3onedata

IES6200-PN-16T4GS-2P48

Managed Industrial Ethernet Switch

User Manual

Document Version: 01

Issue Date: 07/06/2022

Industrial Ethernet Communication Solution Expert **3onedata Co., Ltd.**

Trademark statement

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

Note

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

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

3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen, 518108 China
Technology support:	tech-support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86 0755-2670-3485
Website:	http://www.3onedata.com

Preface

Industrial Ethernet Switch User Manual has introduced this series of switches:

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

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Text Format Convention

Format	Description
" "	Words with “” represent the interface words. Such as: “Port No.”.
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. The font color is as follows: ‘Light Blue’.

Symbols

Format	Description
Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.

Format	Description
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
 Note	Make a necessary supplementary instruction for operation description.
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Revision Record

Version No.	Date	Revision note
01	07/06/2022	First release

Contents

Part One: Operation

1 Login to the Web Interface

1.1 System Requirements for WEB Browsing

Using the industrial Ethernet switch, the system should meet the following conditions.

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

1.2 Configure IP Address of the Device

The device has no IP address by default, so you can search and configure the IP address of the device through PROFINET configuration software such as STEP 7 and TIA Portal. Or use the command line to configure the IP address of the device through the CONSOLE port. If the IP address of the device is configured to 192.168.1.254, the command line operation is as follows:

```
User: admin
```

```
Password: admin
Switch> enable
Switch# configure terminal
Switch(config)# ip address 192.168.1.254/24
```

When logging into the CLI interface of the device, the default username and password are “admin”; please strictly distinguish capital and small letter while entering.

1.3 Setting IP Address of PC

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.

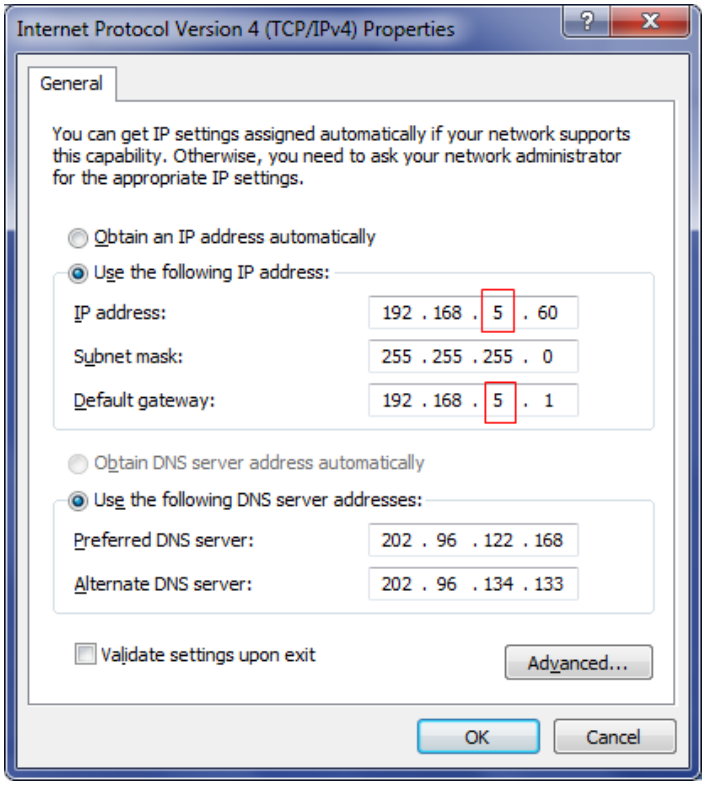
Eg: Assume that the IP address of the device is 192.168.1.47, the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address of the PC to "1".

Operation Steps

Amendment steps as follow:

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

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



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

Step 4 End.

1.4 Log in the Web Configuration Interface

Operation Steps

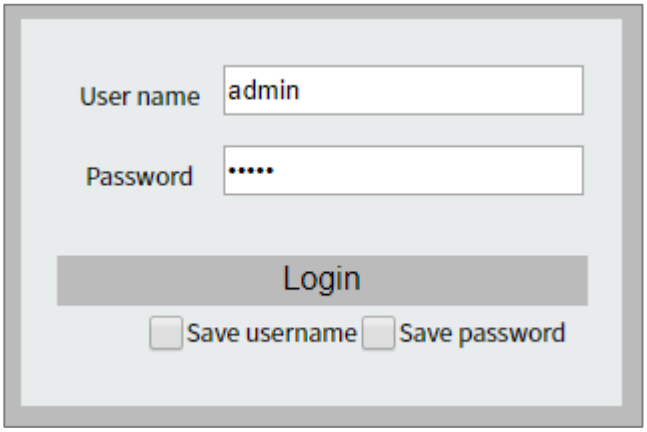
Login in the web configuration interface as follow:

Step 1 Run the computer browser.

Step 2 On the address bar of browser, enter in the IP address of the switch.

Step 3 Click the “Enter” key.

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



Note:

- The default user name and password are “admin”, please strictly distinguish capital and small letter while entering.
- The default user password is with administrator privileges.

Step 5 Click “OK”

Step 6 End.

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

Note:

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

2 System Information

Function Description

On the System Information page, you can view connection information of device interface, network load, dropped frames, error frames and log reports.

Operation Path

Open in order: "Main Menu > System Information"

Interface Description

System information interface as follows:

The main element configuration description of state information interface:

Interface Element	Description
Port Information	**Port Information area box**
Overview	In the “Overview” tab, the status information of each port of the device is displayed, such as port work status, port speed, half/duplex mode and peer IP address.
Netload	In the "Network Load" tab, the network bandwidth load of each port of the device is displayed.
Discards	In the “Drop Frames” tab, the number of frames dropped by each port of the device is displayed.
Errors	In the "Error Frames" tab, the number of error frames in each port of the device is displayed.
Message	**Report Area Frame**
Message	Number of logs, click the report icon to view the log information content.
Delete messages	Delete button is used to delete the contents of log information.
Delete counter	Delete button is used to clear the number of logs.

Interface Element	Description
Current time	Current system time information. Users can specify the time zone and server in “NTP Configuration”.
Running time	Running time of the current device.
System voltage value	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.
CPU usage	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.

Note

Port information icon is as follows:

- No fault: the port communication is normal and has no fault;
- Alarm: the port has a fault, but it doesn't cause the abnormal communication. The alarm information can be processed locally.
- Fault: the port has a fault, and the port can't communicate normally, so the fault information should be dealt with in time;
- No connection/no communication: the port is not connected, and the device/network fails to communicate.

3 System Configuration

3.1 Version Information

Function Description

On the “Version Information” page, you can preview the following configuration information and link related configuration pages:

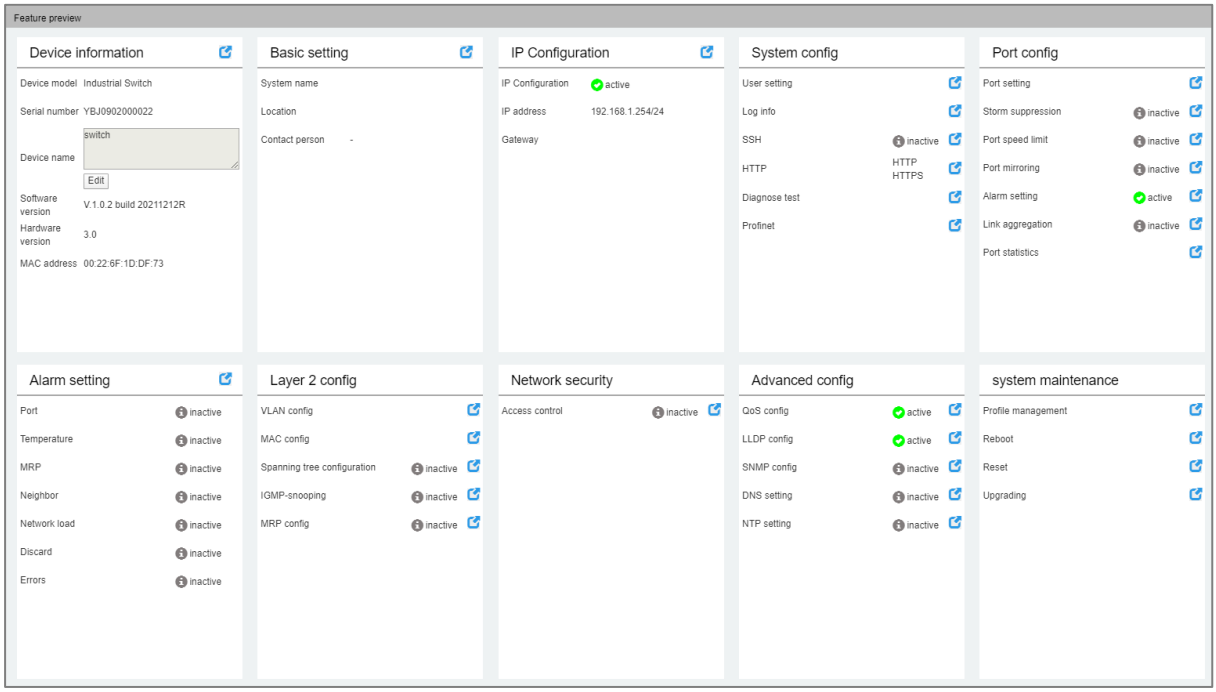
- Device information
- Basic Settings
- IP Configuration
- System Configuration
- Port configuration
- Alarm Settings
- Layer 2 Configuration
- Network Security
- Advanced Configuration
- System Maintenance

Operation Path

Open in order: "Main Menu > System Config > Version Information".

Interface Description

The version information interface is as follow:



The main element configuration description of version information interface:

Interface Element	Description
Device information	**Device Information Configuration Bar**
Device model	The batch number used by the device to facilitate the management of device tags.
Serial number	Serial number of the device
Device name	Network identity used by the device, which can be entered manually
Software Version	Current software version information, updated software version with more features.
Hardware Version	Current hardware version information, pay attention to the hardware version limits in software version.
MAC address;	Hardware address of device factory configuration.
Basic Settings	**Setting the basic configuration bar**
System Name	Device name.
Location	Device installation location.
Contact person	Device contact information.
IP Configuration	**IP Configuration Bar**
IP Configuration	Display the activated state of IP configuration
IP address	IP address and subnet mask information of the device
Gateway	Gateway address information of the device

Interface Element	Description
System Configuration	**System Configuration Area Bar**
System Configuration	System configuration functions and edit button options are as follows: • User Settings • Log Information • SSH: SSH service status • Telnet: TELNET service status • HTTP: HTTP or HTTPS status - HTTP: HTTP enable - HTTPS: HTTPS enable - HTTP HTTPS: HTTP and HTTPS enabled • Diagnose Test • PROFINET
Port Configuration	**Port Configuration Area Bar**
Port Configuration	Port configuration functions and edit button options are as follows: • Ports Configuration • Storm Suppression • Port Speed Limit • Port mirroring • Alarm Settings • Link Aggregation • Port Statistics
Alarm Settings	**Alarm Settings Area Bar**
Alarm Settings	Alarm settings function and edit button options are as follows: • Port • Temperature • MRP • Neighbor • Network Load • Discard • Errors
Layer 2 Configuration	**Layer 2 Configuration Area Bar**
Layer 2 Configuration	Layer 2 configuration functions and edit button options are as follows:

Interface Element	Description
	• VLAN Configuration • MAC Configuration • Spanning-tree Configuration • IGMP-snooping Configuration • MRP Configuration
Network Security	**Network Security Area Bar**
Network Security	Network security features and edit button options are as follows: • Access Control
Advanced Configuration	**Advanced Configuration Area Bar**
Advanced Configuration	Advanced configuration functions and edit button options are as follows: • QOS Configuration • LLDP Configuration • SNMP Configuration • DNS Configuration • NTP Configuration
System Maintenance	**System Maintenance Area Bar**
System Maintenance	System maintenance functions and edit button options are as follows: • Profile management • Reboot • Reset • Upgrading

3.2 Basic Settings

Function Description

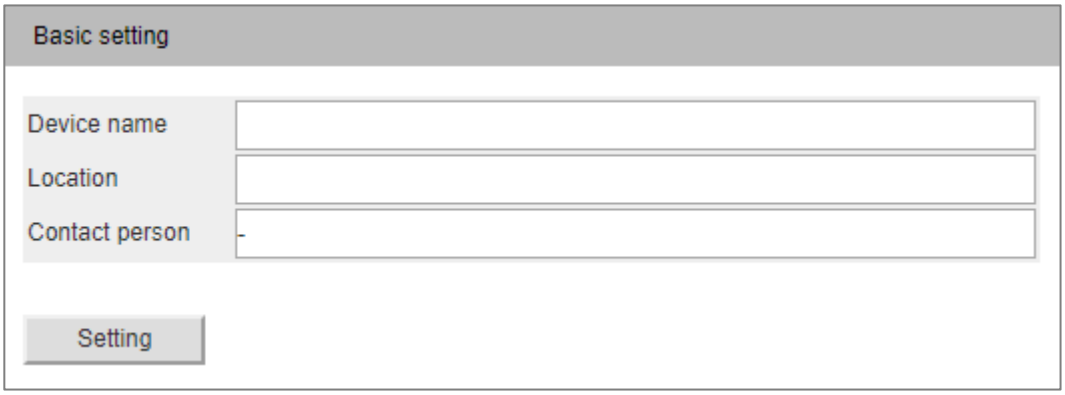
On the “Basic Settings” page, you can configure information such as the name, location and contact person of the device.

Operation Path

Open in order: "System Configuration > Basic Settings".

Interface Description

The basic settings interface as follows:



The main element configuration description of basic settings interface:

Interface Element	Description
Device name	Identification name of the device in the network.
Location	Installation position of device, which is convenient for locating.
Contact person	Device contact name.

3.3 Network Setting

Function Description

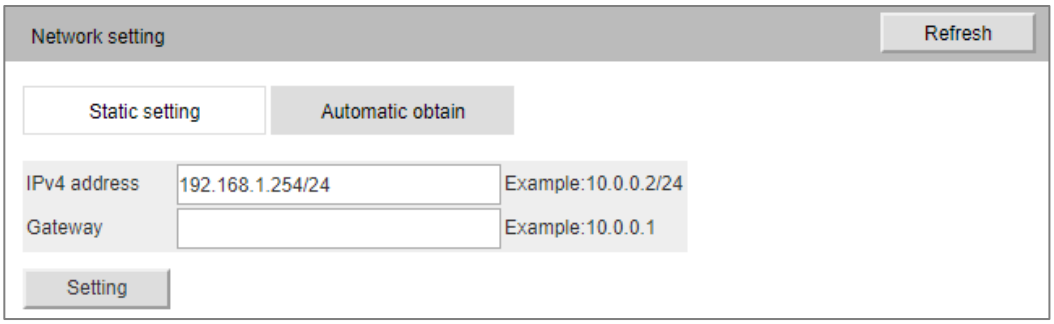
On the “Network Settings” page, user can set the IP address and gateway of this device. Network settings support two modes, static settings and automatic acquisition.

Operation Path

Open in order: " System Configuration > Network Setting".

Interface Description

Network Setting interface as follow:



The main element configuration description of network setting interface:

Interface Element	Description
Network Setting	The access method of IPv4 address, manual configuration and DHCP. • “Static setting”, that is entering static IP address. User needs to fill in IPV4 address and gateway manually; • "Auto obtain", auto-obtain means that the DHCP function is enabled. At this time, the IP address of the device can be obtained through the HyperTermina.
IPv4 address	Manually enter the IP address and subnet mask information of the device, for example: 10.0.0.0/24.
Gateway	Fill in the gateway address information of the device, for example: 10.0.0.1.

3.4 User Settings

Function Description

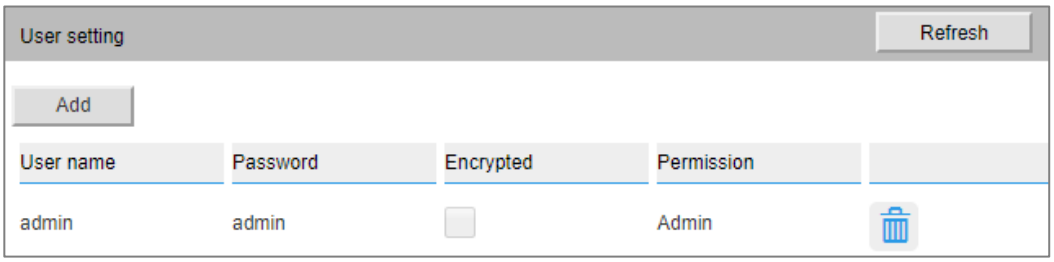
In the "User setting" page, users can add and delete users freely. Users need to access the device by login with user name and password. The initial user name and password are both: admin.

Operation Path

Open in order: "Main Menu > System Config > User setting".

Interface Description

User settings interface as follows:



The main element configuration description of user configuration interface:

Interface Element	Description
Username	Visitor ID, cannot be empty. Note: Up to 31 characters, if the system already has this user, change the corresponding password and permissions.
Password	Password for Visitor, cannot be empty, up to 31 characters.
Encrypted	Encryption mode check box: • Check: Use encrypted password • Uncheck: use cleartext password
permission	The visitor's privilege: • User • Admin Note: • Privilege user: Only conduct read-only operation in the command line; • Privilege admin: It can conduct all operations. • In this device, these privileges only work when user adopts Telnet or HyperTerminal to access the device. Any privilege in the WEB interface can perform all operations.

3.5 Log Information

Function Description

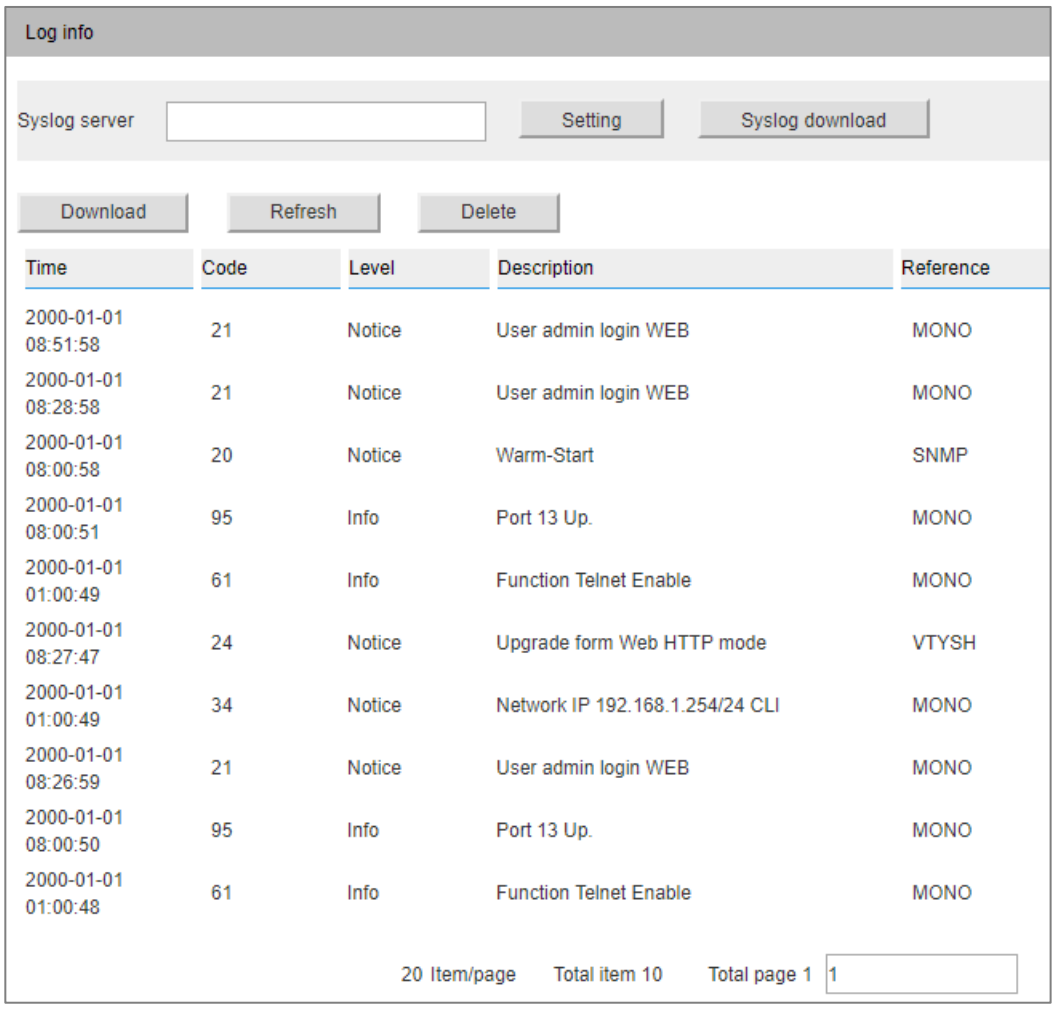
On the "Log Configuration" page, user can view the log information of the device and download the log information to the local host.

Operation Path

Open in order: “Main Menu > System Configuration > Log Information”.

Interface Description

Log information interface as follow:



Main elements configuration description of log information interface:

Interface Element	Description
Syslog Server	The IP address of the log server can remotely monitor the log information of the device.
Time	The date and time when the log information occurred, the format is: Year-Month-Day Hour:Minute:Second
Code	Log information code, please refer to the Appendix for the corresponding specific description and level.
Level	Alarm level of log information.
Description	Description of specific log information events
Reference	Log Information Module.
Operation	The operation button options are as follows: • Download: Download the current log information ".log" file

Interface Element	Description
	to the local host; • Refresh: Refresh the log information and reload the log list; • Delete: Clear all current log information.

3.6 SSH HTTP Settings

The full English name of SSH is Secure Shell. SSH is a security protocol based on application layer and transmission layer. SSH is a reliable protocol which provides security for remote login sessions and other network services. Using SSH protocol can effectively prevent information leakage in the process of remote management, and can also prevent DNS and IP spoofing. In addition, the transmitted data is compressed so that the transmission speed can be increased.

Currently there are two incompatible versions of SSH: SSH1 AND SSH2. SSH1 could be divided into two versions, 1.3 and 1.5. SSH2 uses DSA (Digital Signature Algorithm) and RSA (Asymmetric Cryptographic Algorithm) to switch. SSH2 uses DSA (Digital Signature Algorithm) and Diffie-Hellman (DH) to replace RSA in exchanging symmetric key. Device supports encryption algorithms like AES, ARC4 and 3DES.

To achieve the secure connection of SSH during communication, there are five stages to go through between server and client:

- Version number negotiation: at present, SSH includes two versions, SSH1 and SSH2. The version to be used is determined via version negotiation.
- Key and algorithm negotiation phase: SSH supports multiple encryption algorithms, both sides negotiate a algorithm that it eventually uses according to the supported algorithms.
- Authentication phase: SSH client sends authentication request to server, then the server authenticates the client.
- Session request phase: client sends cession request to server when the authentication is approved;
- Session phase: server and client exchange information when the session request

is approved.

