP address becomes

Interface Element	Description
	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.
Query max response time	Maximum response time of IGMP universal group query.
Last member query interval	Time interval when the inquirer sends IGMP specific group inquiry message.
Last member query count	Number of IGMP specific group inquiry messages sent by the inquirer.
Operation	Click the "Edit" button to edit relevant parameters; Click the "Delete" button to delete the entry.

5.6.3 Routing Port Configuration

Function Description

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

Operation Path

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

Interface Description

Routing port configuration interface is as below:

The Description of each Interface Element of the Routing Port interface are as follows:

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

5.6.4 Routing Port Information

Function Description

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

Operation Path

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

Interface Description

Routing port information interface is as follows:

The Description of each Interface Element of the Routing Port interface are as follows:

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

5.7   Port Loopback Detection

Loop Detection technology is to periodically send a special detection message from the interface, and then detect whether the message returns to the device, and then judge whether there is a loop between the interface, the device's down-link network or the device and the device's dual interfaces:

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

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

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

5.7.1   Global Configuration

Function Description

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

Note:

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

Operation Path

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

Interface Description

Global configuration interface is as follows:

The Description of each Interface Element of the Global Configuration interface are as follows:

Interface Element	Description
Enable	Global enable switch of port loop detection.
Port	The corresponding port number of this device's Ethernet port.

Interface Element	Description
Protected	The state of the port protected by a loop.
State	The connection status of this port, values are: ● Down: the port is physically disconnected ● Up: the port is connected ● Shutdown: the port is closed ● No Shutdown: the port is not closed
Port recovery time	Recovery time after detection of loop action. If the disabled port does not receive the loop monitoring message after the "port recovery time", it is judged that the loop has been eliminated and the port is reactivated.
Protected VLAN	The VLAN ID of the loop protection.
Loop VLAN	The VLAN ID of the currently generated loop.
Stable packet sending interval	After the ports are started and stable, that is, after three "packet-sending intervals", a loop monitoring message is sent at a "stable packet-sending interval" to determine whether there is a loop at each port and whether the loop on the port has been eliminated.
Packet sending interval	When the port is just started, the default time interval for sending loop monitoring messages is 1s, a total of 3 times, and then the packet issuing interval returns to the normal packet issuing interval.

5.7.2   Port Configuration

Function Description

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

Operation Path

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

Interface Description

Check port configuration interface as below:

81

The Description of each Interface Element of the Port Configuration interface are as follows:

Interface Element	Description
Port	The corresponding port number of this device's Ethernet port.
Protected	The state of the port protected by a loop.
State	The connection status of this port, values are: ● Down: the port is physically disconnected ● Up: the port is connected ● Shutdown: the port is closed ● No Shutdown: the port is not closed
Port recovery time	The resume time after the action of detecting a loop. The value range: 300-600, its unit is seconds.

Interface Element	Description
Protected VLAN	The VLAN ID of loop protection. It is None by default. The value range: 1-4094, the number of VLAN ID is ≤16. Note: This parameter must be configured, otherwise there would be errors in sending the data.
Loop VLAN	The VLAN ID of the currently generated loop.
Stable packet sending interval	After the ports are started and stable, that is, after three "packet-sending intervals", a loop monitoring message is sent at a "stable packet-sending interval" to determine whether there is a loop at each port and whether the loop on the port has been eliminated. Stable packet issuing interval time, value range is 10-300, and the unit is in seconds.
Packet sending interval	When the port is just started, the default time interval for sending loop monitoring messages is 1s, a total of 3 times, and then the packet issuing interval returns to the normal packet issuing interval.

6 Layer 3 Configuration

6.1 Interface Configuration

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

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

Category A, B, C addresses are unicast addresses; category D address is multicast address; category E address is reserved address for the future special purpose. Currently, most of the usable IP addresses belong to category A, B, C address ranges.

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

The IPv6 address is expressed as a series of 16-bit hexadecimal number separated by colons. Each IPv6 address is divided into eight groups, 16 bits in each group is expressed by four hexadecimal numbers, two groups are separated by a 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.

The IPv6 address is composed of two parts: address prefix and interface identification. Thereinto, the address prefix is the network number field part in the IPv4 address. The interface identification is the host number part in the 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, which represents how many bits in the leftmost of IPv6 address is the address prefix.

6.1.1 Layer 3 Interface

The Layer 3 interface IP address could be used as the device management address or gateway. The Layer 3 interface IP address needs to be configured at the 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 > Layer-3 Interface".

Interface Description

Layer-3 Interface configuration as follows:

Interface Configuration >	Layer-3 Interface	Loopback Interface Configuration

	Interface	State	IPv4 address	Enable	Operation
☐	vlanif1	up	192.168.1.254/24	enable	Edit Delete

Total item 1   Total page 1   Current page   ‹ 1 ›

The Description of each Interface Element of the layer-3 Interface are as follows:

Interface Element	Description
Interface	Layer 3 interface names, such as, vlanif1, value range: vlanif1-vlanif4094.
State	Interface state information, options: • Up. • Down.
IPv4 address	IPv4 address and subnet mask, such as 192.168.1.1/24.
Enable	Interface switch options as follows: • enable. • disable.
Operation	Click "Edit" button to set interface and IPv4 address, enable/disable interface switch. Click "Delete" under "operation" to delete the corresponding interface configuration directly.