2 verification modes during SSH login:

- Verification mode based on account and password;
  - The client uses the session key generated during key and algorithm negotiation phase to encrypt account, authentication mode and password, and sends the results to the server.
  - The server uses the obtained session key to decrypt messages and gets the account and password.
  - The server judges this account and password, if failed, it would send authentication failure message to the client, which includes the list of reauthentication methods.
  - The client selects a method from the authentication method list to re-authenticate.
  - This process would repeat until the authentication succeeds or authentication times reach the limit. The server closes this TCP connection.
- Verification mode based on public and private key. This verification mode is not available on this device presently.

This series device supports SSH server function, which can accept connections of multiple SSH clients, so as to login to the remote device via SSH. SSH configuration function needs to be enabled on the WEB interface, authenticated username and password need to be configured on the command line interface.

Function Description

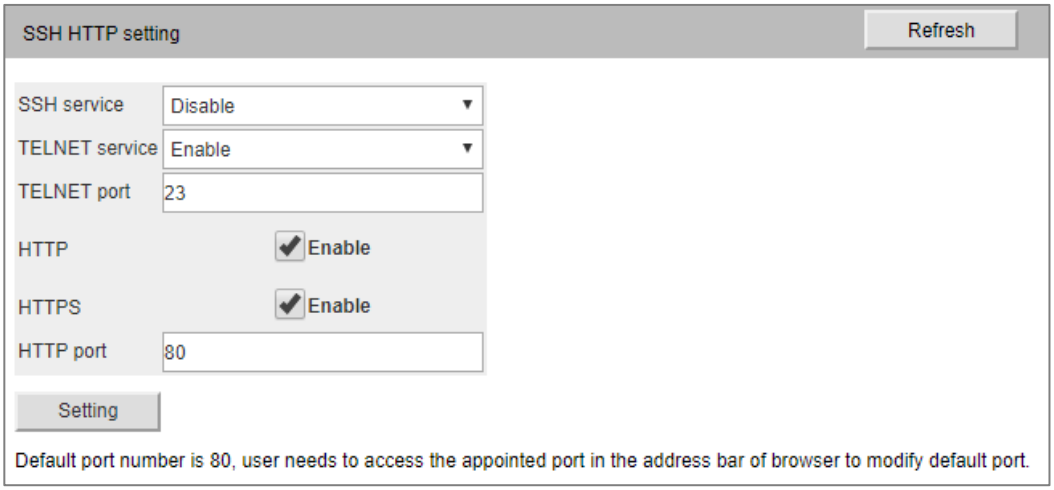
On the “SSH HTTP Settings” page, you can enable/disable service functions such as SSH, TELNET, HTTP and HTTPS, and configure the port number corresponding to the protocol.

Operation Path

Open in order: "Main Menu > System Configuration > SSH HTTP Configuration".

Interface Description

SSH HTTP configuration interface is as follows:



The main element configuration description of SSH HTTP settings interface:

Interface Element	Description
SSH service	SSH service function status, the options are as follows: • Enable; • Disable
TELNET Service	TELNET service function status, the options are as follows: • Enable; • Disable
TELNET port	TELNET service port number, default port number is 23.
HTTP	Device HTTP protocol function status, enable check box. Note: HTTP access format is: HTTP://192.168.1.254, Address is corresponding switch IP address.
HTTPS	Device HTTPS protocol function status, enable checkbox. Note: HTTPS access format is: HTTPS://192.168.1.254, Address is corresponding switch IP address.
HTTP port	HTTP protocol service port number, the default port number is 80, if the default port is modified, specify the port number in the browser address bar while accessing.

3.7 Diagnostic Test

3.7.1 Ping

Function Description

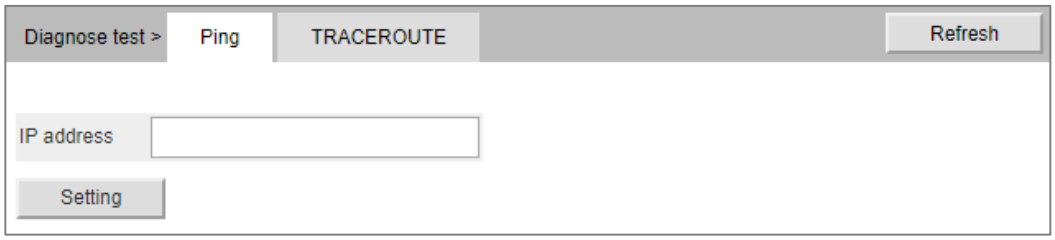
On the "Ping" page, Ping is used to check whether the network is open or network connection speed. Ping utilizes the uniqueness of network machine IP address to send a data packet to the target IP address, and then ask the other side to return a similarly sized packet to determine whether two network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

Operation Path

Open in order: "Main Menu > System Config > Diagnosis > Ping".

Interface Description

The Ping interface is as follows:



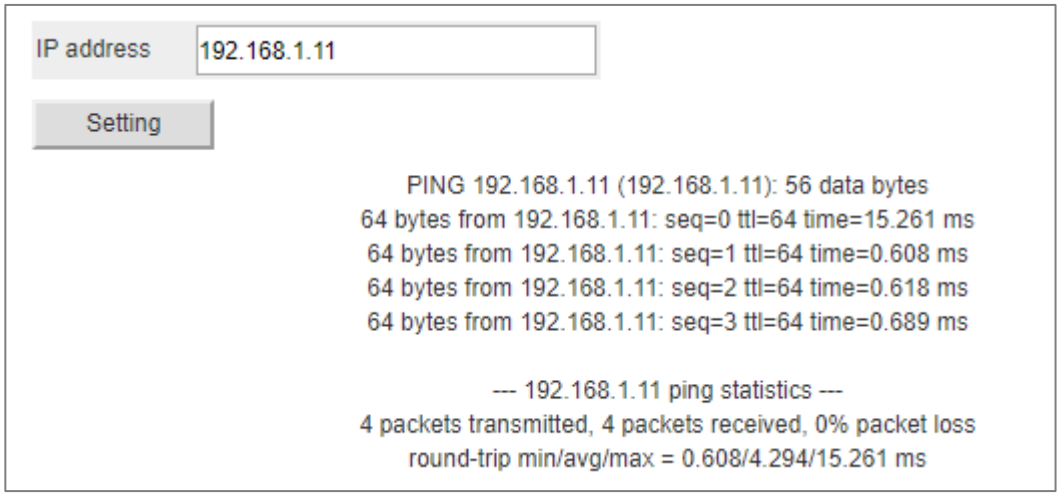
The main elements configuration description of Ping configuration interface:

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

Ping Configuration:

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

Step 2 Click the "Set" to see the Ping results;



Step 3 End.

3.7.2 TRACEROUTE

Function Description

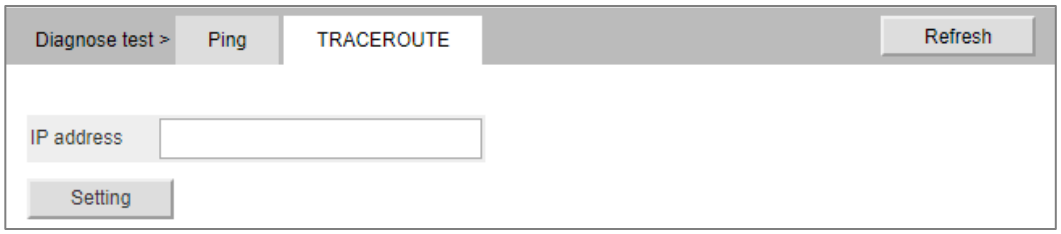
In the "Traceroute" page, users can test the network situation between the switch and the target host. Traceroute measures how long it takes by sending small packets to the destination device until they return. Each device on a path Traceroute returns three test results. Output result includes each test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

Operation Path

Open in order: "Main Menu > System Config > Diagnosis > Traceroute".

Interface Description

TRACEROUTE interface as follows:



The main element configuration description of Traceroute interfaces:

Interface Element	Description

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.

3.8 PROFINET

Function Description

On the "PROFINET" page, users can configure DCP functions and download GSD configuration files.

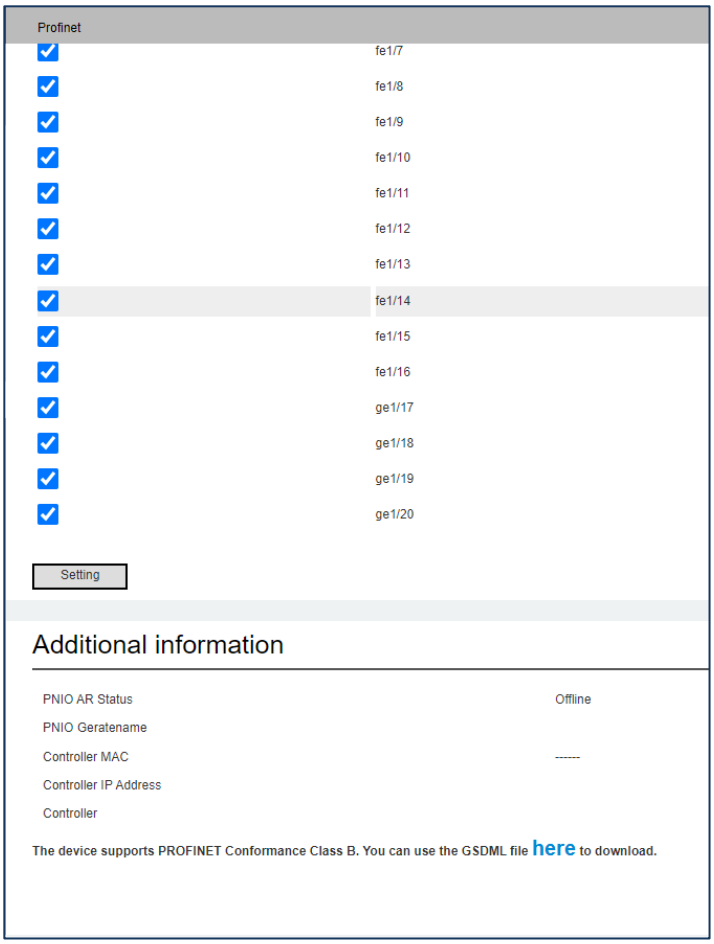
PROFINET is an open industrial Ethernet technology based on Ethernet applicable to the real-time automation industry. This switch is a PROFINET IO device, which meets the consistency category CC-B, can connect to PC/PG/MHI devices, distributed IO devices and IO controllers, etc., and supports non-cyclic transmission of engineering configuration data, diagnostic data and interruption, as well as cyclic transmission of user data.

Operation Path

Open in order: "System Configuration > PROFINET".

Interface Description

PROFINET interface is as below:



Main elements configuration descriptions of PROFINET interface:

Interface Element	Description
DCP Configuration	**DCP Configuration Area Box**
Enable DCP-TX	Check box, enable state configuration of port DCP.
Port	Device port name.
Additional Info.	**Additional information area box**
PNIO AR status	Profinet IO device application relationship status.
PNIO device name	The name of Profinet IO device.
Controller MAC	Controller MAC address information.
Controller IP address	Controller IP address.
Regulator	Regulator name.

4 Port Configuration

4.1 Port Settings

Function Description

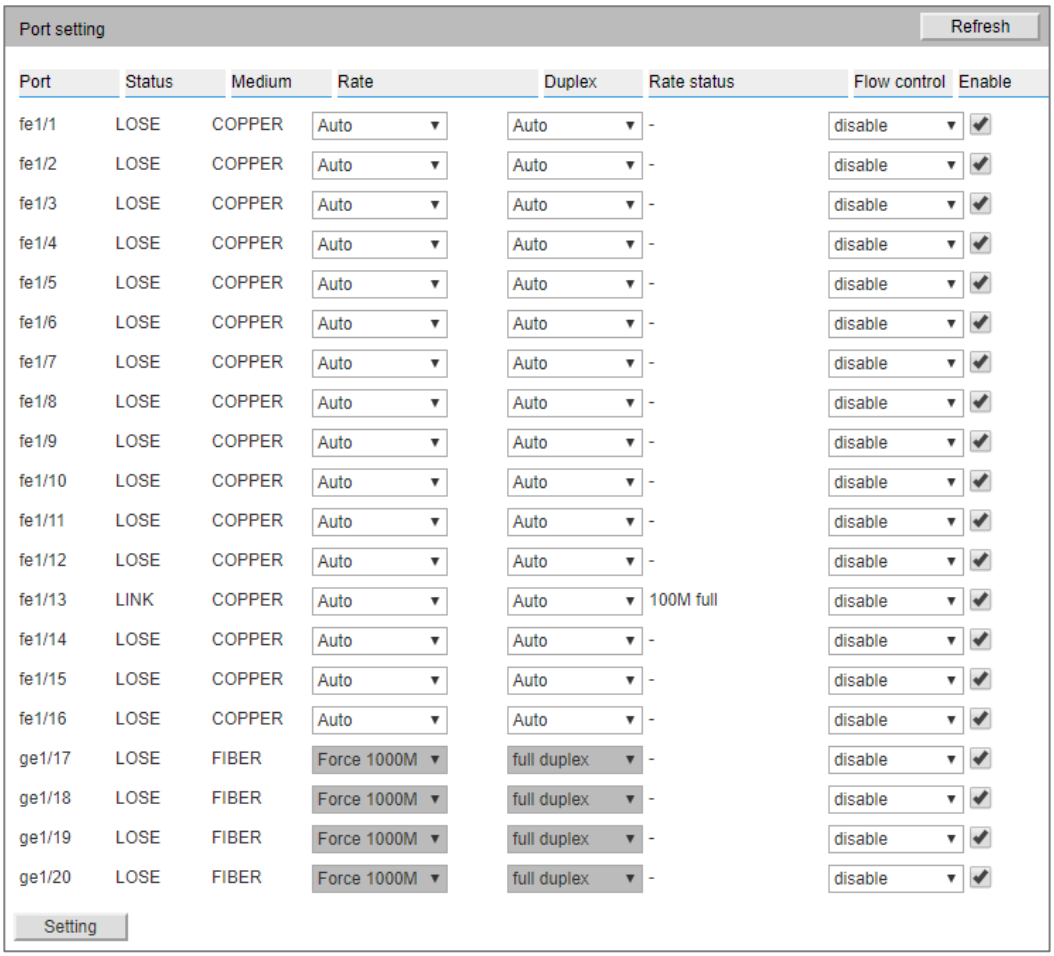
On the "Port Setting" page, user can check port type, rate and connection state, set rate mode, duplex mode, port enable, flow control and other parameters.

Operation Path

Open in order: "Main Menu > Port Config > Port Settings".

Interface Description

Port setting interface as follows:



Main elements configuration description of port settings interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Status	Ethernet port connection status, display status as follows: • LOSE: represent the port is disconnected; • LINK: represent the port is connected.
Medium	Ethernet port connection type, display medium as follows: • COPPER; • FIBER.
Rate	Ethernet port working speed, optional speed as follows: • Auto: that is 10/100/1000M speed self-adaption; • Specified 10M; • Force 100M; • Force 1000M.
Duplex	Under current Ethernet working mode, optional mode as follows: • Auto;

Interface Element	Description
	• Full duplex; • Half duplex
Rate Status	Current Ethernet port working rate, display rate as follows: • -: port is disconnected; • 1000M full: Gigabit full duplex; • 100M full: 100M full duplex; • 100M half: 100M half duplex; • 10M full: 10M full duplex; • 10M half: 10M half duplex.
Flow control	Port flow control status, options as follows: • Close: disable; • tx: enable the port to send data flow control; • rx: enable flow control of port data receiving; • All: Enable port data sending and receiving flow control.
Enable	Enable Ethernet port. Notice: If user doesn't check the port "Enable" checkbox, the port won't be connected to use.

4.2 Storm Suppression

Function Description

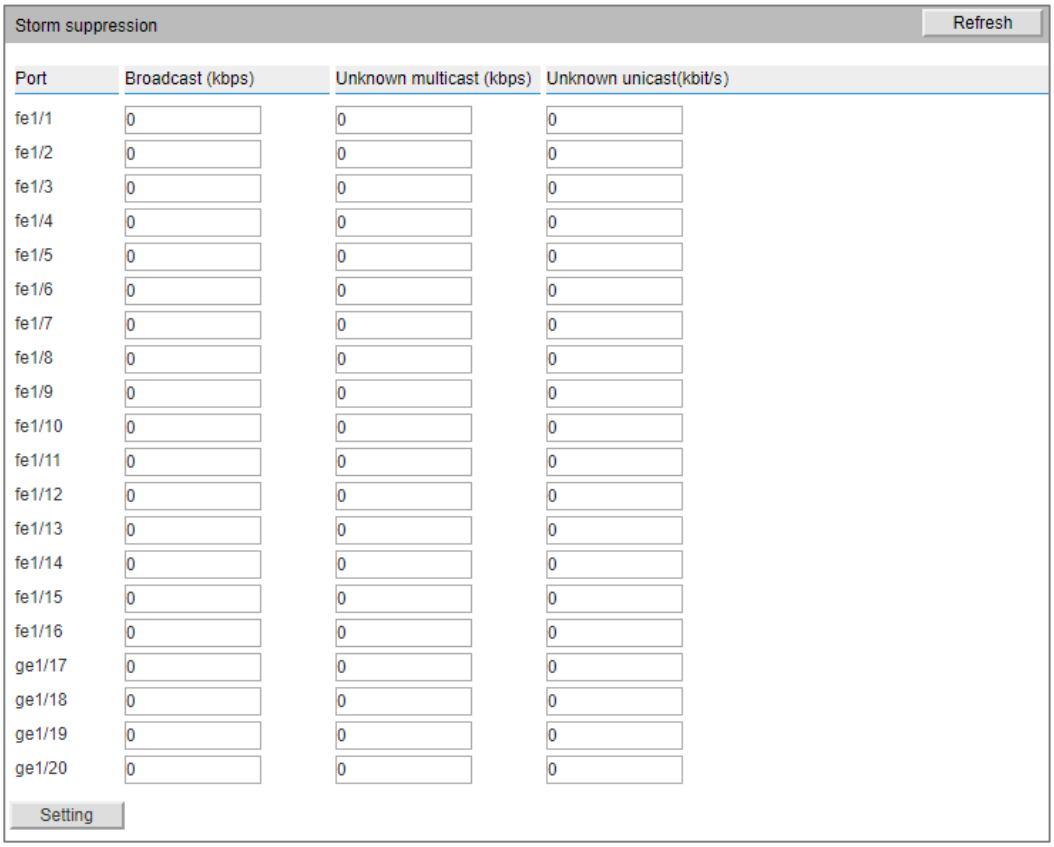
On the "Storm Control" page, user can set the maximum broadcast, multicast or unknown unicast packet flow the port allows. When the sum of each port broadcast, unknown multicast or unknown unicast flow achieves the value user sets, the system will discard the packets beyond the broadcast, unknown multicast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

Operation Path

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

Interface Description

Storm control interface as follows:



Main elements configuration description of storm suppression interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Broadcast (kbps)	The port control for broadcast packet transmission speed, input value range 0-100000. Note: • Broadcast packet, namely, the data frame with the destination address of FF-FF-FF-FF-FF-FF. • The input value needs to be an integral multiple of 64, otherwise it would adjust to smaller value automatically.
Unknown Multicast (kbps)	The port control for unknown multicast data packet transmission speed, input value range 0-1000000. 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.

Interface Element	Description
	• The input value needs to be an integral multiple of 64, otherwise it would adjust to smaller value automatically.
Unknown Unicast (kbps)	The port control for unknown unicast data packet transmission speed, input value range 0-1000000. 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. • The input value needs to be an integral multiple of 64, otherwise it would adjust to smaller value automatically.

4.3 Port Rate Limit

Function Description

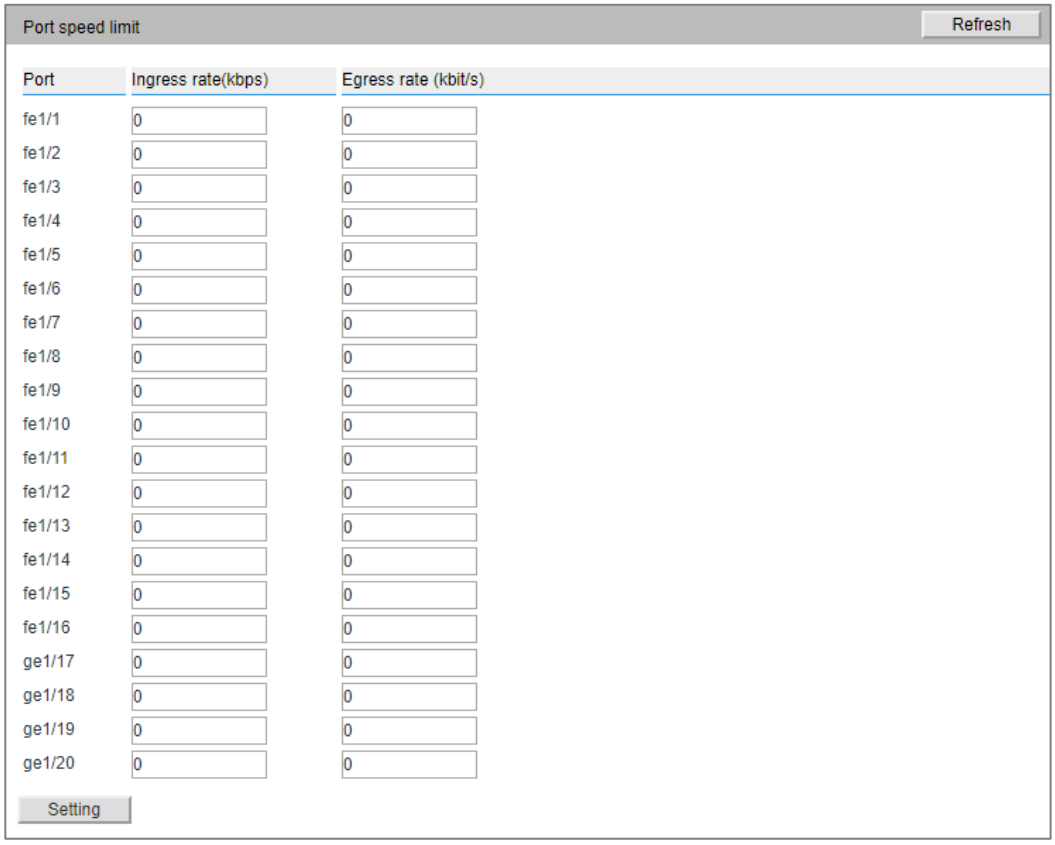
On the "Port rate-Limit" page, User can limit the communication flow of each port or cancel the port flow limit. The device provides port speed limit, including entrance and exit speed limit. User can select a fixed speed, its range is: 0kbps~1000Mbps (1000M), the device will discard the packet or adopt flow control to limit the transmission speed or receiving speed of opposite device according to the flow control is enabled or not.

Operation Path

Open in order: "Main menu > Port Config > Port rate-Limit".

Interface Description

Port rate limit interface as follows:



The main element configuration description of port rate limit interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Ingress Rate(kbps)	The port limit for all input data transmission speed, input value range 0-1000000.
Egress Rate(kbits)	The port control for all output data transmission speed, input value range 0-1000000.

Note

1. When using the port rate limit, flow control should be enabled, otherwise the rate between devices will no longer be a smooth curve;
2. 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.
3. Port speed limit has high requirements on network cable quality, otherwise lots of conflict packets and broken packet would appear.

4.4 Port Mirroring

Function Description

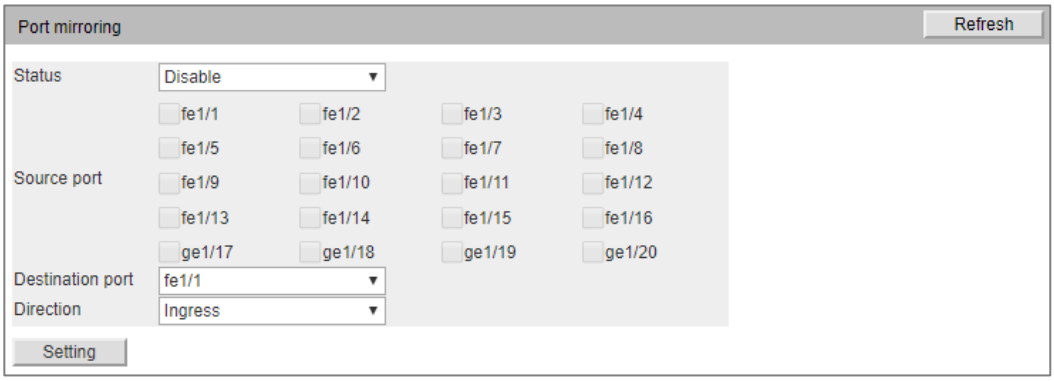
On the "Port mirroring" page, user can copy the data from the origin port to appointed port for data analysis and monitoring.

Operation Path

Open in order: "Main Menu > Port Config > Mirror".

Interface Description

Port mirror interface as follows:



The main element configuration description of port mirror interface:

Interface Element	Description
Status	Port mirroring enable drop-down list, options are as follows: • Enable • Disable: disable
Source port	A set of monitored ports, which will collect data from these ports in the specified direction, and the mirror port can be one or more.
Destination port	A port for monitoring, and the device outputs data from the port to the specified direction.
Direction	This parameter specifies the direction of the monitoring port data, a total of "ingress", "egress", "both" three options. Monitor can choose according to their own needs. • ingress: import data, the packet received by the port will be mirrored to the destination port;

Interface Element	Description
	• egress: export data, the message sent by the port will be mirrored to the destination port; • Both: all data, mirror the port receiving and sending packets at the same time.

Note

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

4.5 Alarm Settings

Function Description

On the page of "Alarm Warning", user can configure the trigger event and receiving method of alarm; when the equipment runs abnormally, it can promptly notify the administrator, and quickly repair the equipment to avoid excessive loss. The alarm functions are as follows:

- Port;
- Temperature;
- Voltage;
- MRP;
- Neighbor;
- Network Load;
- Discarded Packets;
- Error.

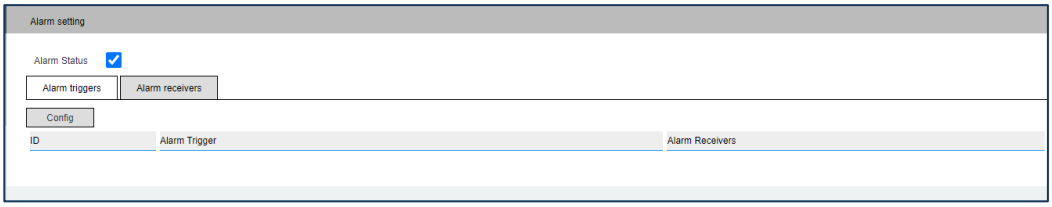
Operation Path

Open in order: "Main Menu > Port Config > Alarm Settings".

4.5.1 Alarm Trigger

Interface Description

Alarm Trigger interface as below:

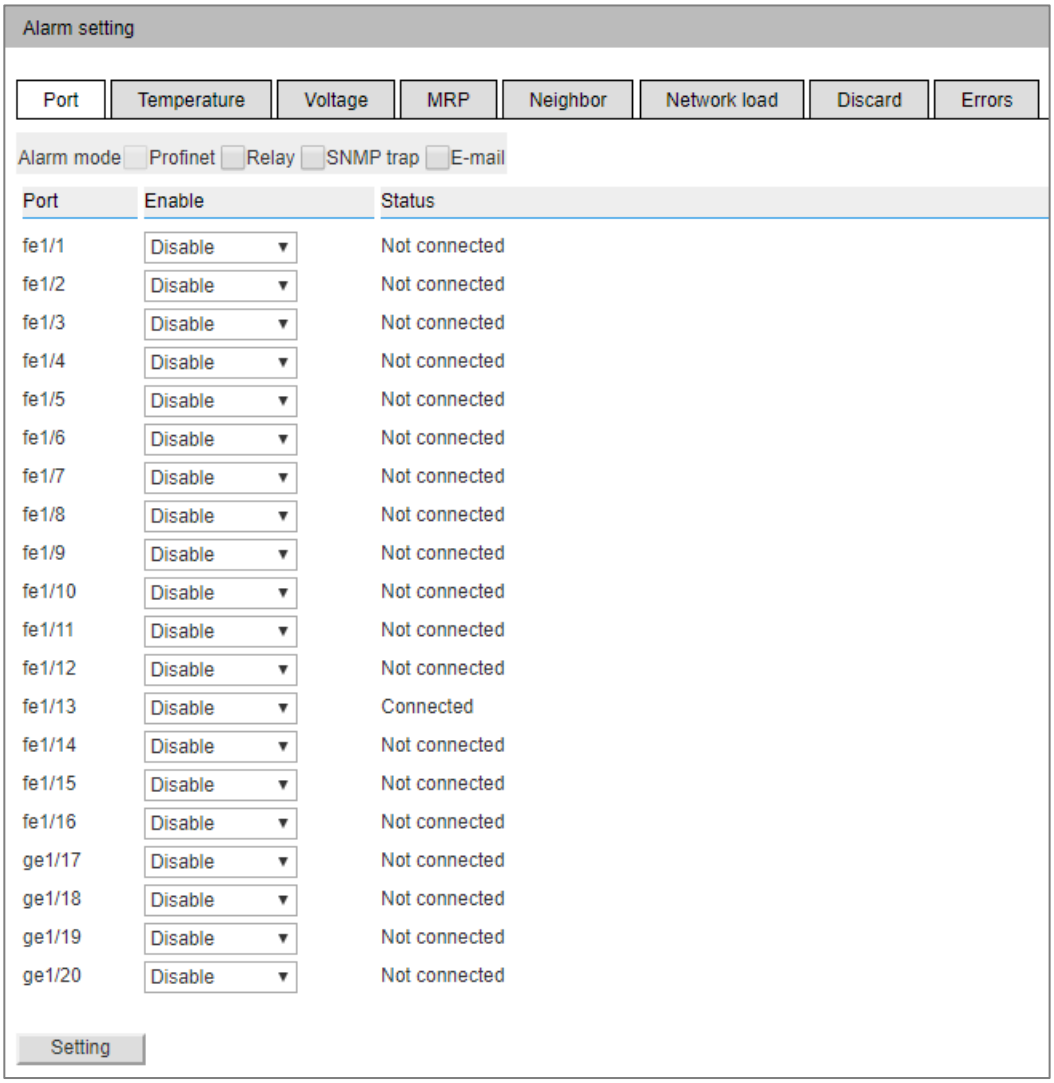


The main element configuration description of alarm Trigger:

Interface Element	Description
Alarm status	Alarm status check box, when checked, the alarm function can be turned on.
ID	Alarm ID
Alarm Trigger	Trigger an alarm event, and support alarms such as port, temperature, MRP, neighbor, network load, packet loss, error, etc.
Alarm receivers	The alarm receiving mode supports PROFINET, Relay, SNMP Trap and e-mail.
Buttons	Configuration: Configure alarm triggering events. Edit: Edit the current alarm entry. Delete: delete the the current alarm entry.

Interface Description: Port

Port interface as below:



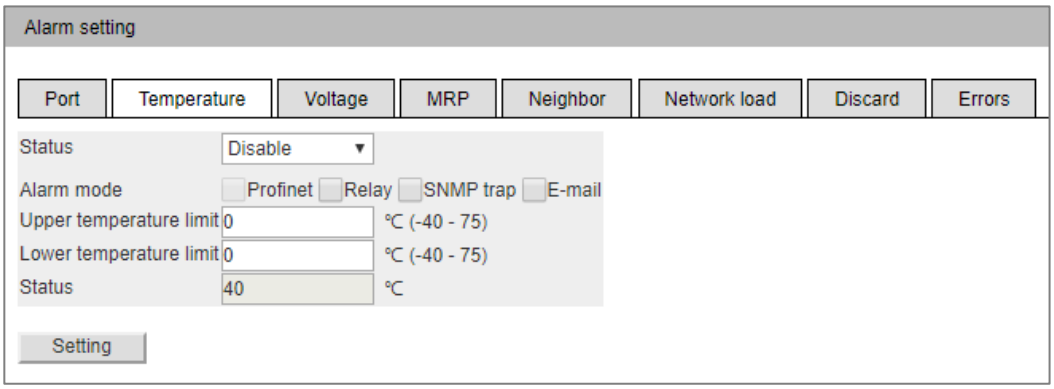
The main element configuration description of port interface:

Interface Element	Description
Alarm mode	Alarm mode check box, the options are as follows: • Profinet: display the alarm mode of Profinet. If the device is configured on the configuration software and related alarm items are configured, the corresponding Profinet check box will be checked. The related alarm items cannot be modified on the page after being checked. • Relay: send alarm information by changing the state of relay; • SNMP trap: send alarm information through SNMP trap protocol; • E-mail: Send alarm information by mail.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Enable	Port alarm function status, options as follows: • Enable; • Disable. Note: After enable port alarm, when port occurs abnormal status, such as connection break down, the device will output a signal to hint the abnormal operation of device.
Status	Port link status, display items as follows: • Not connected; • Connected.

Interface Description: Temperature

Temperature interface is as below:



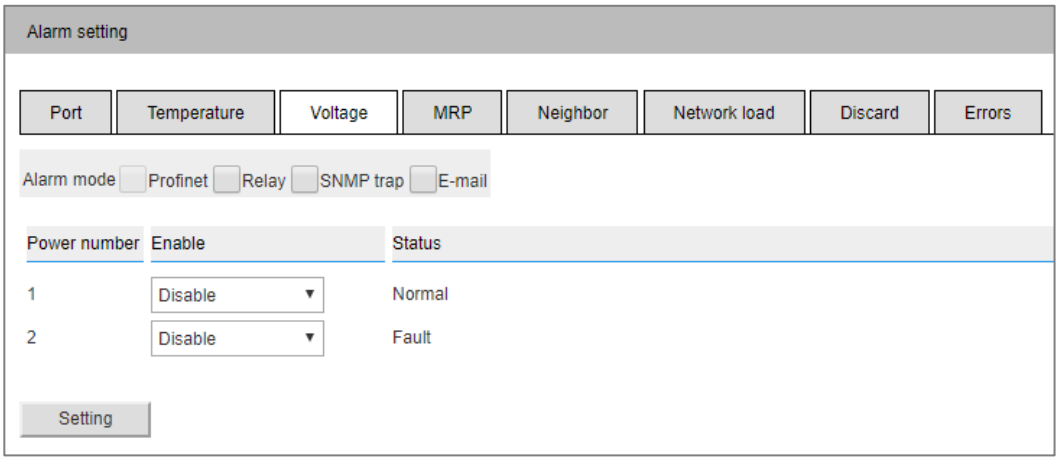
Configuration description of main elements of the Temperature interface:

Interface Element	Description
Status	The drop-down list of Temperature alarm status. The options are as follows: • Disable; • Enable.
Alarm mode	Alarm mode check box, the options are as follows: • Profinet: display the alarm mode of Profinet. If the device is configured on the configuration software and related alarm items are configured, the corresponding Profinet check box will be checked. The related alarm items cannot be modified on the page after being checked.

Interface Element	Description
	• Relay: send alarm information by changing the state of relay. • SNMP trap: send alarm information through SNMP trap protocol. • E-mail: Send alarm information by mail.
Upper temperature limit	The upper limit alarm value of the working temperature of the device, unit: ℃, the valid input range is-40~85.
Lower temperature limit	The lower limit alarm value of the working temperature of the device, unit: ℃, the valid input range is-40~85.
Status	Current operation temperature of the device.

Interface Description: Voltage

Voltage interface is as below:



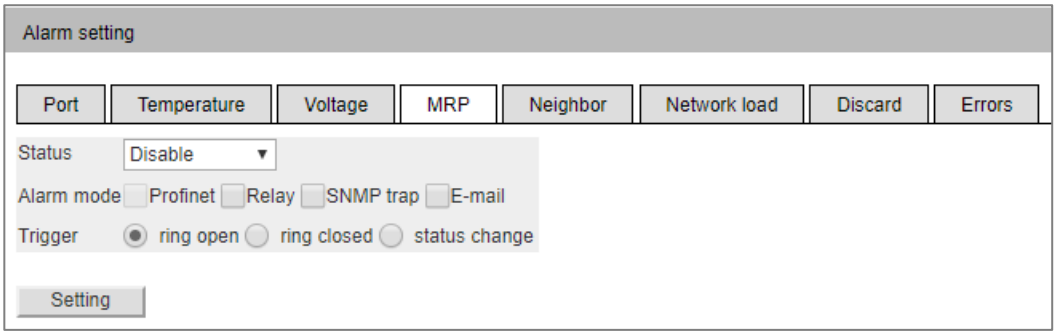
Configuration description of main elements of the Voltage interface:

Interface Element	Description
Alarm mode	Alarm mode check box, the options are as follows: • Profinet: display the alarm mode of Profinet. If the device is configured on the configuration software and related alarm items are configured, the corresponding Profinet check box will be checked. The related alarm items cannot be modified on the page after being checked. • Relay: send alarm information by changing the state of relay. • SNMP trap: send alarm information through SNMP trap

Interface Element	Description
	protocol. • E-mail: Send alarm information by mail.
Power number	The corresponding number of this device's power supply
Enable	The state of power supply alarm function, options are as follows: • Disable • Enable Note: • DC provides 2 power supplies, when one power supply goes wrong, another power supply can supply electricity soon, dual power supply hot standby is supported. • After enabling power supply alarm, the device will output alarm signal to hint abnormal operation of power supply when power supply runs abnormally.
Status	The power supply status of the device.

Interface Description: MRP

MRP interface as below:



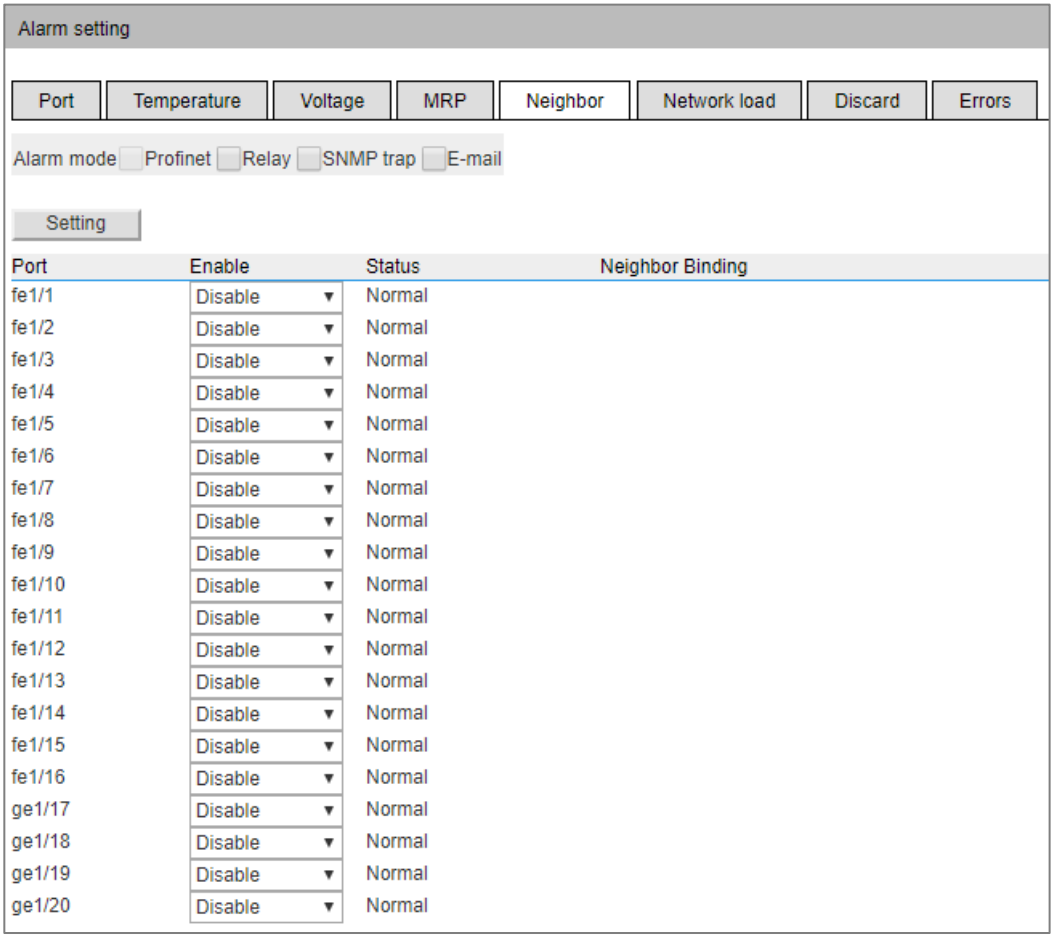
Main elements configuration descriptions of MRP interface:

Interface Element	Description
Status	The drop-down list of MRP alarm status. The options are as follows: • OFF; • Enable.
Alarm mode	Alarm mode check box, the options are as follows: • Profinet: display the alarm mode of Profinet. If the device is configured on the configuration software and related

Interface Element	Description
	alarm items are configured, the corresponding Profinet check box will be checked. The related alarm items cannot be modified on the page after being checked. • Relay: send alarm information by changing the state of relay. • SNMP trap: send alarm information through SNMP trap protocol. • E-mail: Send alarm information by mail.
Trigger	Trigger MRP alarm event, radio box, and the optional events are as follows: • Open loop: the ring network is disconnected; • Closed loop: the ring network is closed; • State change: the state of the ring network changes.

Interface Description: Neighbor

Neighbor interface is as follows:

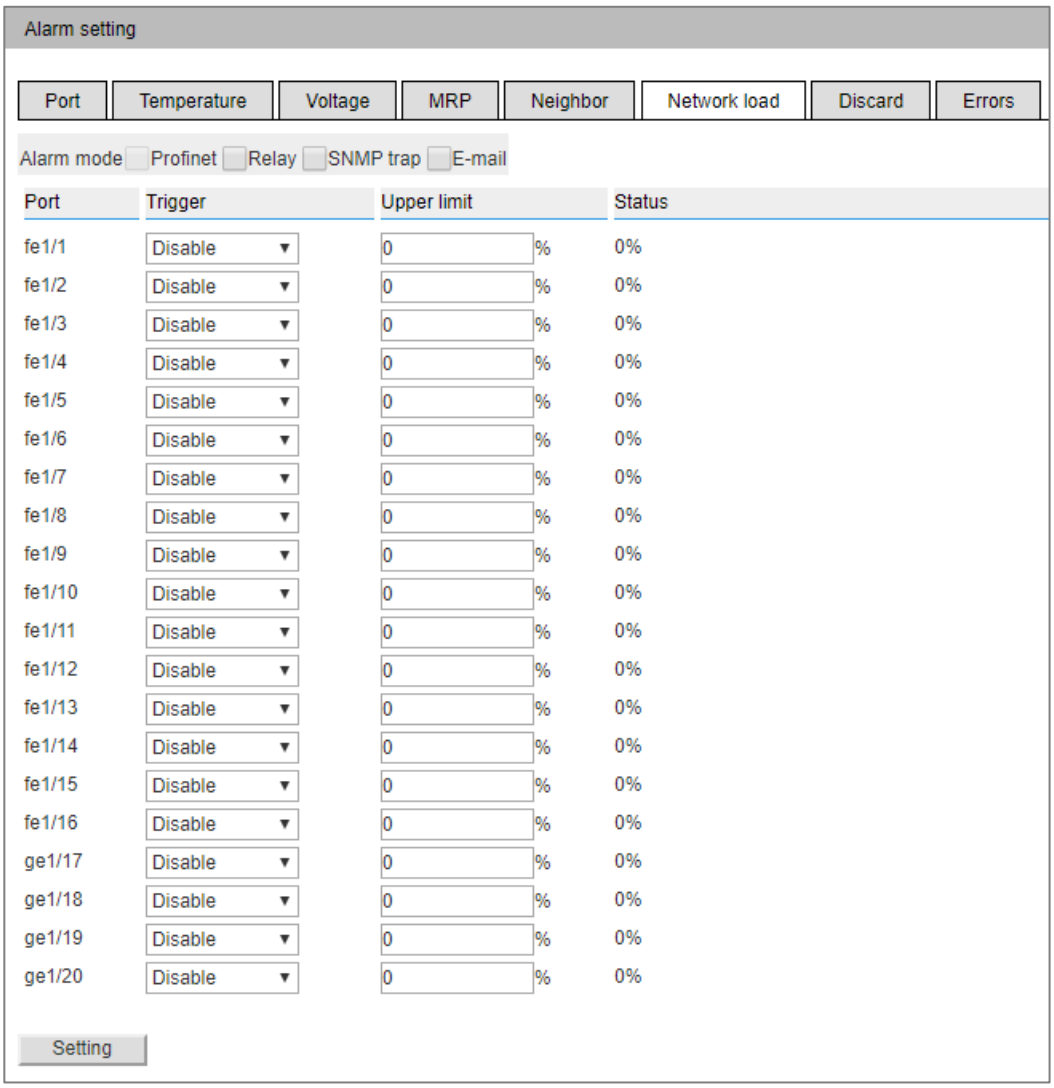


Main elements configuration description of neighbor interface:

Interface Element	Description
Alarm mode	Alarm mode check box, the options are as follows: • Profinet: display the alarm mode of Profinet. If the device is configured on the configuration software and related alarm items are configured, the corresponding Profinet check box will be checked. The related alarm items cannot be modified on the page after being checked. • Relay: send alarm information by changing the state of relay. • SNMP trap: send alarm information through SNMP trap protocol. • E-mail: Send alarm information by mail.
Port	The corresponding port name of the device Ethernet port.
Enable	Displays the neighbor alarm enabled status. Note: Neighbor alarm enable is configured by configuration software, and this page supports alarm mode configuration and related information display.
Status	Display the status of neighbor alarms.
Neighbor Binding	The binding neighbor address of the port.