Interface Element	Description
Add	Click "edit" button to add the configuration of layer 3 interface.
Delete	Check the radio box of layer 3 interface entry, and click the "delete" button to delete the layer 3 interface entry.

6.1.2 Loopback Interface

The Loopback interface is a virtual interface, and most of the platforms use it to simulate a 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 interfaces of the device is down. It would only be invalid when the router no longer has effect.

Function Description

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

Operation Path

Open in order: "L3 forward Configuration > Interface Configuaration > Loopback Interface Configuration".

Interface Description

Loopback Interface Configuration interface as follows:

Interface Configuration >	Layer-3 Interface	Loopback Interface Configuration

+ Add	🗑 Delete			
☐	Interface	State	IPv4 address	Operation

The Description of each Interface Element of the Loopback Interface Configuration interface are as follows:

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

6.2   ARP Configuration

ARP (Address Resolution Protocol) is the protocol that resolves the IP address into an 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 an 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 follows:

The Description of each Interface Element of the Arp Information interface are as follows:

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 "To Static" to convert dynamic address to static address.

6.2.2 Static ARP

Function Description

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

Operation Path

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

Interface Description

Static ARP Configuration interface as follows:

The Description of each Interface Element of the Static ARP Configuration interface are as follows:

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 Parameter Configuration" page, user can conduct ARP Aging time configuration.

Operation Path

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

Interface Description

ARP Parameter Configuration interface as follows:

The Description of each Interface Element of the ARP Parameter Configuration interface are as follows:

Interface Element	Description
Interface	Interface Name.
Aging Time	Aging 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).

7 Unicast Routing Table

7.1   IPv4 Configuration

7.1.1   IPv4 Routing Table

Function Description

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

Operation Path

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

Interface Description

The IPv4 Routing Table interface as follows:

The Description of each Interface Element of the IPV4 Routing Table interface are as follows:

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

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

7.1.2 IPv4 Static Route

Static route refers to the route information that the user or network administrator manually configures. When the network topology structure or link status changes, the 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, the network administrator can clearly know the network topology structure, which is convenient for setting the correct route information.

Function Description

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

Operation Path

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

Interface Description

The IPv4 Static Route interface as follows:

The Description of each Interface Element of the IPV4 Static Route interface are as follows:

Interface Element	Description
Destination IP address	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 interfacet	Interface Name.
Operation	Click the "Delete" button to delete the the current entry.

8 Multicast Routing

8.1 Multicast Routing

8.1.1 Multicast Routing

Function Description

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

Operation Path

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

Interface Description

The multicast routing interface is shown as follows:
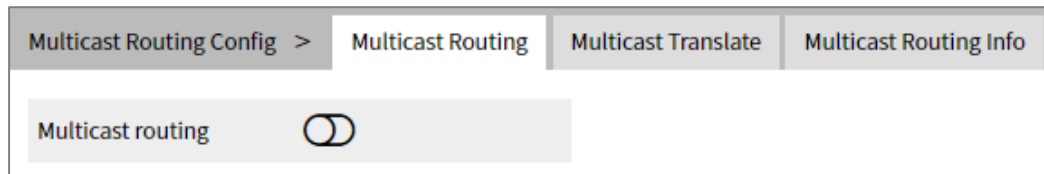
Main elements of the multicast routing interface:

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

8.1.2 Multicast Translate

Function Description

On the "Multicast Translate" page, you can configure multicast translation between two VLANs.

Operation Path

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

Interface Description

Multicast Translate interface is as follows:

The Description of each Interface Element of the Multicast Translate interface are as follows:

Interface Element	Description
ID	VLAN ID number of Multicast Translate, value range is 1-64.
ACL	ACL number or name, used for multicast translation control.
Old VID	The old VLAN ID of multicast packet, with a value range of 1-4094.
New VID	The new VLAN ID after multicast packet transparent transmission, with a value range of 1-4094.
Operation	You can edit or delete the current entry.

8.1.3 Multicast Routing Information

Function Description

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

Operation Path

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

Interface Description

The multicast routing information interface is as follows:

Multicast Routing Config >	Multicast Routing	Multicast Translate	Multicast Routing Info				
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed						
Source address	Group address	Uptime	Expires	Owner	Flgs	Incoming interface	Outgoing interface (TTL)
Total item 0 Total page 0 Current page < 1 >						

The Description of each Interface Element of the Multicast Routing Information interface are as follows:

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

Interface Element	Description
Outgoing interface (TTL)	Multicast data egress interface. The interface that forwards multicast data out.

8.2 IGMP Configuration

8.2.1 Interface Configuration

Function Description

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

Operation Path

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

Interface Description

Interface configuration interface as follows:

The Description of each Interface Element of the Interface Configuration interface are as follows:

Interface Element	Description
Interface	Layer 3 interface, such as vlanif1.
IGMP	IGMP status: • enable. • disable.
Version	IGMP version, options are: • 1: IGMPv1, it defines the basic querying and reporting process of group members.