Interface Description: Network Load

Network load interface is as follows:



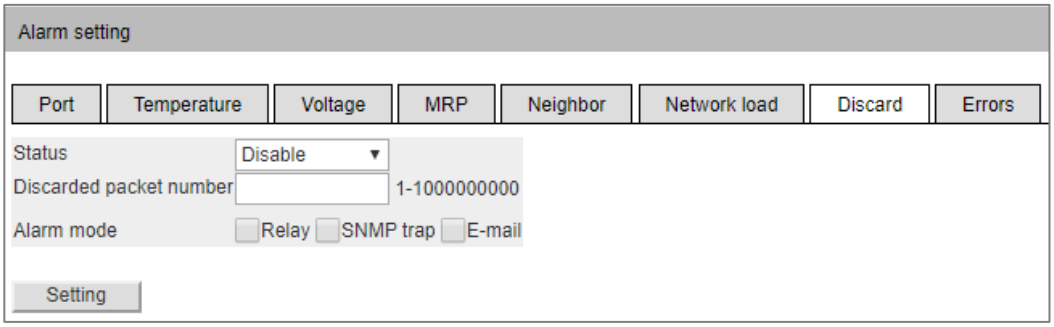
The main element configuration description of network load interface:

Interface Element	Description
Alarm mode	Alarm mode check box, the options are as follows: • Profinet: display the alarm mode of Profinet. If the device is configured on the configuration software and related alarm items are configured, the corresponding Profinet check box will be checked. The related alarm items cannot be modified on the page after being checked. • Relay: send alarm information by changing the state of relay. • SNMP trap: send alarm information through SNMP trap protocol. • E-mail: Send alarm information by mail.
Port	The corresponding port name of the device Ethernet port.
Trigger	Trigger the drop-down list of network load alarm enable. The

Interface Element	Description
	options are as follows: • Enable • Disable
Upper limit	Upper limit value that triggers network load alarm.
Status	Network bandwidth load status.

Interface Description: Packet Loss

Dropped Packets interface is as below:

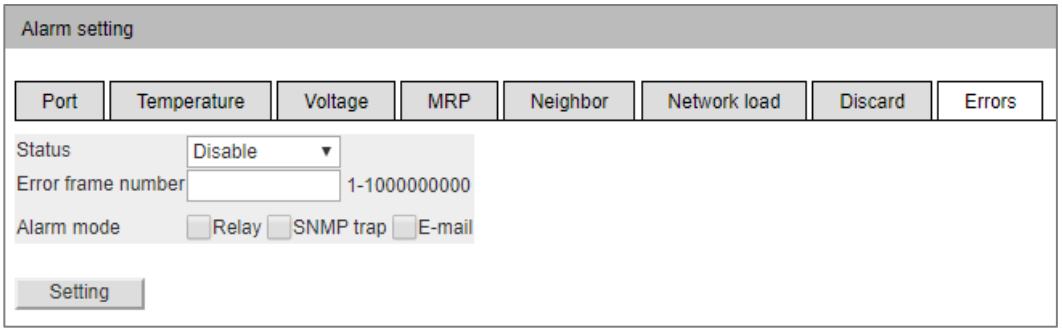


Configuration description of main elements of the Dropped Packets interface:

Interface Element	Description
Status	The status of packet loss alarm, options: • Disable • Enable
Discarded packet number	Threshold value of packet loss alarm
Alarm mode	Alarm mode check box, the options are as follows: • Relay: send alarm information by changing the state of relay. • SNMP trap: send alarm information through SNMP trap protocol. • E-mail: Send alarm information by mail.

Interface Description: Error

Error interface as follows:



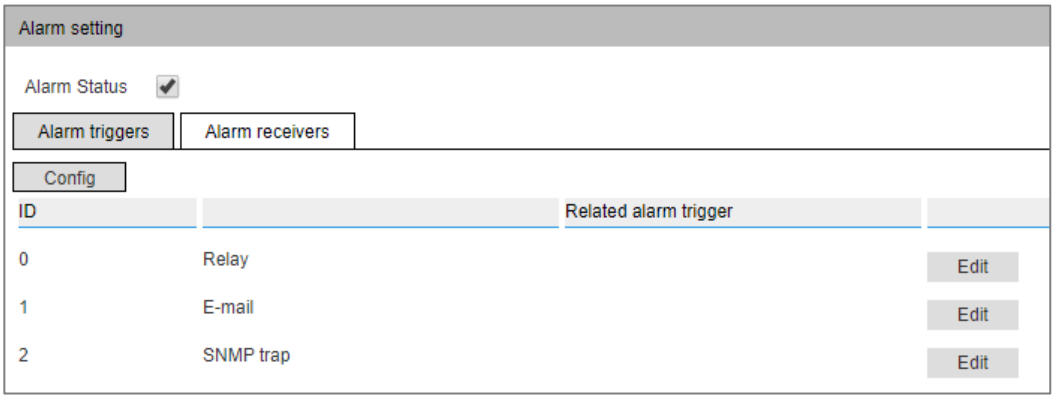
Configuration description of main elements of the Error interface:

Interface Element	Description
Status	Frame alarm status, options: • Disable • Enable
Error frame number	Threshold value of error frame alarm
Alarm mode	Alarm mode check box, the options are as follows: • Relay: send alarm information by changing the state of relay. • SNMP trap: send alarm information through SNMP trap protocol. • E-mail: Send alarm information by mail.

4.5.2 Alarm Setting

Interface Description

Alarm setting interface is as below:

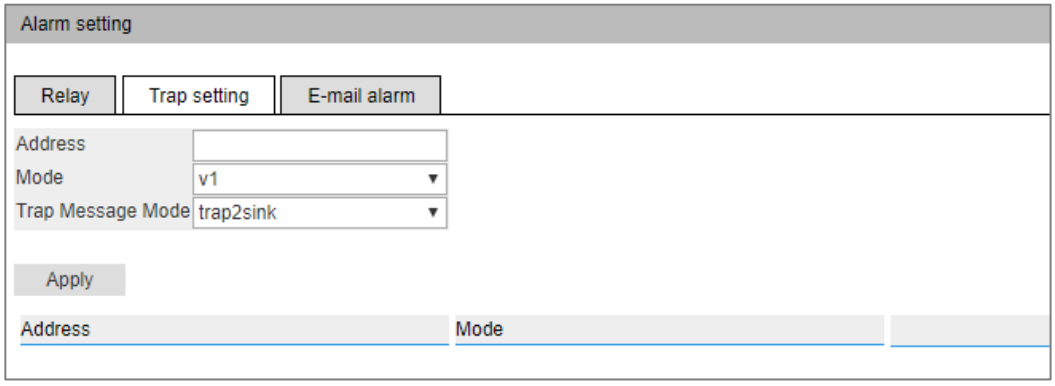


Configuration description of main elements of the Alarm receiving:

Interface Element	Description
Alarm status	Alarm status check box, when checked, the alarm function can be turned on.
ID	Alarm ID
Alarm receiving	The alarm receiving mode and configuration information, it supports relay, SNMP Trap and e-mail.
Related alarm triggering	Alarm triggering events supported by the receiving mode, such as port, temperature, MRP, neighbor, network load, packet loss, error and other alarms.
Buttons	Configuration: Configure the alarm receiving mode. Edit: edit the current alarm receiving method.

Interface Description: Trap Settings

Trap settings interface as follows:



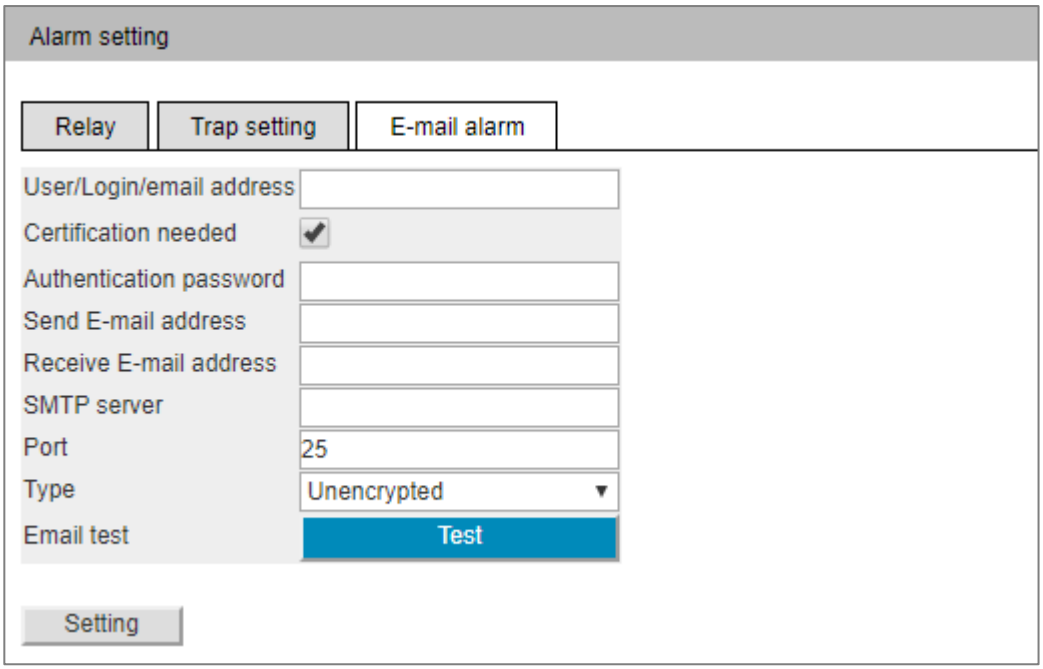
The main element configuration description of Trap settings interface:

Interface Element	Description
Address	Destination IP address of SNMP trap message
Mode	SNMP version drop-down list, the options are as follows: • v1 • v2c
Trap Message Mode	Under SNMP v2c version, the device supports sending different message types, and the options are as follows: • Trap2sink: the device sends Trap information to the network management system. • Informsink: the device sends Inform information to the

Interface Element	Description
	network management system. After sending the Inform alarm, the network management system needs to confirm the receipt. If the device does not receive the confirmation information, it will repeatedly send the alarm until the confirmation information is received or the sending times reach the maximum retransmission times.

Interface Description: Email Alerts

E-Mail Alarm interface is as follows:



Main elements configuration description of E-mail alarm interface:

Interface Element	Description
User/login/email address	Address of the mailbox server.
Certification needed	Require authentication check box.
Authentication Password	Authentication information or login password of sender's mailbox server.
Send e-mail address	E-mail address of sender, account name used for logging in to the E-mail server.

Interface Element	Description
Receive e-mail address	E-mail address used by abnormal event receiver.
SMTP server.	The SMTP email server address should be based on the used email account. The host IP address or used host name that provides E-mail delivery service for the device.
Port	Port number of SMTP server address.
Type	Encryption type, options: • Unencrypted • TLS • STARTTLS
Email test	The device sends an alarm email to the receiving mailbox through the sending mailbox, which is used to test whether the email is in normal communication.

4.6 Link Aggregation

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

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

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

4.6.1 Static Link Aggregation

Function Description

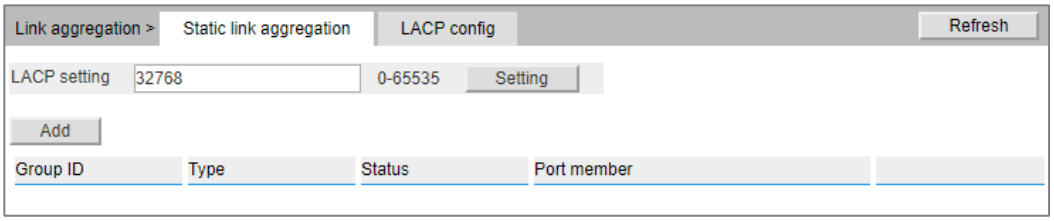
Under static aggregation mode, the member port in aggregation group disables LACP protocol, its port status is maintained manually.

Operation Path

Open in order: "Main Menu > Port Configuration > Link Aggregation > Static Link Aggregation".

Interface Description

Static Link Aggregation interface as below:



The main element configuration description of Static Link Aggregation interface:

Interface Element	Description
LACP setting	LACP priority level setting, LACP setting range 0-65535, defaults to 32768. Note: The smaller of interface LACP priority level value is, the higher priority level is, which is used for distinguishing the priority degree of selecting different ports as active port.
Group ID	Added aggregation group ID number of each port, support maximum 16 groups, each group can configure up to 8 ports to join aggregation.
Type	Aggregation group mode: • Manual: static aggregation; • LACP: Dynamic aggregation.
Status	Aggregation group connection state: • UP: Port member is connected; • DOWN: Port member is disconnected.
Port member	Port member in the aggregation group.
Add	Click "Add" button to add the related configuration of static link

Interface Element	Description
	aggregation.

4.6.2 LACP Configuration

Function Description

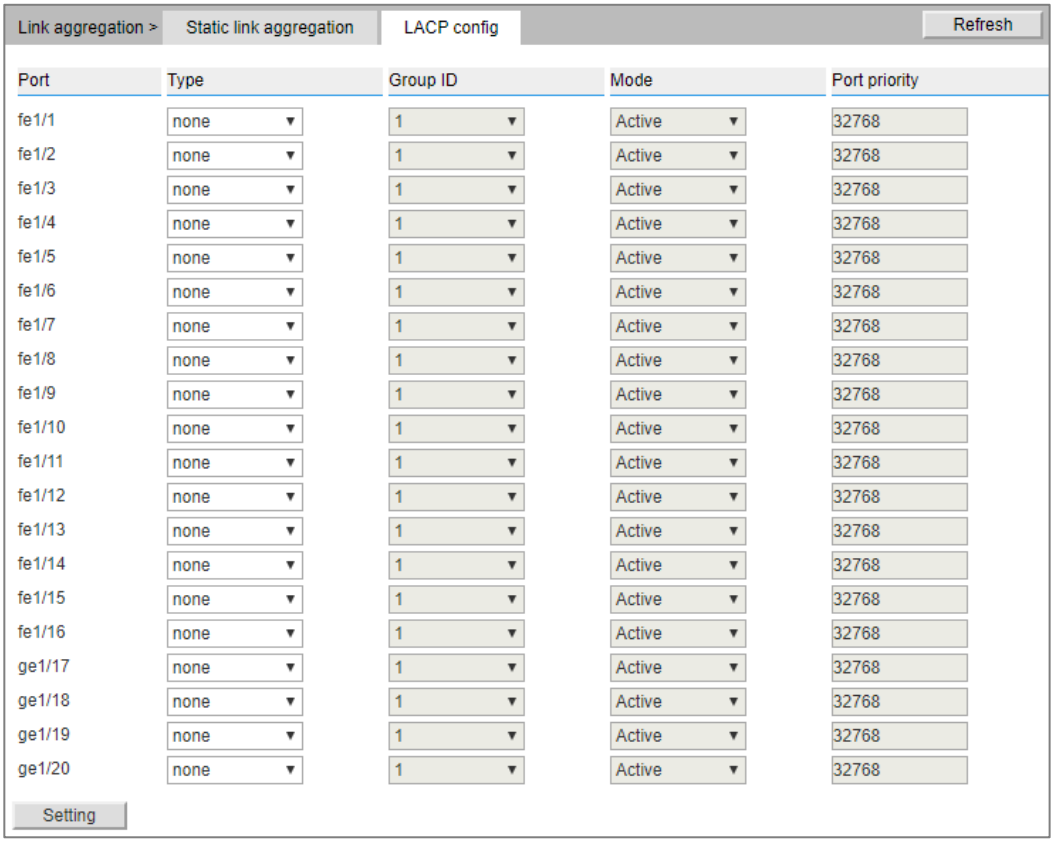
Dynamic aggregation is an aggregation method in which system automatically creates or deletes aggregation group, the port addition and deleting in the dynamic aggregation group is done automatically by LACP protocol. Only ports connected to the same device with same rate, duplex property, and basic configuration can create a dynamic aggregation. Even one port can also create dynamic aggregation, at this time, its single port aggregation. In dynamic aggregation, port LACP protocol is in enable state.

Operation Path

Open in order: "Main Menu > Port Config > Link Aggregation > LACP Config".

Interface Description

LACP configuration interface as follows:



The main element configuration description of LACP configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Type	Setting port aggregation function: • None: Represent the port disabling link aggregation function; • Static: Represent the port is static aggregation mode; • Dynamic (LACP): Represent the port is dynamic aggregation mode.
Group ID	Group ID, the range is 1-16.
Mode	Mode refers to LACP negotiation mode, it's divided into: • Active: The port sends LACP message periodically; • Passive: The port doesn't send LACP message in normal time, once receiving the LACP message of opposite terminal, it will normally send LACP message.
Port priority	Dynamic LACP port priority, defaults to 32768.

4.7 Port Isolation

Function Description

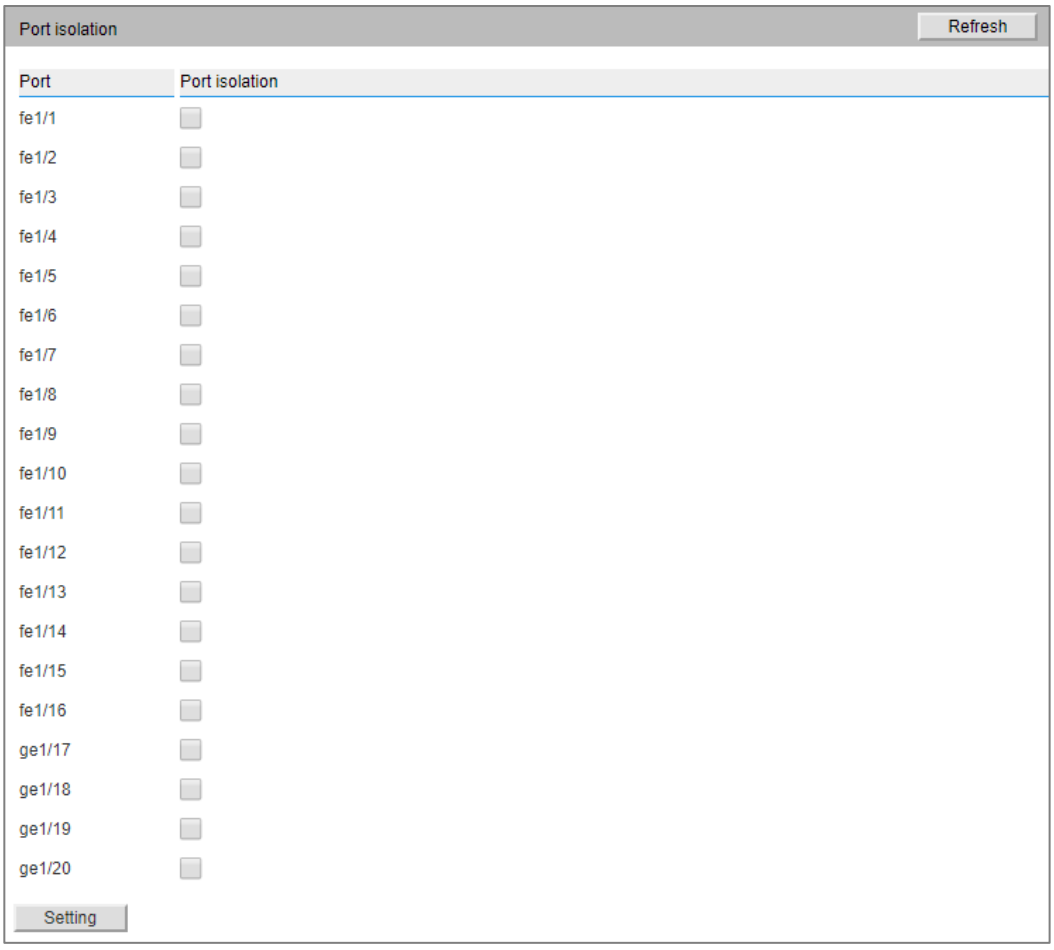
Port isolation is used for the layer 2 isolation between messages. It could add different ports to different VLANs, but waste limited VLAN resources. Adopting isolate-port characteristics can achieve isolation of ports within the same VLAN. After adding the ports to isolation group, user can achieve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

Operation Path

Open in order: "Main Menu > Port Config > Isolate-port Config".

Interface Description

Isolate-port configuration interface as follows:



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

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Port Isolation	Check the port isolation optional box to enable the port isolation function within the same VLAN.

4.8 Port Statistics

4.8.1 Port Statistics

Function Description

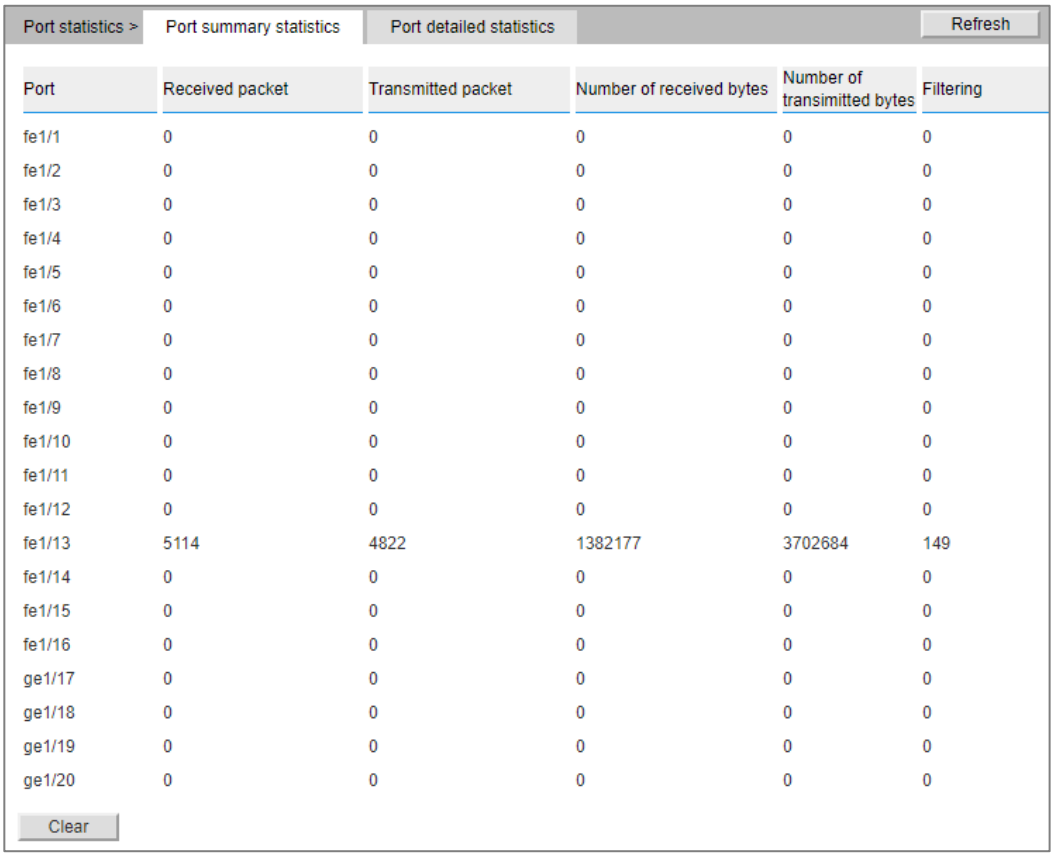
On the "Port Stats" page, user can check the data packet and byte number that each port sends or receives.

Operation Path

Open in order: "Main Menu > Port Config > Port Statistics > Port summary statistics".

Interface Description

Port Statistics interface as follows:



4.8.2 Detail Port Stats

Function Description

On the "Detail port stats" page, user can check the data sum and message size classified statistic that each port sends or receives.

Operation Path

Open in order: "Main Menu > Port Config > Port statistics > Detail port stats".

Interface Description

Detail port stats interface as follows:


Port statistics >
Port summary statistics
Port detailed statistics
Refresh
Port
fe1/1
Clear
Number of received message 0
Number of transimitted message 0
Number of received bytes 0
Number of transimitted bytes 0
Received unicast message 0
Transimitted unicast message 0
Received multicast message 0
Transimitted multicast message 0
Received broadcast message 0
Transmitted broadcast message 0
Received flow control frame 0
Transmitted flow control frame 0
Message up to 64 Byte 0
65-127 Byte message 0
128-255 Byte message 0
256-511 Byte message 0
512-1023 Byte message 0
Message more than 1024 Byte 0

5 Layer 2 Configuration

5.1 VLAN Configuration

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

VLAN advantages mainly include:

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

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

5.1.1 PVlan Configuration

Function Description

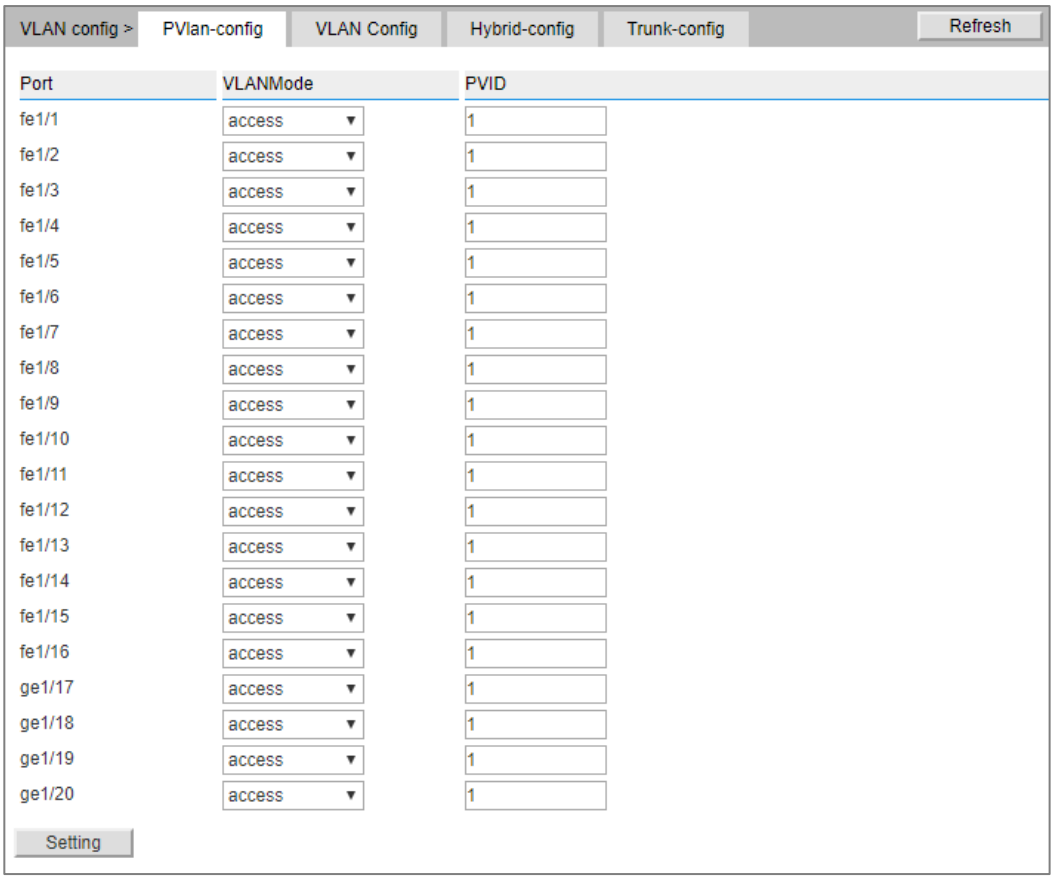
On the "PVlan-config" page, user can configure the port VLAN mode (access, trunk and hybrid), and the VLAN ID: PVID of the port.

Operation Path

Open in order: "Main Menu > Layer 2 Config > VLAN Config > PVlan-config".

Interface Description

PVlan configuration interface as follows:



The main element configuration description of PVlan configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
VLAN Mode	There are three port link types that the switch supports: • Access: Port can only belong to 1 VLAN, which is generally used to connect user device. All default ports belong to access port. • Trunk: Ports can belong to multiple VLAN, receive and send multiple VLAN messages, generally used in the connection between network devices. • Hybrid: port can belong to multiple VLANs. Hybrid port

Interface Element	Description
	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.
PVID	Port-base Vlan ID is the ID number of the port VLAN, which is relative to the VLAN TAG mark when the port receives and sends data frame.

5.1.2 VLAN Configuration

Function Description

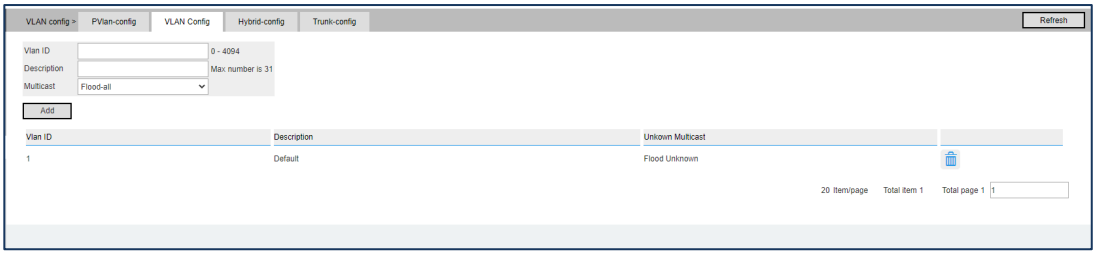
On the "Vlan-config" page, user can configure the VLAN ID description.

Operation Path

Open in order: "Main Menu > Layer 2 Config > VLAN Config > Vlan-config".

Interface Description

Vlan configuration interface as follows:



The main element configuration description of Vlan configuration interface:

Interface Element	Description
Vlan Id	VLAN ID number, value range is 0-4094.
Description	Vlan ID description, maximum 31 characters.
Multicast	Multicast process method; • Flood-all: Flooding all multicast packets;

Interface Element	Description
	• Flood-unknow: Flooding unknown multicast packets; • drop: drop the multicast packets.

5.1.3 Hybrid Configuration

Function Description

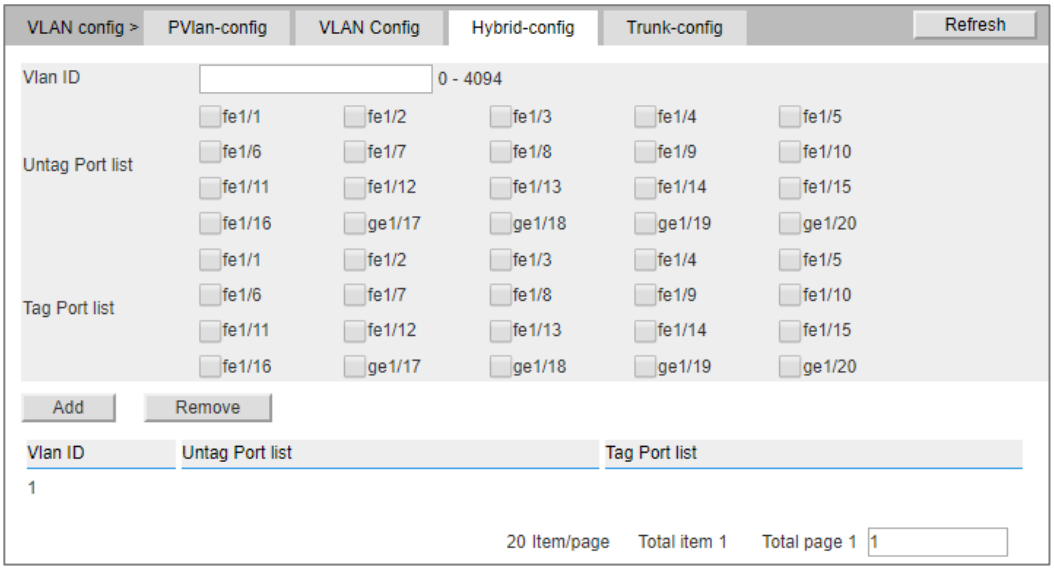
On the "Hybrid Configuration" page, user can configure the port Untag and Tag port list.

Operation Path

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

Interface Description

Hybrid configuration interface as follow:



The main element configuration description of Hybrid configuration interface.

Interface Element	Description
Vlan ID	VLAN ID number, value range is 0-4094.
Untag Port list	Untagged port member to conduct untagged process to sending data frame.
Tag Port list	Tag port member to conduct tagged process to sending data

Interface Element	Description
	frame.

5.1.4 Trunk Configuration

Function Description

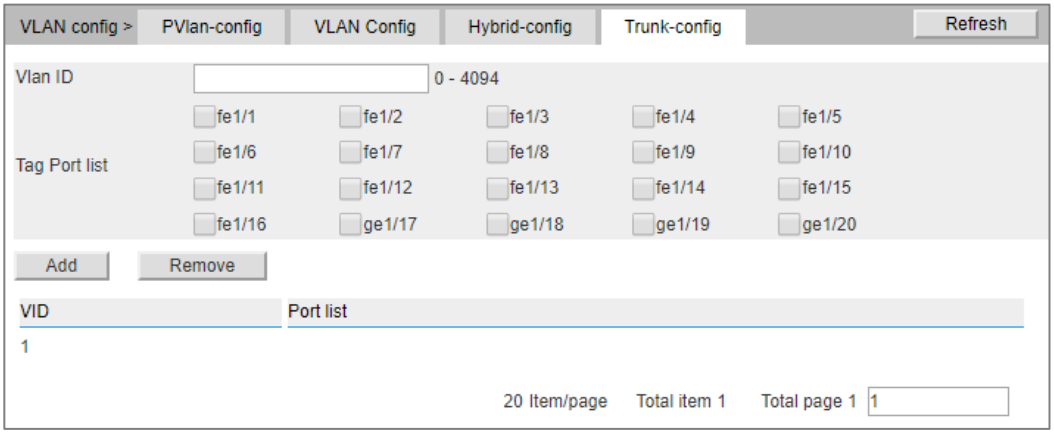
On the "Trunk-config" page, user can configure the port Untagged and Tag port list.

Operation Path

Open in order: "Main Menu > Layer 2 Config > VLAN Config > Trunk-config".

Interface Description

Trunk configuration interface as follows:



The main element configuration description of Trunk configuration interface:

Interface Element	Description
Vlan ID	VLAN ID number, value range is 0-4094.
Tag Port list	Tag port member to conduct tagged process to sending data frame.

Process for Port Receiving Message

Interface type	Process for Receiving Untagged Message	Process for Receiving Tagged Message
Access	Receive this message and	• Receive the message when the

Interface type	Process for Receiving Untagged Message	Process for Receiving Tagged Message
	tag it with default VLAN ID.	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.

Configuration Instance: typical configuration instance of port-based VLAN

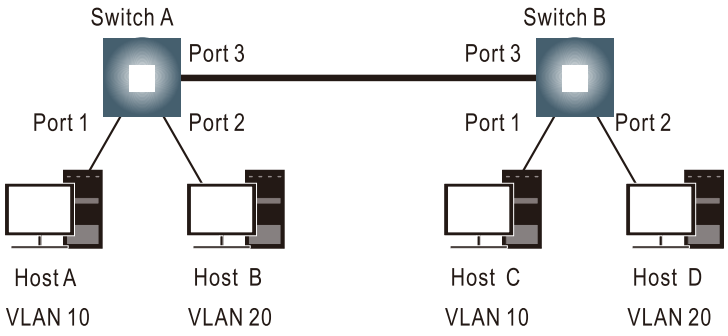
Networking Demand

- Host A and Host B belong to Department A, but they connect to the company network via different devices; Host B and Host D belong to Department B, they

connect to the company network via different devices as well.

- To ensure the safety of communication and prevent broadcast storm, the company can use VLAN technology to isolate the layer 2 flow between departments when it hopes the users with the same business can access each other and the users with different business cannot. Department A uses VLAN 10, and Department B uses VLAN 20.
- In this way, regardless of whether the same device is used to access the corporate network, the hosts within the same VLAN can communicate with each other, that is, host A and host C can communicate with each other, and host B and host D can communicate with each other.

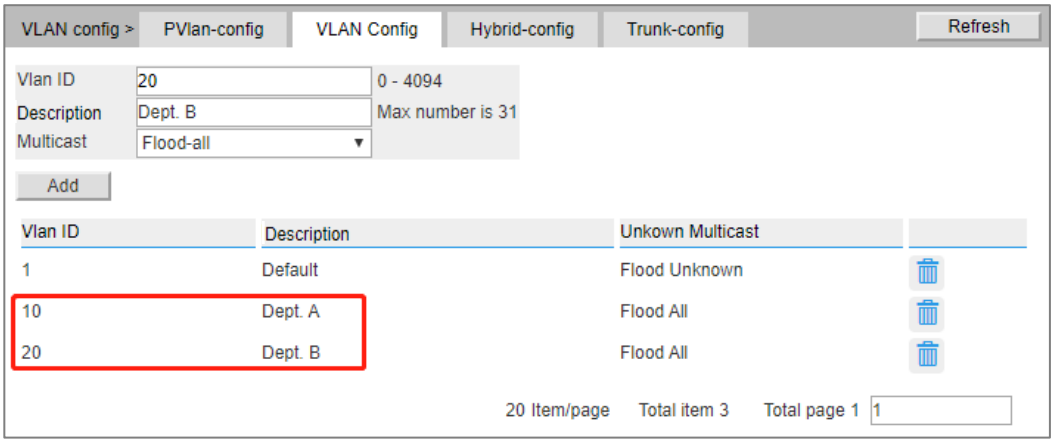
Topological Graph



Operation Steps

Step 1 Configure Switch A

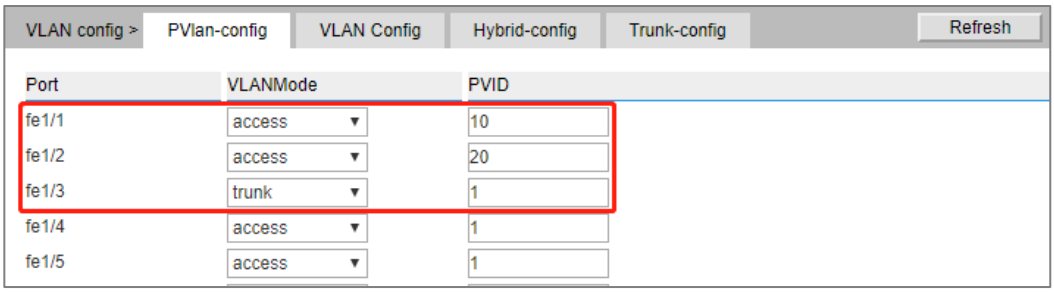
1. Create VLAN 10 and VLAN 20 as shown below:



- Login to the WEB interface of this device
- Enter "Main Menu > Layer 2 Configuration > VLAN Configuration > Vlan Config" interface.

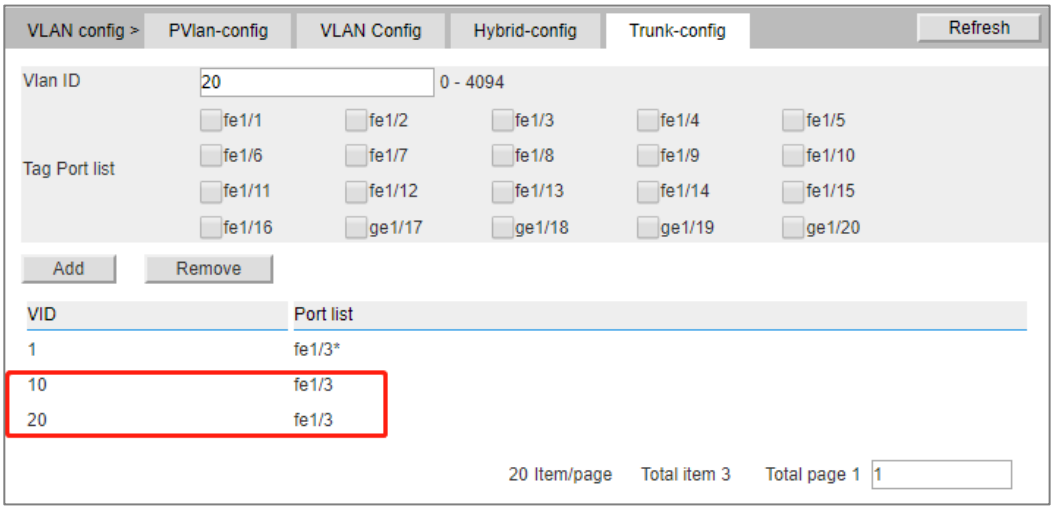
- Enter VLAN ID “10” in "Vlan ID" text box of Department A.
- (Optional) enter name “Dept. A” in the textbox of “Description”.
- (Optional) select “Flood-unknown” in the drop-down list of “Multicast”.
- Click “Add/Edit” button.
- Enter VLAN ID “20” in "Vlan ID" text box of Department B.
- (Optional) enter name “Dept. B” in the textbox of “Description”.
- (Optional) select “Flood-unknown” in the drop-down list of “Multicast”.
- Click “Add/Edit” button.
- End.

2. Configure port type and PVID as shown below.



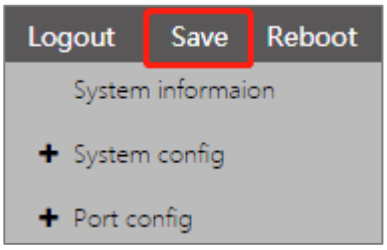
- Enter "Main Menu > Layer 2 Config > VLAN Config > PVlan Config” interface.
- Select mode “access” in the drop-down list of “VLAN Mode” of port fe1/1, enter ID “10” in the “PVID” textbox.
- Select mode “access” in the drop-down list of “VLAN Mode” of port fe1/2, enter ID “20” in the “PVID” textbox.
- Select mode “trunk” in the drop-down list of “VLAN Mode” of port fe1/3.
- Click “Apply” button.
- End.

3. Configure VLAN ID as shown in the picture below.



- Enter "Main Menu > Layer 2 Configuration > VLAN Configuration > trunk Configuration" interface.
- Enter VLAN ID "10" in "Vlan ID" text box.
- Check the port "fe1/3" in the "join port".
- Click "Add" button.
- Enter VLAN ID "20" in "Vlan ID" text box.
- Check the port "fe1/3" in the "join port".
- Click "Add" button.
- End.

4. Save the configuration as shown in the picture below.



- Enter the "Main Menu" interface.
- Click "Save" button.
- End.

Step 2 Configure Switch B, Switch B shares the same configuration with Switch A, so it is not described here.

Step 3 End.

Password Verification

Host A and Host C can access each other via ping, Host B and Host D can access each other via ping, Host A/C and Host B/D cannot access each other via ping.

Check VLAN configuration information via command line:

```
Profinet> enable
Profinet# show vlan
Vid  Status Name
-----------------------------------
1    STATIC Default
     TagPorts:
     Untag   : fe1/3 fe1/4 fe1/5 fe1/6 fe1/7 fe1/8 fe1/9 fe1/10
fe1/11 fe1/12 fe1/13 fe1/14 fe1/15 fe1/16 ge1/17 ge1/18 ge1/19
ge1/20

10   STATIC Dept. A
     TagPorts: fe1/3
     Untag   : fe1/1

20   STATIC Dept. B
     TagPorts: fe1/3
     Untag   : fe1/2
```

5.2 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.

5.2.1 MAC Configuration

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

Function Description

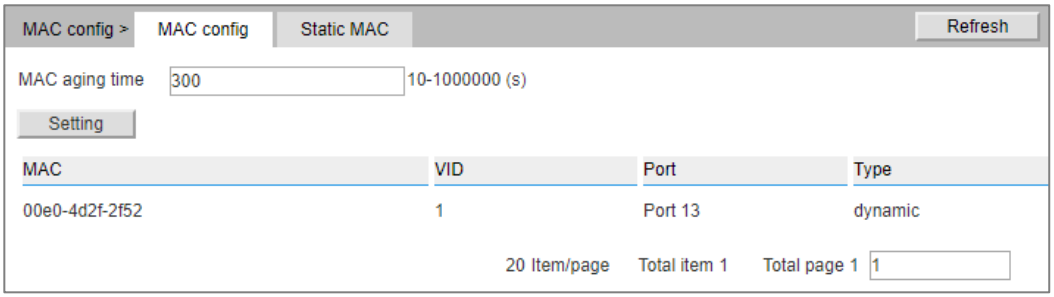
On the "MAC Config" page, user can configure the ageing time of dynamic MAC address and check static and dynamic MAC address information.

Operation Path

Open in order: "Main Menu > Layer 2 Config > MAC Config > MAC Config".

Interface Description

MAC configuration interface is as follows:



The main element configuration description of MAC configuration interface:

Interface Element	Description
MAC Aging Time	MAC address aging-time, unit is second, default value is 300, and range is 10-1000000.
MAC	Access the device MAC address.
VID	VLAN ID number the data MAC address sending belongs to.
Port	Corresponding port number of the MAC address.
Type	MAC address type, dynamic MAC and static MAC address,

Interface Element	Description
	display as follows: • Dynamic; • Static.

5.2.2 Static MAC

Function Description

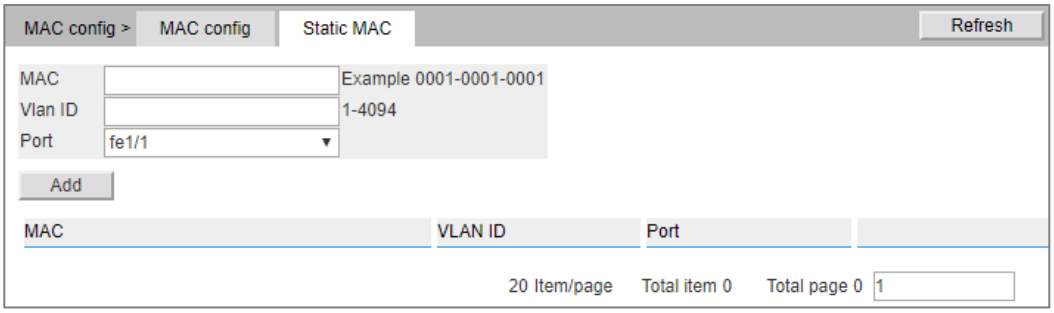
On the "Static Mac" page, user can manually configure the static MAC address and bind the source MAC address without aging.

Operation Path

Open in order: "Main Menu > Layer 2 Config > MAC Config > Static Mac".

Interface Description

Static MAC interface as follows:



The main element configuration description of static MAC interface:

Interface Element	Description
MAC	Fill in the MAC address that needs to bind the interface, such as 0001-0001-0001.
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.
Port	Select the binding port number via the drop-down arrow.