Interface Element	Description
	• 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 an IGMP message, the current switch will send it to IGMP protocol module for processing by default regardless of whether its IP header contains Router-Alert option.
Unlimited same subnet	Limit the multicast source and interface to the same subnet, otherwise the port cannot receive multicast messages.
Robustness coefficient	Specify the robustness of the IGMP query, ranging from 2 to 7. This coefficient is used to specify the default value of the number of times an IGMP query message is sent by the IGMP query at startup, and the number of times an IGMP query message is sent by the IGMP query after the IGMP query receives the message leaving the group.
Other querier present timer	Timer time of non-inquirer. • Before the timer expires, if the inquiry message from the inquirer is received, reset the timer. • Otherwise, the original inquirer is considered invalid, and a new inquirer election process is initiated.
Fast leave ACL	By default, when the interface works in IGMP v2 or v3, after receiving IGMP leave message, it will send a specific group query message to determine whether to age multicast

Interface Element	Description
	member entries. After configuring the fast leave ACL, if the group address specified by the leave message is within the group address range specified by the ACL, the multicast member table entry can be aged immediately.
Deny multicast ACL	List of restricted multicast groups.
Multicast group Max	The maximum number of multicast supported.
Operation: edit	Modify IGMP entries.
Operation: delete	Delete the current IGMP entry.

8.2.2 SSM-Map Configuration

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

The mechanism of IGMP SSM Mapping is: by statically configuring SSM address Mapping rules on the router, information in IGMPv1 and IGMPv2 report packets are converted into the 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, the user can add or delete the IGMP configuration of the Ethernet ports.

Operation Path

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

Interface Description

The SSM-Mapping Configuration interface is as follows:

The Description of each Interface Element of the SSM-Mapping Configuration interface are as follows:

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

8.2.3 Group Members

Function Description

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

Operation Path

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

Interface Description

The multicast group information interface is as follows:

The Description of each Interface Element of the Group Members interface are as follows:

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

9 Advanced Configuration

9.1 DHCP - Server Configuration

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

9.1.1 DHCP Switch

Function Description

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

Operation Path

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

Interface Description

DHCP Switch interface as follows:

The Description of each Interface Element of the DHCP Switch interface are as follows:

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

9.1.2　DHCP Pool Configuration

After the user defines the DHCP range and exclusion range, surplus addresses constitute an address pool; addresses in the address pool can be dynamically distributed to hosts in the network. The 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 the IP address and other relative parameters for the client from the address pool.

DHCP server adopts a tree structure: Tree root is the address pool of natural network segments. Branch is the subnet address pool of the network segment. Leaf node is the manually binding client's address. The order of address pool at the same level is decided by the configuration order. This kind of tree structure realizes the inheritance of configuration, that is, subnet configuration inherits the configuration of natural network segments, 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 are as follows:

When the parent-child relationship is established, sub address pool will inherit the existing configuration of parent address pool.

1. 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 does not include the configuration, it will inherit the configuration of parent address pool.

   – If the child address pool has included the configuration, it will not inherit the configuration of the parent address pool.

Function Description

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

Operation Path

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

Interface Description

DHCP Address Pool Configuration interface as follows:

The Description of each Interface Element of the Address Pool Configuration interface are as follows:

Interface Element	Description
Address pool name	The name of the address pool, up to 32 characters.
Assigned segment	Address pool distributes the IP address network segment of the client, for example: 192.168.0.1/24.
Lease time	IP address utilization valid time of client, format: day, hour, minute, range is 0-30 day, 0-24h and 0-60m, which are separated by space. Note: When the time of IP address obtained by the 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.

Interface Element	Description
Delete	Check address pool entry, click "delete" button to delete address pool information.

9.1.3 Server Configuration

Function Description

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

Operation Path

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

Interface Description

Server configuration interface as follows:

The Description of each Interface Element of the Server Configuration interface are as follows:

Interface Element	Description
Add	Click the "Add" button to configure the 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.

Interface Element	Description
	• WINS server: parse the NetBIOS host name using the Windows Microsoft operating system to an IP address. • Log server.
IP	Server address pool, which supports up to three different server IP addresses.
Operation	Click "Delete" under "operation" to delete the corresponding server address pool.

9.1.4 MAC Bind

Function Description

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

Operation Path

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

Interface Description

The MAC Bind configuration interface is as follows:

The Description of each Interface Element of the MAC Bind interface are as follows:

Interface Element	Description
Add	Click the "Add" button to add a static binding between the IP address assigned by the address pool and the MAC address of the device.
Delete	After checking the entry, click the "Delete" button to delete the binding of the corresponding IP address and MAC address.

Interface Element	Description
Address pool name	Corresponding list name of DHCP address pool.
IP address	IP addresses distributed by DHCP address pool, IP addresses obtained by this MAC address.
MAC address	The MAC address information of this device.
Operation	Click "Delete" under "operation" to delete this MAC binding.

9.1.5 Port Bind

Function Description

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

Operation Path

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

Interface Description

Port Bind configuration interface as follows:

The Description of each Interface Element of the Port Bind interface are as follows:

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

9.1.6 Client List

Function Description

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

Operation Path

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

Interface Description

Client list interface as follows:

The Description of each Interface Element of the Client List interface are as follows:

Interface Element	Description
IP address	IP address of DHCP client-side device.
MAC address;	MAC address of DHCP client device.
Start time	Valid start time of DHCP client.
End time	Valid end time of DHCP client.
Remaining time	Valid remaining time of DHCP client.

9.2 DHCP-Snooping Configuration

The function of DHCP Snooping:

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

1   Ensure that clients get IP addresses from legitimate servers.

If there is a pseudo-DHCP server set up privately in the network, it may cause the DHCP client to get the wrong IP address and network configuration parameters and cannot 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 trusted 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 the DHCP server and other DHCP Snooping devices need to be set as trusted ports. Other ports should be set as untrusted ports, to ensure that the 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 the DHCP client.

DHCP Snooping records DHCP Snooping entries by listening to DHCP-REQUEST messages and DHCP-ACK messages received by trusted ports, including MAC

110

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 messages are legal or not, so as to prevent ARP attacks 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, messages sent by the DHCP client to the DHCP server, adds Option 82 to the message and sends it to the DHCP server.

Administrators can obtain location information of the DHCP client from Option 82, so as to locate the DHCP client and realize control over security and billing of the 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-options, 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), Sub-Option 2 (Remote ID, Remote ID sub-option) and Sub-Option 3 (Subscriber ID, Subscriber ID sub-option).

9.2.1   Global Configuration

Function Description

On the "Global Configuration" page, User can enable/disable DHCP Snooping.

Operation Path

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

Interface Description

Global configuration interface is as follows:

The Description of each Interface Element of the Global configuration interface are as follows:

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 the 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 in seconds and the default is 30s.

9.2.2 VLAN Enable Configuration

Function Description

On the "VLAN Enable Configuration" page, user can specify 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:

The Description of each Interface Element of the VLAN Enable Configuration interface are as follows:

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

9.2.3 Binding Configuration

Function Description

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

Operation Path

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

Interface Description

The Binding Configuration interface is as follows:

The Description of each Interface Element of the Binding Configuration interface are as follows:

Interface Element	Description
VLAN ID	Binding VLAN indentification information, for example: 1-4096.
Port	The corresponding port name of the device's 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.
Operating: edit	Modify the port binding information.
Operating: delete	Delete the port binding configuration of the current row.

9.2.4 Port Configuration

Function Description

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

Operation Path

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

Interface Description

Check the Port Configuration interface as follows:

The Description of each Interface Element of the Port Configuration interface are as follows:

Interface Element	Description
Port	The corresponding port name of the device's Ethernet port.
Trust Enable	Port Trust Enable, and the trust port forwards the received DHCP message normally.
Message Rate	Message transmission speed of port, the input range is 10-1000 (s), and the default value is 1000s.
Option 82 Check	When Option 82 Check is turned on, the location information of the DHCP client can be obtained from Option 82.
Option 82 Strategy	Option 82 Dealing Strategy, options are as follows:

Interface Element	Description
	• Drop: Discard messages. • Keep: Adopt different modes to fill Option 82, replace prime Option 82 in message and forward and filling modes will be described as below. • Replace: Keep Option 82 in messages unchanged and forward.
Circuit Type	Circuit ID sub-option filling type, options are as follows: • Normal: Normal mode. • String: Detailed mode.
Circuit ID	Circuit ID sub-option filling content, support ASCII and HEX mode. Note: • The input length is limited between 2 and 64. • When Hex is selected, the input content is a combination of uppercase and lowercase letters and numbers. • When ASCII is selected, the content is not limited.
Remote Type	Remote ID sub-option filling type, options as follows: • Normal: Normal mode. • Sysname: Directly adopt device system name to fill Option 82. • String: Detailed mode.
Remote ID	The filling content of the remote ID sub-option supports ASCII and HEX formats. Note: • The input length is limited between 2 and 64. • When Hex is selected, the input content is a combination of uppercase and lowercase letters and numbers. • When ASCII is selected, the content is not limited.
Subscriber Type	User option fill type, which supports ASCII format.
Subscriber ID	The filling content of Subscriber ID sub-option supports ASCII and HEX formats. Note: • The input length is limited between 2 and 64.

Interface Element	Description
	• When Hex is selected, the input content is a combination of uppercase and lowercase letters and numbers. • When ASCII is selected, the content is not limited.

9.3   DHCP-Relay Configuration

Function Description

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

Operation Path

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

Interface Description

DHCP-Relay configuration interface is as follows:

The Description of each Interface Element of the DHCP-Relay Configuration interface are as follows:

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 are as follows: • Enable: enable the Option82 function of DHCP relay.

Interface Element	Description
	• Disable: disable the Option82 function of DHCP relay. Note: When the Option82 function is enabled, the relay message sent by the relay process would carry Option82.
Option82 Policy	The processing strategy of Option82 is shown as follows: • untouched • append • discard • replace
Server IP	IP address information of proxy server.
Operation: edit	Click "edit" button to set the parameters of the switch and Option82.
Operation: delete	Check Relay interface configuration entry, click "delete" to delete Relay interface configuration.