Note

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

5.3 Spanning-tree Configuration

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

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

Spanning-tree protocol has two main functions:

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

5.3.1 Bridge Settings

Function Description

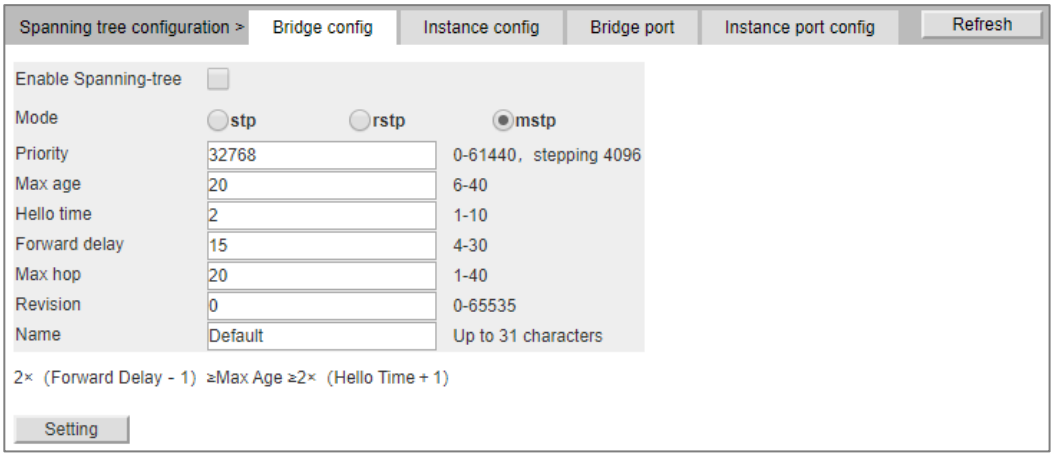
On the "Bridge Settings" page, user can configure relative parameters of spanning-tree.

Operation Path

Open in order: "Main Menu > Layer 2 Config > Spanning-tree Config > Bridge Settings".

Interface Description

Bridge configuration interface as follows:



The main element configuration description of bridge settings interface:

Interface Element	Description
Enable Spanning-tree	Enable Spanning-tree.
Mode	Three modes for spanning-tree protocol choice: • STP: Spanning-tree; • RSTP: Rapid spanning tree; • MSTP: Multiple spanning-trees.
Priority	Bridge priority level, value range is 0-61440. Note: Smaller the priority level value is, higher the priority level is.
Max age	The maximum lifetime of the message in the device, range is 6-40. It's used to determine whether the configuration message times out.
Hello time	Message sending cycle, value range is 1-10. Note: The spanning tree protocol sends configuration information every Hello time to check whether the link is faulty.
Forward delay	Port state transition delay, value range is 4-30.
Max hop	The maximum hop in MST region, 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.
Revision	MSTP revision level, 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.
Name	MST domain name, up to 31 characters.

5.3.2 Instance Configuration

Function Description

On the "Instance Configuration" page, user can configure instance-to-VLAN mapping.

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

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

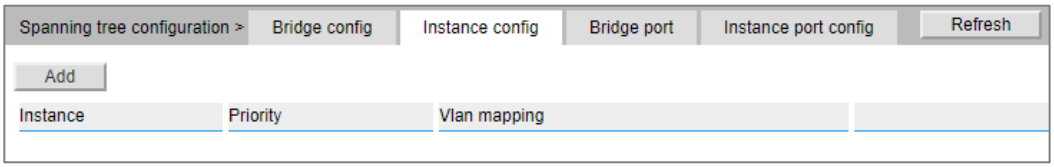
VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI.

Operation Path

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

Interface Description

Instance configuration interface as follows:



The main element configuration description of instance configuration interface:

Interface Element	Description
Instance	Multiple Spanning-tree instance ID number.
Priority	Device priority level, value range is 0-61440, default to 32769, step is 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 mapping	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

Interface Element	Description
	describe the mapping relation between VLAN and MSTI. MSTP achieves load balancing based on the VLAN mapping table.

5.3.3 Bridge Ports

Function Description

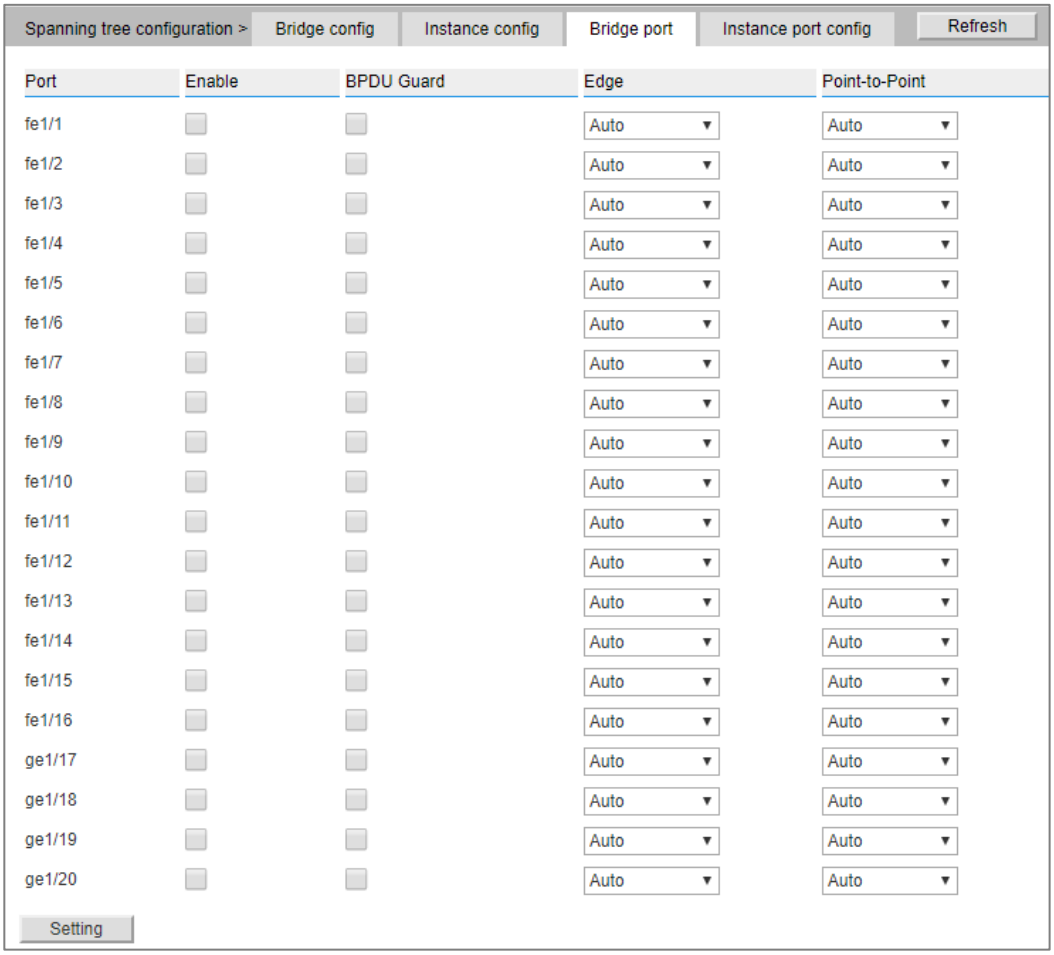
On the "Bridge Port" page, user can enable port to participate in spanning-tree and configure port type, link type and BPDU protection function.

Operation Path

Open in order: "Main Menu > Layer 2 Config > Spanning-tree > Bridge Ports".

Interface Description

Bridge ports interface as follows:



The main element configuration description of bridge ports interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Enable	Enable checkbox to participate in spanning-tree.
BPDU Guard	BPDU (Bridge Protocol Data Unit) protection function.
Edge	Configure port type: • Auto: Automatic system detection; • Force True: Edge port; • Force False: No edge port.
Point-to-Point	Port link type: • Auto: Automatic system detection; • Force True: Point-to-point link; • Force False: Non point-to-point link.

5.3.4 Instance Port Configuration

Function Description

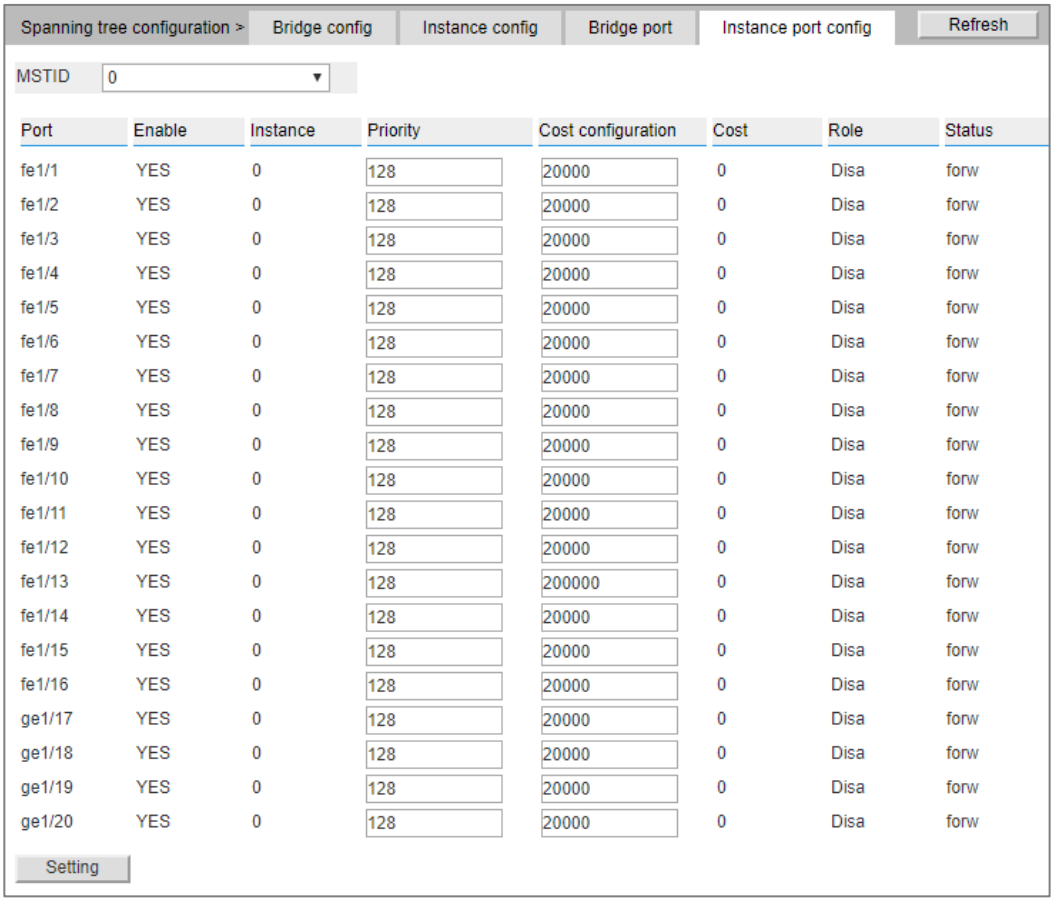
On the "Inst Port Config" page, user can configure port priority level and cost.

Operation Path

Open in order: "Main Menu > Layer 2 Config > Spanning-tree > Inst Port Config".

Interface Description

Instance port configuration interface as follows:



The main element configuration description of instance port configuration interface:

Interface Element	Description
MSTID	Choose multiple Spanning-tree ID number.
Port	The corresponding port name of the device Ethernet port.
Enable	Port enable status: • YES: enable, participate in spanning-tree; • NO: not enabled, not participate in spanning-tree.
Instance	Instance ID number port belongs to.
Priority	Port priority 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.
Cost configuration	The path cost from network bridge to root bridge, which would affect the selection of the path
Cost	Path cost from current port to root bridge.
Role	Port role. • unkn: Unknown; • root: Root port;

Interface Element	Description
	• desg: Designated port; • altn: Alternate port; • back: Backup port; • disa: Disable port.
Status	Port status in spanning-tree: • Disable: Port close status; • Blocking: Blocked state; • Listening: Monitoring state. • Learning: Learning state; • Forwarding: Forwarding state;

5.4 IGMP-snooping

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

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

5.4.1 IGMP Snooping

Function Description

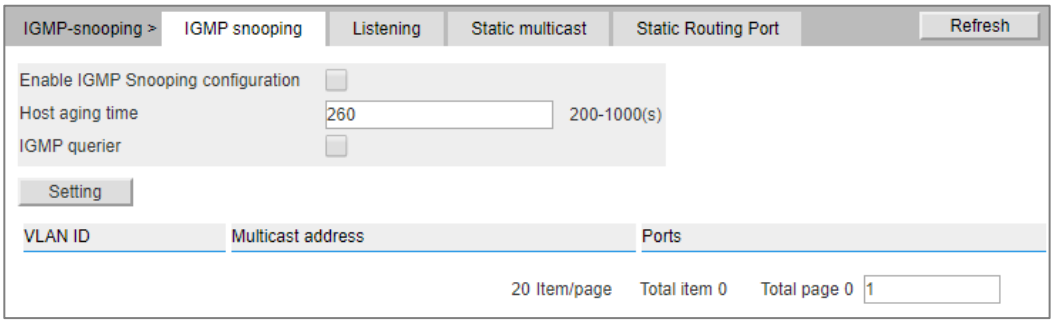
On the "IGMP-snooping" page, users can enable/disable IGMP and configure the host aging time.

Operation Path

Open in order: "Main Menu > Layer 2 Configuration > IGMP-snooping > IGMP-Snooping".

Interface Description

IGMP Snooping interface as below:



The main element configuration description of IGMP Snooping interface:

Interface Element	Description
Enable IGMP-snooping	Enable IGMP-snooping configuration checkbox.
Host aging time	Host aging time, value range is 200-1000s.
IGMP querier	Enable IGMP Querier, the device can join in IGMP Querier election. It would send query message and receive report message of the member to maintain the relationship of multicast group member.
VLAN ID	Port number VLAN ID number.
Multicast address	Multicast IP address.
Ports	The corresponding port name of the device Ethernet port.

5.4.2 IGMP Monitoring -VLAN

Function Description

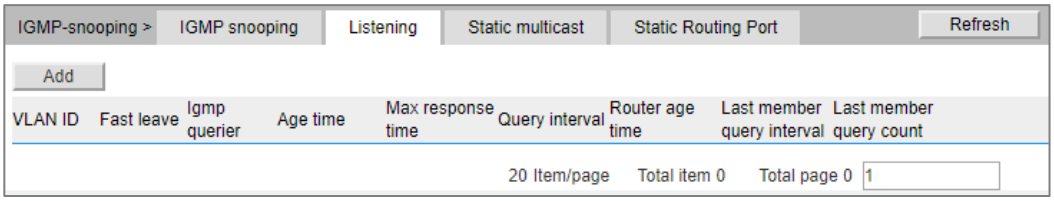
On the page of "IGMP monitoring -VLAN", you can configure the basic functions of VLAN-based IGMP Snooping, and the device can establish and maintain the layer 2 multicast forwarding table to realize the on-demand distribution of multicast data messages in the data link layer.

Operation Path

Open in order: "Main Menu > Layer 2 Config > IGMP-snooping Config > Listening".

Interface Description

IGMP-snooping VLAN configuration interface as follows:



The main element configuration description of IGMP-snooping-VLAN configuration interface:

Interface Element	Note (Click "Add" to add snooping entry)
VLAN ID	The VLAN ID monitored by IGMP, with a value of 1-4094.
Fast Leave	Fast Leave allows the member ports in VLAN to leave the multicast group quickly.
Igmp Querier	IGMP Snooping query function of VLAN.
Age time	Aging time of dynamic member ports in VLAN, in integer form, ranging from 1 to 255, and the unit is seconds.
MAX response time	The maximum response time of IGMP universal group query message in VLAN, an integer ranging from 1 to 25 in seconds. The default value is 10s.
Query interval	IGMP universal group query message sending time interval, in integer form, ranging from 2 to 300, and the unit is seconds.
Router age time	Dynamic router port aging time in VLAN, in integer form,

Interface Element	Note (Click "Add" to add snooping entry)
	ranging from 2 to 300, and the unit is seconds.
Last member query interval	The last member query time interval in VLAN, that is, the sending time interval of IGMP specific group query message, is in integer form, with the value range of 1-5 and the unit of seconds.
Last member query count	IGMP robustness coefficient, that is, the number of times Query messages are sent in integer form, and the value range is 1-255.

5.4.3 Static Multicast

Function Description

On the "Static multicast" page, user can add or delete static multicast.

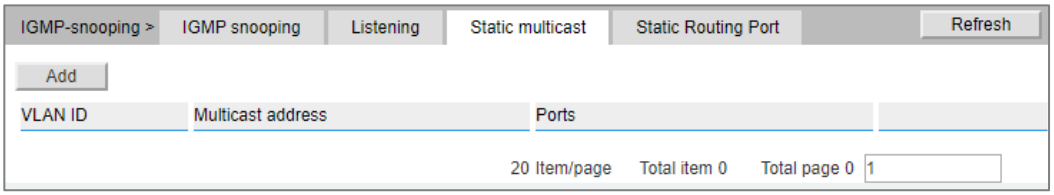
Main function of static multicast: Add certain ports to a multicast group; these ports can receive data when data is sent to this multicast address.

Operation Path

Open in order: "Main Menu > Layer 2 Configuration > IGMP-snooping > Static Multicast".

Interface Description

Static multicast interface as follows:



The main element configuration description of static multicast interface:

Interface Element	Description
VLAN ID	VLAN ID number, value range is 1-4094.
Multicast address	Multicast IP address information, such as: 225.1.2.3.
Ports	The display device ports form multicast group.

Interface Element	Description
Add	Click "Add" button to set Vlan ID, multicast address, port list, etc.

5.4.4 Static Routing Port

Function Description

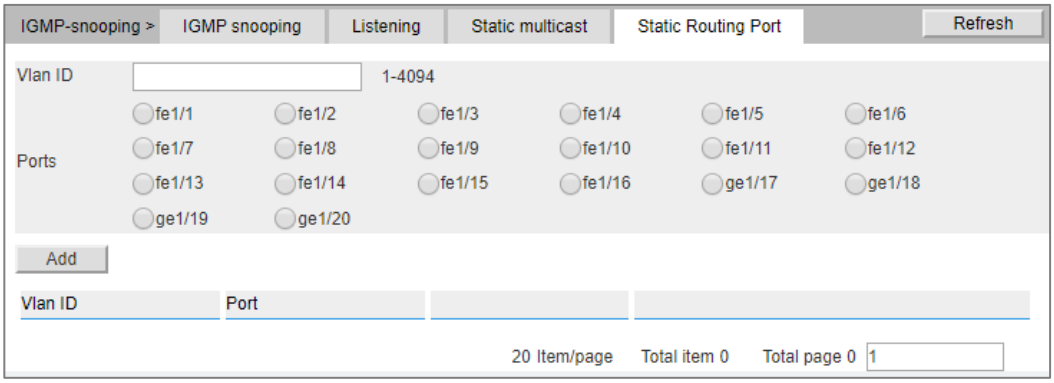
On the "Static Routing Port" page, user can configure the port of multicast router.

Operation Path

Open in order: "Main Menu > Layer 2 Config > IGMP Snooping > Static Routing Port".

Interface Description

The static routing port interface as follows:



The main elements configuration description of static routing port configuration interface:

Interface Element	Description
VLAN ID	VLAN ID number, value range is 1-4094.
Ports	Check the checkbox of port list, select device port as the static router port that connects router.

5.5 MRP Configuration

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

5.5.1 Global Configuration

Function Description

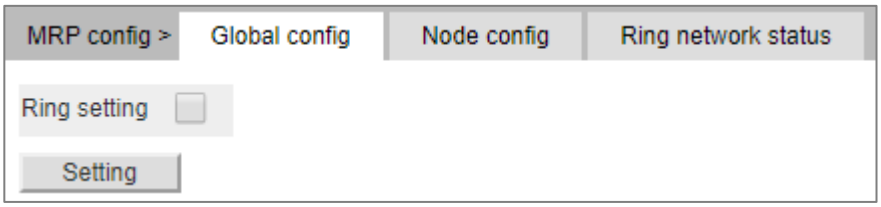
On the "Global Configuration" page, user can enable the MRP media redundancy ring network.

Operation Path

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

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Ring setting	MRP ring network enable check box.

5.5.2 Node Configuration

Function Description

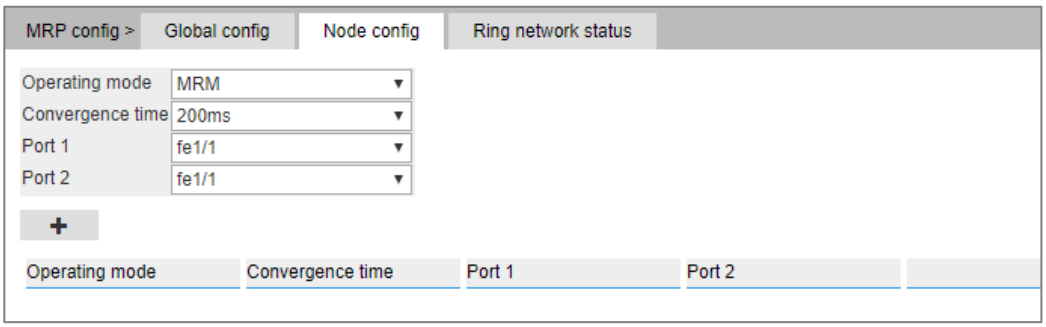
On the "Node Configuration" page, user can configure MRP ring network parameters.

Operation Path

Open in order: "Layer 2 Config > MRP Config > Node Config".

Interface Description

Node configuration interface as follows:



The main element configuration description of node configuration interface:

Interface Element	Description
Operating mode	The working modes of the device are as follows: • MRM: Media Redundancy Manager; • MRC: Media Redundancy Client.
Convergence time	When the MRP ring network is disconnected, the ring network reconfiguration time can be selected as follows: • 200ms; • 500ms.
Port1	MRP ring port1.
Port2	MRP ring port2.

5.5.3 Ring Network State

Function Description

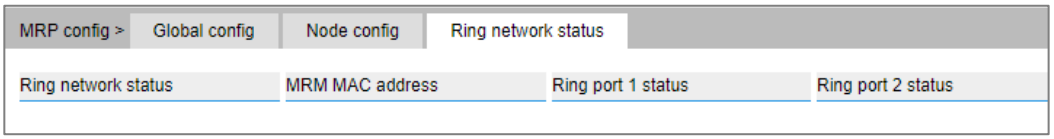
On the “Ring Network Status” page, users can view the MRP ring network status.

Operation Path

Open in order: "Layer 2 Configuration > MRP Configuration > Ring Network Status".

Interface Description

Ring network state interface as follow:



The main element configuration description of ring network state interface:

Interface Element	Description
Ring Network Status	MRP ring network status can be shown as follows: • Enable; • Disable.
MRM MAC Address	The MAC address of MRM device in this ring network.
Ring port1 status	Ring network status of device ring network port 1, the display statuses are as follows: • Forward: the port is forwarding; • Blocking: the port is blocking.
Ring port2 status	Ring network status of device ring network port 2, the display statuses are as follows: • Forward: the port is forwarding; • Blocking: the port is blocking.

5.6 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.

5.6.1 Timer

Function Description

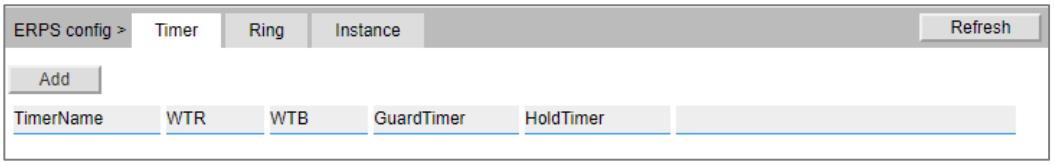
On the "Timer" page, user could configure the timer.