9.4   LLDP Configuration

LLDP is a layer 2 topology discovery protocol, its basic principle is: Devices in a network, send the status information message to the adjacent device. Each port in the device stores its own information. If there are changes in the status of the 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 query the connection status of current layer 2 from the SNMP MIB bank. It should be noted that LLDP is only a remote device status information discovery protocol, which cannot complete the network device configuration, port control and other functions.

9.4.1   Current Configuration

Function Description

On the "Current Configuration" 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:

LLDP Configuration >	Current Configuration	Port Configuration	Neighbor Information

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

The Description of each Interface Element of the Current Configuration interface are as follows:

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

9.4.2 Port Configuration

Function Description

On the "Port Configuration" 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:

LLDP Configuration >	Current Configuration	Port Configuration	Neighbor Information

Config

	Local port	Port status	Port Configuration	Management IP
☐	ge1	down	txrx-enable	0.0.0.0
☐	ge2	down	txrx-enable	0.0.0.0
☐	ge3	down	txrx-enable	0.0.0.0
☐	ge4	down	txrx-enable	0.0.0.0
☐	ge5	down	txrx-enable	0.0.0.0
☐	ge6	down	txrx-enable	0.0.0.0
☐	ge7	down	txrx-enable	0.0.0.0
☐	ge8	down	txrx-enable	0.0.0.0
☐	ge9	down	txrx-enable	0.0.0.0
☐	ge10	down	txrx-enable	0.0.0.0
☐	ge11	down	txrx-enable	0.0.0.0
☐	ge12	down	txrx-enable	0.0.0.0
☐	ge13	down	txrx-enable	0.0.0.0
☐	ge14	down	txrx-enable	0.0.0.0
☐	ge15	down	txrx-enable	0.0.0.0
☐	ge16	down	txrx-enable	0.0.0.0
☐	ge17	down	txrx-enable	0.0.0.0
☐	ge18	down	txrx-enable	0.0.0.0
☐	ge19	down	txrx-enable	0.0.0.0
☐	ge20	down	txrx-enable	0.0.0.0
☐	ge21	down	txrx-enable	0.0.0.0
☐	ge22	down	txrx-enable	0.0.0.0
☐	ge23	up	txrx-enable	0.0.0.0
☐	ge24	down	txrx-enable	0.0.0.0
☐	ge25	down	txrx-enable	0.0.0.0
☐	ge26	down	txrx-enable	0.0.0.0
☐	ge27	down	txrx-enable	0.0.0.0
☐	ge28	down	txrx-enable	0.0.0.0

The Description of each Interface Element of the Port Configuration interface are as follows:

Interface Element	Description
Local port	The corresponding port name of the device's Ethernet port.
Port status	The LLDP working modes of the device's port are as follows: • tx-enable: work mode is Tx, it only transmits LLDP messages and does 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 the network management system. The management address can mark a device, which is beneficial to the drawing of network topology and network management. The management address is encapsulated in the Management Address TLV field of the LLDP message and sent to adjacent nodes. • The management address released by the port in the LLDP message defaults to the main IP address of the smallest VLAN of the specific VLAN this port is in. If the VLAN is not configured with a main IP address, it will be 0.0.0.0.

9.4.3 Neighbor Information

Function Description

On the "Neighbor Information" page, user can look over the relative information of it's neighbors.

Operation Path

Open in order: "Advanced Configuration > LLDP Configuration > Neighbor Information".

Interface Description

Neighbor Information interface as follows:

LLDP Configuration >	Current Configuration	Port Configuration	Neighbor Information
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.

9.5 ACL Configuration

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

9.5.1 Time Range Configuration

Function Description

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

Operation Path

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

Interface Description

Time Range configuration interface as follows:

The Description of each Interface Element of the Time Range Configuration interface are as follows:

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

Click "Add" button to add time entry.

In the "Add" interface, check the "Absolute time" radio box.

123

Interface Description 1: Add-absolute time

The Add-absolute time interface as follows:

The Description of each Interface Element of the Add-absolute time interface are as follows:

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

In the "Add" interface, check the "Regular time" radio box.

Interface Description 2: Add-regular time

The Add-regular time interface as follows:

The Description of each Interface Element of the Add-regular time interface are as follows:

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

9.5.2 IP ACL Configuration

Function Description

On the "IP ACL config" page, user can configure the IP ACL rules. Users can assign numbers to ACLs when creating them, and different numbers correspond to different

types of ACLs. At the same time, in order to facilitate memory and identification, users can also create named ACLs, that is, when creating ACLs, set their names.

Operation Path

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

Interface Description

IP ACL config interface is as follows:

The Description of each Interface Element of the IP ACL config interface are as follows:

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

Click "Add" button to add IP ACL rule entry.

Interface Description: Add

The Add interface is as follows:

The Description of each Interface Element of the Add interface are as follows:

Interface Element	Description
Rule type	The drop-down list of IP ACL rule type. The options are: • Name: ACL is identified by name instead of number. • Number: When creating an ACL, specify a unique number to identify the ACL.
Rule name	IP ACL rule name or number. When the rule type is name, it supports the combination of @, !, _, numbers and letters that does not exceed 16 digits. When the rule type is number, 1-199 or 1300-2699 is supported. Note: • Standard ACL(1-99, 1300-1999): Only the source IP address, fragmentation information and effective time period information of the message are used to define the rule. • Extended ACL (100-199, 2000-2699): both the source IP address of IPv4 message and the destination IP address, protocol type and effective time period can be used to define rules.

Interface Element	Description
Operation	The action drop-down list of ACL rules. The options are: • Permit • Deny
Protocol	The protocol type of extended ACL rules, support filtering messages based on protocol type, and the value range of protocol number is 0-255. You can click the drop-down list of "Protocol" to select an existing agreement name.
Source IP	The source IP address information of the packet, such as 192.168.1.1. No input indicates any IP address.
Source wildcard	Wildcard mask of source IP address, such as 0.0.0.255. The wildcard mask of IP address is a 32-bit numeric string used to indicate which bits in IP address will be checked. "0" means "check the corresponding bit", and "1" means "do not check the corresponding bit".
Destination IP	The destination IP address information of the packet, such as 192.168.1.1. No input indicates any IP address.
Destination wildcard	Wildcard mask of destination IP address, such as 0.0.0.255. The wildcard mask of IP address is a 32-bit numeric string used to indicate which bits in IP address will be checked. "0" means "check the corresponding bit", and "1" means "do not check the corresponding bit".
Time-Range Name	The name of the effective time period of the IP ACL rule.
Operation	Click "Edit" or "Delete" to modify or delete the name of Time-Range.

9.5.3 MAC ACL Configuration

Function Description

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

Operation Path

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

Interface Description

MAC ACL config interface is as follows:

The Description of each Interface Element of the MAC ACL config interface are as follows:

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

Click the "Add" button to add MAC ACL rule entries.

Interface Description: Add

The Add interface is as follows:

The Description of each Interface Element of the Add interface are as follows:

Interface Element	Description
Rule ID	MAC ACL rule number, the value range is 3000-3699.
Operation	The action drop-down list of ACL rules. The options are: • Permit • Deny
Source MAC	The source MAC address information of the packet, such as 0001.0001.0001. No input indicates any MAC address.
Destination MAC	The destination MAC address information of the packet, such as 0001.0001.0001. No input indicates any MAC address.
Ethernet type	Ethernet type of the packet, value range is 1536-65535 (0x0600-0xffff).
Time-Range Name	The name of the effective time period of the IP ACL rule.
Operation	Click "Edit" or "Delete" to modify or delete the name of Time-Range.

9.5.4 ACL GROUP Configuration

Function Description

On the "ACL GROUP config" page, you can configure ports to enable IP ACL and MAC ACL rules.

Operation Path

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

Interface Description

ACL GROUP config interface as follows:

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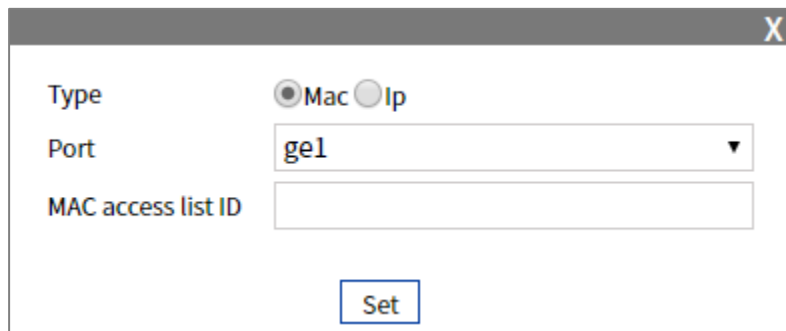
Interface Element	Description
Add	Click "Add" to add port ACL GROUP.
Delete	Check port entry and click "Delete" button to delete specified entries in batches.
Port	The Ethernet port number of the device.
MAC access list ID (direction)	The port supports MAC ACL rules.
IP ACL List ID (in)	The port supports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

Click the "Add" button to add ACL GROUP.

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

Interface Description 1: Add-MAC

The Add-MAC interface is as follows:
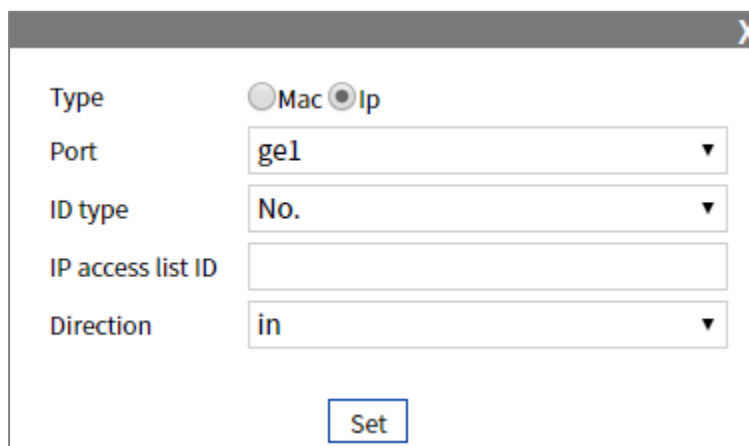
The main elements configuration description of the Add-MAC interface:

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

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

Interface Description 2: Add-IP

The Add-IP interface is as follows:

The Description of each Interface Element of the Add-IP interface are as follows:

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

9.6   SNMP Configuration

Now, the broadest network management protocol in the network is SNMP (Simple Network Management Protocol). SNMP is the industrial standard that is widely accepted and adopted. It is used for guaranteeing the management information transmission between two points in the network, and is convenient for the Network Manager to search information, modify information, to locate faults, to complete fault diagnosis, to conduct capacity plans and generate reports. SNMP adopts a polling mechanism and only provides the most basic function library, especially suitable for using in minitype, rapid and low cost environments. SNMP implementation is based on the connectionless transmission layer protocol UDP, therefore, it can achieve barrier-free connection to many other products.