Operation Path

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

Interface Description

Timer configuration interface is as follows:



Main elements configuration description of timer interface.

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

5.6.2 Loop

Function Description

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

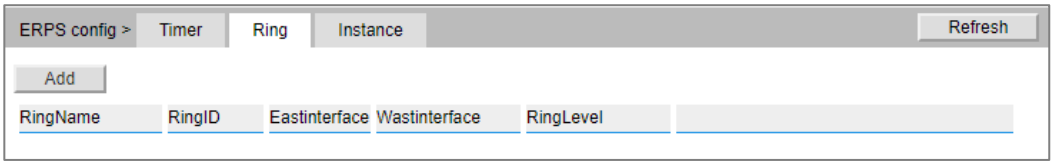
An Ethernet network topology connected in ring is called a ERPS Ring. It could be divided into main ring and subring. Each device in ERPS ring is called a node. The main node is in charge of blocking and opening ports on this node, preventing loops from forming.

Operation Path

Open in order: "Main Menu > Layer 2 Config >ERPS Config > Ring".

Interface Description

Ring interface as follows:



The main element configuration description of ring configuration interface.

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

5.6.3 Instance

Function Description

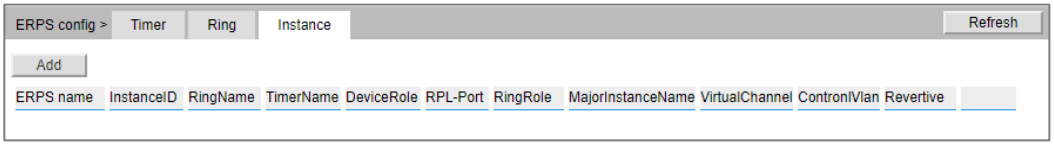
On the "Instance" page, user could configure instance.

Operation Path

Open in order: "Main Menu > Layer 2 Config >ERPS Config > Instance”.

Interface Description

Instance configuration interface as follows:



The main element configuration description of instance configuration interface:

Interface Element	Description
ERPS Name	The default name of ERPS is erp, which is up to 32 bytes
Instance ID	The ID of instance, its value range is 0-63
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

Interface Element	Description
	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
Major Instance Name	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 Channel	After enable virtual channel, the subring protocol packet could transmit across the primary ring; otherwise, the subring protocol packet can only transmit in the ring. Options: • enable • disable
Manage VLAN	The VLAN channel of protocol packet, its value range is 1-4094
Revertive	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.

5.7 Ring Configuration

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

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

fault alarm will be activated and the Ring redundant mechanism enables the backup link to quickly recover the network communication.

5.7.1 Global Configuration

Function Description

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

Operation Path

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

Interface Description

Global configuration interface is as follows:

The main element configuration description of global configuration interface:

Interface Element	Description
Ring Configuration	Ring setting checkbox, enable Ring network function after checking.

5.7.2 Node Configuration

Function Description

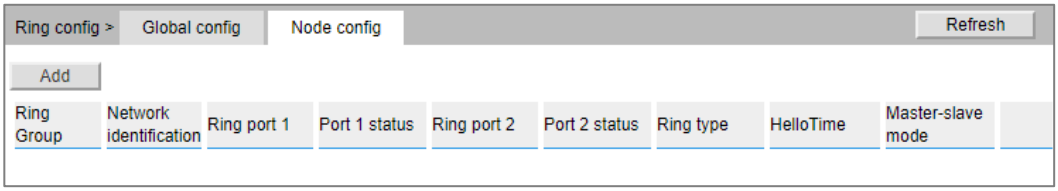
On the "Node Configuration" page, user can enable/disable the ring network.

Operation Path

Open in order: "Main Menu > Layer 2 Config > Ring Config > Node Config".

Interface Description

Node configuration interface as follows:



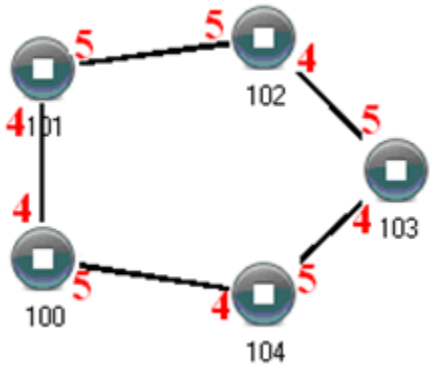
The main element configuration description of node configuration interface:

Interface Element	Description
Ring Group	Support ring group 1-4, it can create 4 ring networks at the same time.
Network Identifivation	When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID.
Ring Port 1	The network port 1 on the switch device used to form a ring. Note: When the ring network type is "Couple", it displays "coupling port". Coupling port is the port that connects different network identities.
Port1 Status	Display the current state of ring port1 in the ring group.
Ring Port 2	The network port 2 on the switch used to form a ring. Note: When the ring network type is "Couple", it displays "console port". Console port is the port in the chain where two rings intersect.
Port2 Status	Display the current state of ring port2 in the ring group.
Ring Type	According to the requirement in the scene, user can choose different ring type. • Single: single ring, using a continuous ring to connect all device together. • Couple: couple ring is a redundant structure used for connecting two independent networks. • Chain: chain can enhance user's flexibility in constructing all types of redundant network topology via an advanced software technology. • Dual-homing: two adjacent rings share one switch. User could put one switch in two different networks or two different switching equipments in one network.
Hello Time	Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends information packet to adjacent device for confirming the connection is normal or not.
Master-slave mode	Master-slave mode, options as follows: • Master: the master device of the ring network;

Interface Element	Description
	• Slave: the slave device of the ring network; Note: Single ring has master/slave device option. One-Master Multi-Slave mode is recommended in one single ring. When the device is set as master device and one end of it is backup link, it can enable backup link to ensure the normal operation of the network when failure occurs in ring network.
Add	Click "Add" button to add related node configuration of ring network.

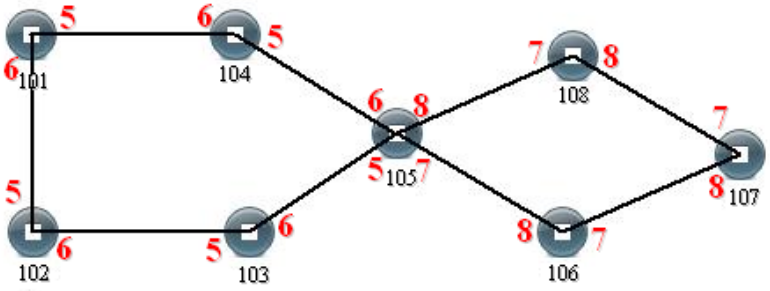
Single Ring Configuration

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



Double Ring Configuration

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



Configuration Method:

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

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

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

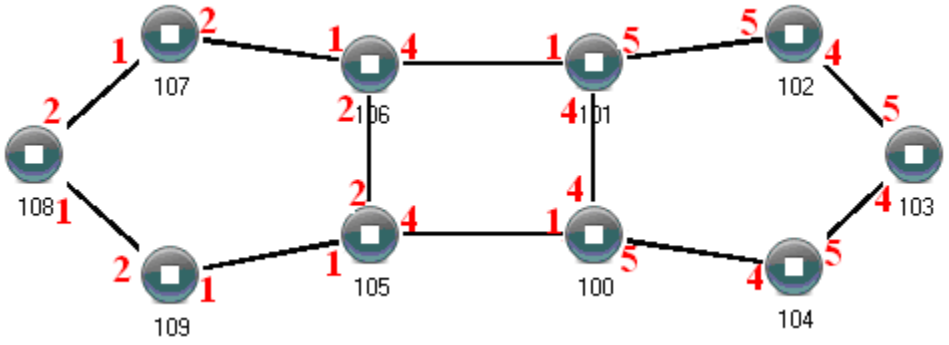
Step 4 Adopt network cable to connect the ring group 2;

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

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

Coupling Ring Configuration

Coupling ring basic framework as the picture below:



Operation method:

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

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

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

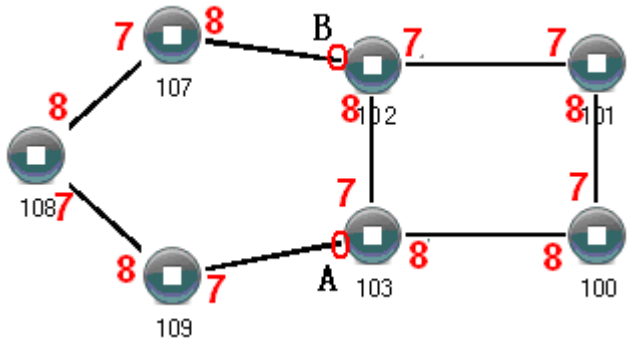
Step 4 Set the ring port of No. 107, 108 and 109 device ring group 1 to port 1 and port 2, network identification to 1, ring type to Single; Set the ring port of No. 102, 103 and 104 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single.

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

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

Chain Configuration

Chain basic framework as the picture below:



Operation method:

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

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

Step 3 Adopt network cable to connect the port 7 and port 8 of three devices No. 107-109, adopt network cable to connect the port 7 and port 8 of four devices No. 100-103 to

the single ring in turn, Then adopt network cable to connect port 7 of No. 107 device and port 7 of No. 109 device to normal ports of No. 102 and 103 device, chain combination is complete.

Note

1. 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;
2. Network identification in the same single ring must be consistent, otherwise it cannot form a normal ring or normal communicate;
3. Network identification in different ring must be different;
4. When forming double ring and other complex ring, user should notice whether the network identification in the same single ring is consistent, and network identification in different single ring is different.

5.8 Loop Detection

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

5.8.1 Global Configuration

Function Description

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

Operation Path

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

Interface Description

Global configuration interface is as follows:

The main element configuration description of global configuration interface:

Interface Element	Description
Global Configuration	**Global configuration bar.**
Enable	The checkbox of enabling loop detection. User can implement relevant configuration on the page of loop detection port configuration after checking the box

5.8.2 Port Configuration

Function Description

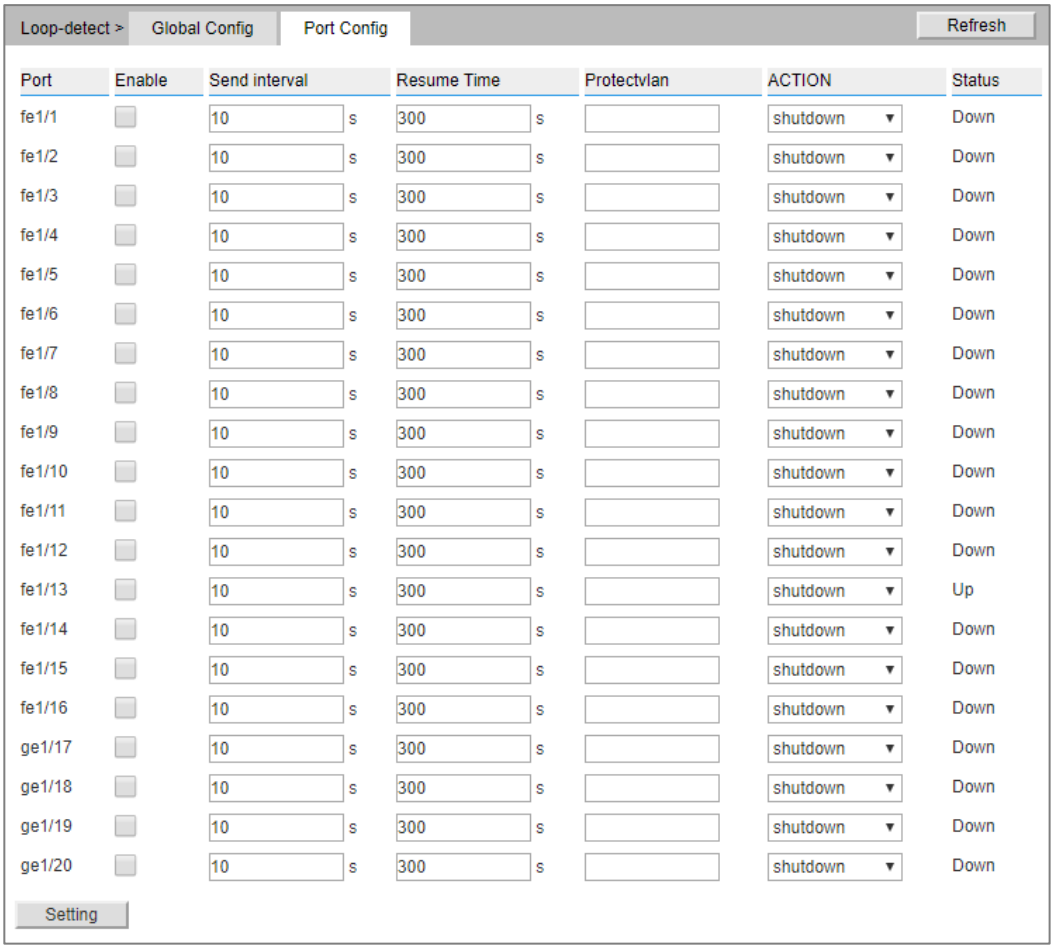
On the "Port config" page, user can implement relevant configuration of port loop detection.

Operation Path

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

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Port Configuration	**Port configuration bar**
Port	The corresponding port number of Ethernet port
Enable	Check the box to enable the loop detection configuration of this port
Send interval	The interval time of loop detection data packet sending, value range: 10-300, its unit is second.
Resume time	The resume time after the action of detecting loop, value range: 10-300, its unit is second.
Protect VLAN	The VLAN ID of loop protection. It is 1 by default. The value range: 1-4094, the number of VLAN ID is ≤5
Action	The selected action after detecting a loop, options are: • Log: log • Shutdown: the port is closed
Status	The status of this port, displayed items are: • Down: the port is physically disconnected

Interface Element	Description
	• Up: the port is connected • Shutdown: the port is closed • No Shutdown: the port is not closed

6 Network Security

6.1 Access Control

Function Description

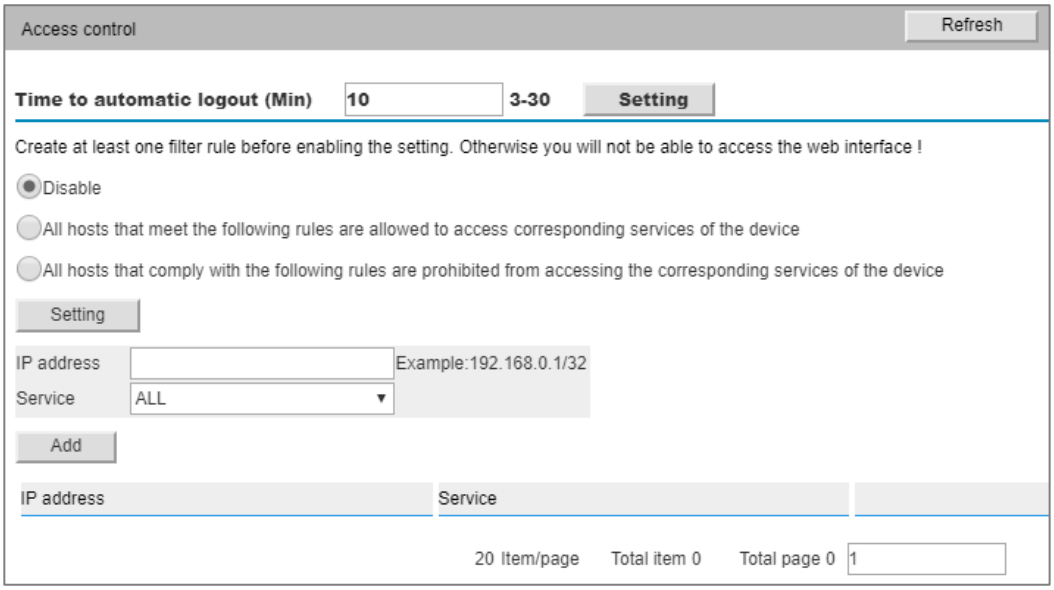
On the "Access Control" page, user can configure access rules and filtering rule.

Operation Path

Open in order: "Main Menu > Network security > Access Control".

Interface Description

Access control interface as follows:



The main element configuration description of access control interface:

Interface Element	Description

Interface Element	Description
Time to automatic logout (min)	Set the time of automatic logout, unit: minutes, default value: 10, value range: 3-30.
Filtering rule	Set filtering rule, default to disable, that is disable access filtering function. Options as follows: • Disable; • All hosts that meet the following rules are allowed to access corresponding service of the device; • All hosts that comply with the following rules are prohibited from accessing corresponding service of the device.
Access rules	**Access rules setting column.**
IP Address	Enable/disable device to access the switch IP address.
Service	Methods of enabling/disabling device to access the switch. Options as follows: • ALL: support HTTP, TELNET, SSH and SNMP access management; • HTTP: Support WEB interface access; • TELNET: Support Telnet client command line access; • SSH: Support SSH client access; • SNMP: Support SNMP network management


Notice

Please first add the rules, and then set the access rules, otherwise it may cause the current web can't be accessed.

6.2 802.1X Configuration

IEEE 802.1X protocol is a port-based network access control protocol, that is, user devices are authenticated on the ports of LAN access devices so that user devices can control access to network resources.

IEEE 802.1x adopts the logic functions of "controllable port" and "uncontrollable port" in the authentication architecture, thus realizing the separation of business and authentication. After the user passes the authentication, the business flow and the authentication flow realize the separation. It has no special request to the subsequent packet processing, the service can be very flexible, and has a great advantage in business especially in carrying out broadband multicast , all services are not restricted by the authentication method.

802.1X structure mainly consists of three parts:

- Supplicant: user or client that wants to get the authentication;
- authentication server: typical example is RADIUS server;
- Authentication system Authenticator: access devices, such as wireless access points, switches, etc

6.2.1 Global Configuration

Function Description

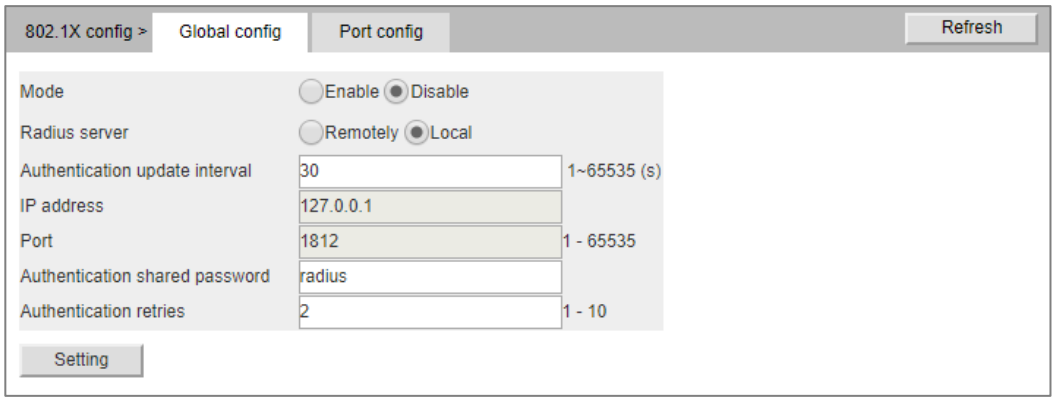
On the "Global Config" page, user can configure 802.1x authentication and Radius server parameters.

Operation Path

Open in order: "Main Menu > Network Security > 802.1X Configuration > Global Configuration".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Mode	IEEE802.1X authentication status settings: • Enable; • Disable.
Radius Server	Local internal Radius server and external Radius server configuration: • Local: built-in Radius server, if choosing internal Radius server, the applicant will only use the username and password of internal Radius database. • Remote: fill in the IP address and port number of the authentication server if using external Radius server.
Authentication upgrade interval	The range of authentication upgrade interval is 1~65535, unit: second. The reauthentication interval of 802.1x used for strengthening the security of authentication.
IP address	IP address of Radius server
Port	The port number of the Radius server. The default is 1812, value range is 1-65535.
Authentication Shared Password	The shared password character string used for device accessing authentication server.
Authentication Retries	The number of retries allowed for authentication ranges from 1 to 10.

Global Configuration Steps:

Step 1 Select “enable” or “disable” 802.1x authentication;

Step 2 Select Radius server “remote” or “local”, fill in authentication upgrade interval;

Step 3 Fill in the IP address, port, shared password for authentication and the number of authentication retries of Radius server;

Step 4 Click “Apply”.

Step 5 End.

6.2.2 Port Configuration

Function Description

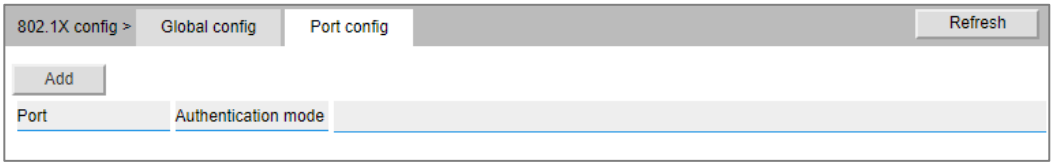
On the "Port Config" page, user can enable 802.1X Port Authentication.

Operation Path

Open in order: "Main Menu > Network Security > 802.1X Configuration > Port Configuration".

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Port	Drop down the port list and select the port name corresponding to the Ethernet port of the device as the authentication port.
Authentication mode	802.1x port authentication mode: • Automatic: normal authentication status, if the host passes authentication, the port would be in forced authentication passing status, if it failed, it would be in forced authentication non-passing status; • Forced authentication passing: Force the interface to become the authenticated state directly; • Forced authentication non-passing: Force the interface to become the unauthenticated state directly.
Add	Click "Add" button to add the related configuration of the port.

7 Advanced Configuration

7.1 QOS Configuration

Quality of Service (QoS) is the service quality. As for network business, service quality includes transmission bandwidth, transfer delay, data packet loss rate and so on. In network, user can improve the service quality by ensuring the transmission bandwidth, reducing transfer delay, data packet loss rate, delay jitter and other measures.

Network resources are always limited, as long as there exists the case of snatching network resources, there will be service quality requirements. Quality of service is relative to the network business, while ensuring the service quality of a certain type of business; it may damage the service quality of other businesses. For example, in the case of total network bandwidth is fixed, if a type of business occupies more bandwidth, other businesses will be able to use less bandwidth, which may influence the usage of other businesses. Therefore, network managers need to make rational planning and distribution of network resources according to the characteristics of various businesses, so that network resources can be efficiently utilized.

QoS function provides 8 internal queues, each queue supports 4 different levels traffic, High-priority data packets stay on the switch for a short period of time, and some latency-sensitive traffic supports lower latency. According to 802.1p priority level tag, IP TOS, the device can classify packets to a certain level.