9.6.1   SNMP Switch

Function Description

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

Operation Path

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

Interface Description

SNMP switch configuration interface as follows:

The Description of each Interface Element of the SNMP Switch interface are as follows:

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

9.6.2   View

Function Description

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

Operation Path

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

Interface Description

View interface is as below:

The Description of each Interface Element of the View interface are as follows:

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

9.6.3 Group

Function Description

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

Operation Path

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

Interface Description

Group interface is as follows:

The Description of each Interface Element of the Group interface are as follows:

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

9.6.4 SNMP Group

Function Description

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

Operation Path

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

Interface Description

SNMP Group interface is as follows:

SNMP Configuration >	SNMP Switch	View	Group	SNMP group	V3 user	Trap alarm	

+ Add		🗑 Delete					
☐	Name		Encryption mode	Read view	Write view	Notification view	Operation

Total item 0   Total page 0   Current page   ‹ 1   ›

The Description of each Interface Element of the SNMP Group interface are as follows:

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

9.6.5 V3 User

Function Description

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

Operation Path

Open in order: " Advanced Config > SNMP Config > V3 user".

Interface Description

V3 user interface as follows:

The Description of each Interface Element of the V3 user interface are as follows:

Interface Element	Description
Username	SNMP V3 user name definition, can only contain numbers, letters, or @_! , no longer than 32 characters.
Group Name	Group name, ranging from 1 to 32 bytes. Note: Group name must be created in the SNMP Group, and only created groups can create SNMP V3 users.
Safe Mode	Whether to authenticate and encrypt the message, values:

Interface Element	Description
	• auth: indicates that the message is authenticated but not encrypted. • noauth: indicates that the message is neither authenticated nor encrypted. • priv: indicates that the message is authenticated and encrypted.
Auth Mode	Authentication mode type, acceptable value: • Md5: Information abstract algorithm 5. • Sha: Secure hash algorithm.
Encryption mode	V3 user data encryption algorithm, options as follows: • Des: Adopt data encryption algorithm. • Aes: Adopt advanced encryption standard.
Operation	You can check this item and click the "Delete" button to delete it.

V3 User: "Add" Interface Description

The Description of each Interface Element of the Add interface are as follows:

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

Interface Element	Description
Encrypted info	V3 user data encryption algorithm, options are as follows: ● Des: Adopt data encryption algorithm. ● Aes: Adopt advanced encryption standard.
Encrypted Password	Encrypted password, character string, length greater than or equal to 8 bytes.

9.6.6 Trap Alarm

Function Description

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

Operation Path

Open in order: "Advanced Config > SNMP Configuration > Trap alarm".

Interface Description

Trap alarm interface is as follows:

The Description of each Interface Element of the Trap alarm interface are as follows:

Interface Element	Description
Address	IP address of SNMP management device, used for receiving alarm information, such as PC.

Interface Element	Description
Version	SNMP management device version, options as below: • V1. • V2c. Note: V3 is not supported temporarily.
Team name	Community name or SNMPV3 username.
Operation	You can check this item and click the "Delete" button to delete it.

9.7　NTP Configuration

NTP protocol refers to Network Time Protocol. Its function 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.
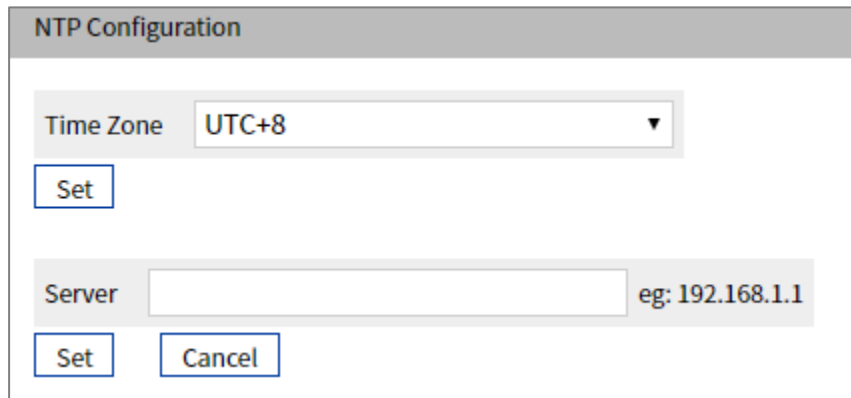
Function Description

On the "NTP Configuration" 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 is as follows:

The Description of each Interface Element of the NTP Configuration interface are as follows:

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

10 System Maintenance

10.1 Configure File Management

10.1.1 Global Configuration

Function Description

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

Operation Path

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

Interface Description

Current Configuration interface is as follows:

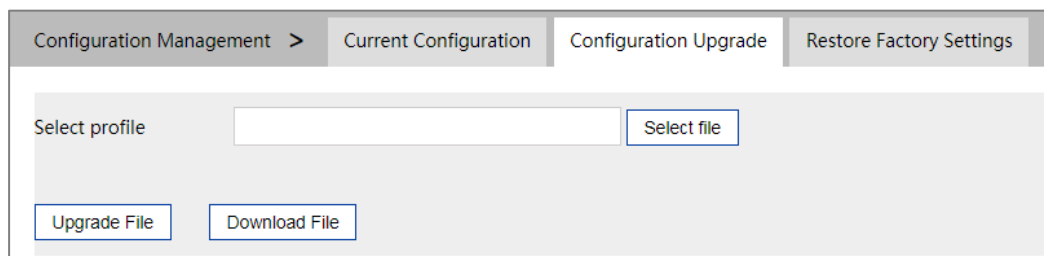# 10.1.2 Configuration File Update

Function Description

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

Operation Path

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

Interface Description

Configuration Upgrade interface is as follows:

Configuration Management >	Current Configuration	Configuration Upgrade	Restore Factory Settings

Select profile   [   ]   Select file

[Upgrade File]   [Download File]

The Description of each Interface Element of the Configuration Upgrade interface are as follows:

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.

10.1.3 Restore Factory Settings

Function Description

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

Operation Path

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

Interface Description

Restore Factory Settings interface is as follows:

The Description of each Interface Element of the Restore Factory Settings interface are as follows:

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

10.2 Alarm Configuration

10.2.1   Port Alarm

Function Description

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

Operation Path

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

Interface Description

Port interface as below:

The Description of each Interface Element of the Port interface are as follows:

Interface Element	Description
Port	The corresponding port name of the device's 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 the port alarm and click "Enable" to enable this function. Note: After the port alarm is enabled, and when the port has an abnormal status, such as a connection break, the device will output a signal to hint the abnormal operation of the device.
Disable	Check the port that needs to disable port alarm and click "Disable" to disable this function.

10.2.2   Power Alarm

Function Description

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

Operation Path

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

Interface Description

Power interface is as follows:

The Description of each Interface Element of the Power interface are as follows:

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	Port alarm function status, options as follows: • Enable. • Disable.
Enable	Check the port that needs to enable power alarm and click "Enable" to enable this function.
Disable	Check the port that needs to disable power alarm and click "Disable" to disable this function.

10.3 Upgrade

Function Description

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

Operation Path

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

Interface Description

The Software Upgrade interface is as follows:

Software Upgrade

Select file   [   ]   Select file

Upgrade

The Description of each Interface Element of the Software Upgrade interface are as follows:

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

10.4 Log Information

10.4.1 Log Information

Function Description

On the "Log Information" page, user can check the log information of the device. Log information mainly records user operation, system failure, system safety and other information, including user log, security log and diagnostic log.

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

Operation Path

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

Interface Description

Log Information interface is as follows:

The Description of each Interface Element of the Log Information interface are as follows:

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

10.4.2 Syslog Server

Function Description

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

Operation Path

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

Interface Description

The Syslog server interface is as follows:

Log Information >	Log Information	Syslog server

Syslog server		eg: 192.168.1.1:80

Set

The Description of each Interface Element of the Syslog server interface are as follows:

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

The Second Part:
Frequently Asked Questions

11 FAQ

11.1 Sign In Problems

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

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

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

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

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

   Both configurations are the same, without conflict.

11.2 Configuration Problems

1. **Why can't the bandwidth be increased after configuring the Port 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 do I resolve the problem where switch ports are impassable?**

   When some ports on the switch are impassable, it may be the network cable, the network adapter or the switch port faults. Identify the faults via the following tests:

   – Stay connected to the computer. The switch ports shall remain unchanged and replace the network cables.

   – Keep connected network cable and switch port unchanged, change other computers.

   – Keep connected network cable and computer unchanged, change other switch port;

   – If the switch port faults are confirmed, please contact supplier for support.

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

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

11.3 Indicator Problems

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

   Possible reasons include:

   – Not connected to the power socket. Ensure you are connected to the power

socket.

– Power supply or indicator faults.   Change the power supply or test the device's input power.

– Power supply voltage can't meet the device requirements. Configure the power supply voltage according to the device's manual.

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

Possible reasons include:

– The network cable portion of the Ethernet copper port is disconnected or there is a bad contact. Reconnect the network cable again.

– Ethernet terminal device or network card works abnormally. Troubelshoot to eliminate the terminal device's fault.

– Not connected to the power socket. Confirm you are connected to the power socket.

– Interface rate doesn't match the pattern. Confirm whether the device's 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 powered on or the network configuration changes, the device and switch configuration in the network will need some time. Continue troubleshooting after the device and switch configuration are complete. If the Ethernet data is impassable, power off the system, and power on again.

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

Reasons may include:

– Surrounding environment affects the product. The product grounding requires shielding from the interference source.

– Site wiring is not normal. Inspect the optical fiber and network cable. The 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.