Function Description

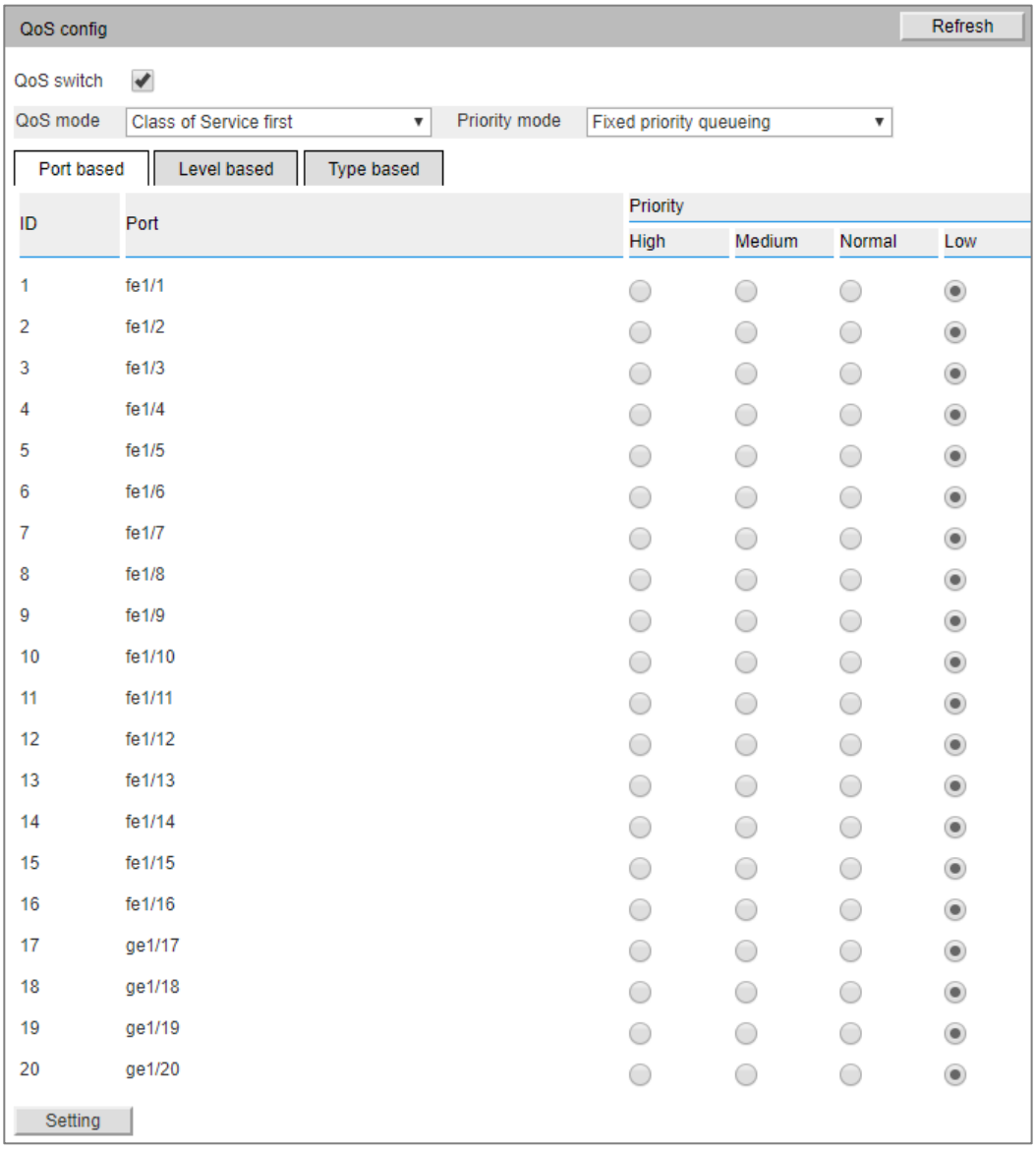
On the “QoS Configuration” page, you can configure QoS mode, priority mode, etc.

Operation Path

Open in order: "Main Menu > Advanced Config > QoS Config".

Interface Description 1: Port-based

Check QoS-Port-based configuration interface as below:



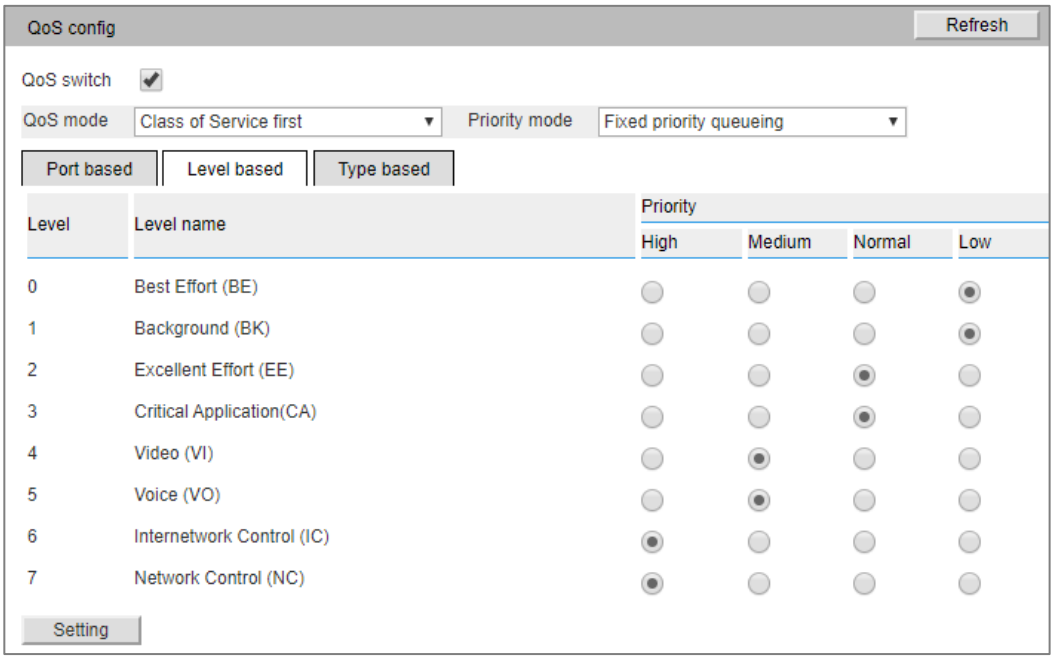
The main element configuration description of QoS-Port-based configuration interface:

Interface Element	Description
QoS switch	Check to enable Qos function
QoS mode	The drop-down box of QoS mode: • Port based only • Class of Service only • Type of Service only

Interface Element	Description
	• Class of Service first: • Type of Service first:
Priority mode	The drop-down box of priority mode: • Fixed priority queue: sends the group of the higher-priority queues strictly according to the priority level from high to low; • 8-4-2-1 weighted fair queueing: Each queue is configured with a weighted value of 12-8-4-2-1, and how many messages are dispatched by each queue can be configured, and the queues are scheduled in turn, thus avoiding the disadvantage that messages in low priority queues may not be served for a long time when fixed priority queues are adopted.
Port-Based	**Port-Based Configuration bar** Note: This function can only be configured when Port based only, Class of Service first or Type of Service first is selected in QoS mode.
ID	Port-based ID number
Port	Ethernet port number of the switch.
Priority	Set the priority level of the port: • High; • Medium; • Normal; • Low.

Interface Description: Level-based

QoS Config-level-based interface is as follows:



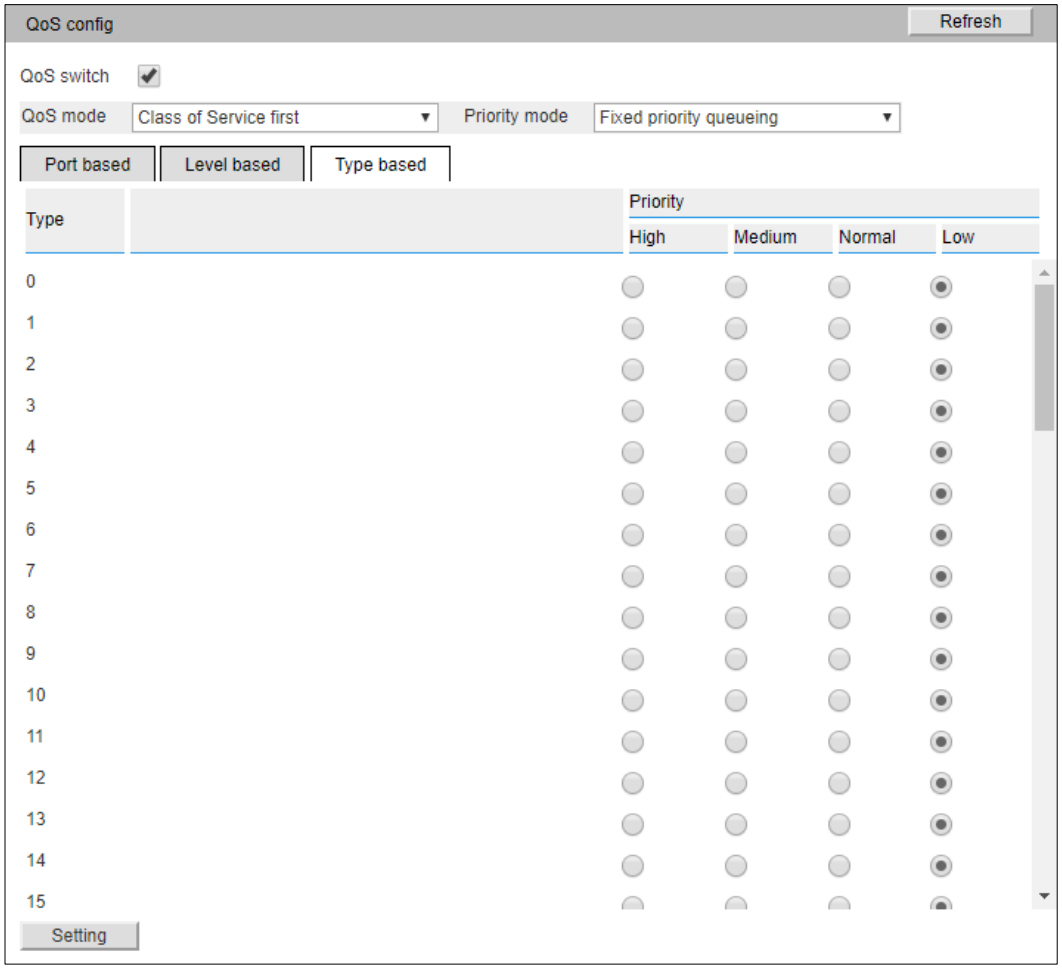
The main element configuration description of QoS Config-class-based interface:

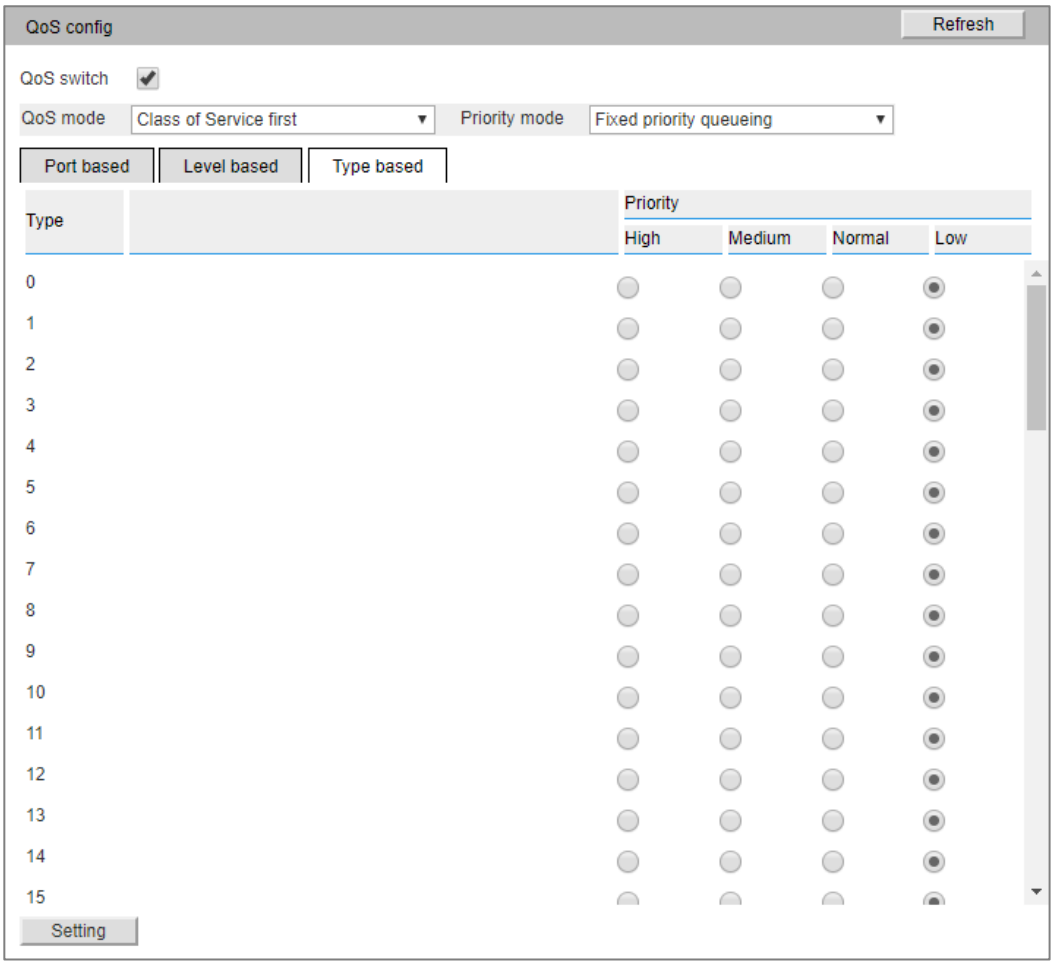
Interface Element	Description
QoS switch	Check to enable Qos function
QoS mode	The drop-down box of QoS mode: • Port based only • Class of Service only • Type of Service only • Class of Service first: • Type of Service first:
Priority mode	The drop-down box of priority mode: • Fixed priority queue: sends the higher-priority queues strictly according to the priority level from high to low. • 8-4-2-1 weighted fair queueing: Each queue is configured with a weighted value of 33-25-17-12-8-4-2-1, and how many messages are dispatched by each queue can be configured, and the queues are scheduled in turn, thus avoiding the disadvantage that messages in low priority queues may not be served for a long time when fixed priority queues are adopted.
Level-based	**Level-based configuration bar** Note: This function can only be configured when Class of Service only, Class of Service first or Type of Service first is selected in QoS

Interface Element	Description
	mode.
Level	Level of service, value range is 0-7.
Level name	Level name corresponding to service class: • Best Effort (BE) • Background (BK) • Excellent Effort (EE) • Critical Application(CA) • Video (VI) • Voice (VO) • Internetwork Control (IC) • Network Control (NC)
Priority	Set the priority of CoS: • High; • Medium: • Normal: • Low.

Interface Description: Type based

QoS Config-class-based configuration interface is as follows:


QoS config
Refresh
QoS switch
QoS mode
Class of Service first
Priority mode
Fixed priority queueing
Port based
Level based
Type based
Type
Priority
High
Medium
Normal
Low
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Setting



The main element configuration description of QoS Config-class-based interface:

Interface Element	Description
QoS switch	Check to enable Qos function
QoS mode	The drop-down box of QoS mode: • Port based only • Class of Service only • Type of Service only • Class of Service first: • Type of Service first:
Priority mode	The drop-down box of priority mode: • Fixed priority queue: sends the higher-priority queues strictly according to the priority level from high to low. • 8-4-2-1 weighted fair queueing: Each queue is configured with a weighted value of 33-25-17-12-8-4-2-1, and how many messages are dispatched by each queue can be configured, and the queues are scheduled in turn, thus avoiding the disadvantage that messages in low priority

Interface Element	Description
	queues may not be served for a long time when fixed priority queues are adopted.
Type-based	**Class-based Configuration** Note: This function can only be configured when Type of Service only, Class of Service first or Type of Service first is selected in QoS mode.
Type	DSCP priority level value is 0-63, 63 is the highest priority level, 0 is the lowest priority level.
Priority	Configure the Priority of DSCP: • High; • Medium: • Normal: • Low.

7.2 LLDP Configuration

LLDP is a layer 2 topology discovery protocol, its basic principle is: Devices in network send the status information message to adjacent device, and each port in the device stores its own information, if there is change in the status of local device, it can also send updated information to the adjacent device directly connected to it. Adjacent devices will store the information in standard SNMP MIB bank. The network management system could inquiry the connection status of current layer 2 from SNMP MIB bank. It should be noted that LLDP is only a remote device status information discovery protocol, which cannot complete the network device configuration, port control and other functions.

Function Description

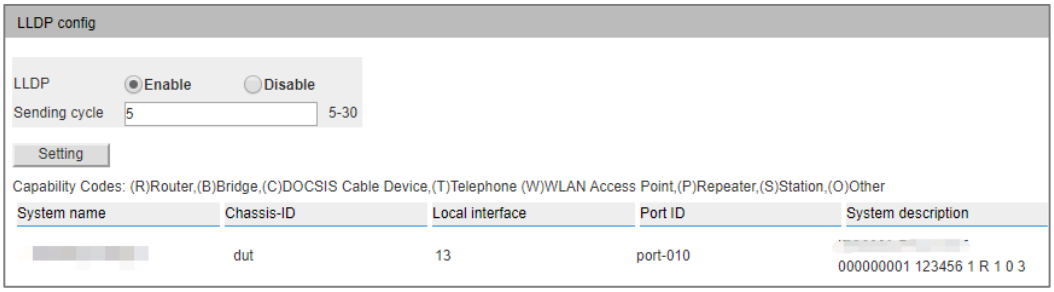
On the "Global Config" page, user can configure LLDP and check neighbor information.

Operation Path

Open in order: "Main Menu > Advanced Config > LLDP Config".

Interface Description

LLDP configuration interface is as follows:



The main element configuration description of LLDP configuration interface:

Interface Element	Description
LLDP	LLDP function status, options as follows: • Enable; • Disable.
Sending cycle	The range of LLDP sending period is 5-30. Note: When no device status changes, the device periodically sends LLDP packets to its adjacent nodes. The interval is called the period for sending LLDP packets.
System name	System name or model of the neighbor device.
Chassis-ID	Bridge MAC address of neighbor device or port.
Local interface	Local port number of local switch connected to adjacent devices.
Port ID	Neighbor device port ID number.
System Description	System property, abbreviated code as below: • R: Router; • B: Bridge; • C: DOCSIS Cable Device; • T: Telephone; • W: WLAN Access Point; • P: Repeater; • S: Station; • O: Other.

7.3 SNMP Configuration

SNMP Introduction

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

SNMP Working Mechanism

SNMP is divided into NMS and Agent:

- Network Management Station (NMS) is the work station that runs client procedure, at present, common network management platforms include Quid View, Sun Net Manager and IBM Net View. Agent is the server software that runs in network device.
- NMS can send Get Request, Get Next Request and Set Request messages to Agent, after receiving these request messages from NMS, Agent will conduct Read or Write operation, generate Response message and return messages to NMS according to the message type. When the device appears abnormal situation or the state changes (such as device resets), Agent will forwardly send Trap message to NMS and report occurred event to NMS.

Any managed resource is represented as an object, called a managed object. MIB (Management

MIB (Management Information Base) is the collection of managed objects. NMS manages the device via MIB. MIB has defined the hierarchical relationship between the nodes and a set of properties of objects, such as objects' name, access privilege and data type, etc. Each Agent has its own MIB. Managed device has its own MIB files; compiling these MIB files in NMS can generate MIB of the device. NMS conducts read/write operation according to access privilege, and achieves Agent management. Relationship of NMS, Agent and MIB as the picture below.

MIB is organized according to a tree structure, consisting of a number of nodes; each node represents a managed object that can be uniquely identified by a string of path-specific numbers starting from the root, this string of OID (Object Identifier) ".

SNMP supports three basic operations:

- Get operation: Manager adopts the operation to inquire a variable value of Agent;
- Set operation: Manager adopts the operation to set a variable value of Agent;
- Trap operation: Agent adopts the operation to send abnormal alarm information to manager.

SNMP Protocol Version

At present, SNMP Agent in the device supports SNMP v1 version, SNMP v2c and SNMP v3 version. SNMP v1, SNMP v2c adopt community name authentication, SNMP message of community name without device authentication will be discarded. SNMP community name is used for defining the relationship of SNMP, NMS and SNMP Agent. Community name plays a role similar to password, and can limit SNMP NMS to access SNMP Agent in device. User can choose and appoint one or more characters relative to community name:

- Define MIB view that community name can access.
- Configure MIB object access privilege of community name as read-write privilege or read-only privilege. Community name with read-only privilege can only inquire the device information; community name with read-write privilege can configure the device.
- Set the basic access control list appointed by community name.

7.3.1 Global Configuration

Function Description

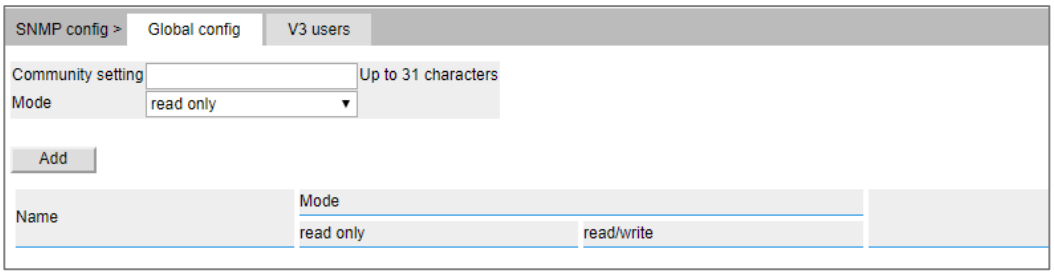
On the "Global Configuration" page, user can add/delete SNMP community. Define MIB view that community name can access, set MIB object access privilege of community name as read-write privilege or read-only privilege.

Operation Path

Open in order: "Main Menu > Advanced Config > SNMP Config > Global Config".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Community settings	SNMP community name definition, support 31 characters input.
Mode	Community mode setting, the options are as follows: • Read-only: Read-only mode community. • Read-write: Read-write mode community.
Name	Display community name.
Read only	Display community read-only mode.
Read/write	Display the community read-write mode.
Add	Click the "Add" button to add the community-related configuration.

7.3.2 V3 User

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

Function Description

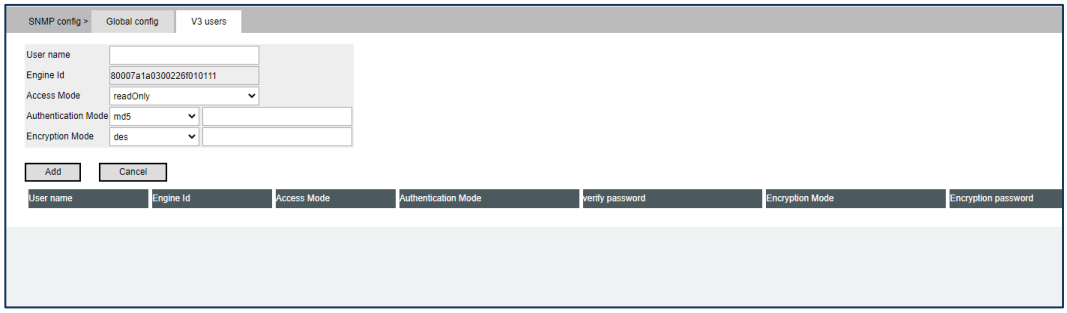
On the "V3 User" page, user can configure SNMP V3 user information.

Operation Path

Open in order: " Main Menu > Advanced Config > SNMP Config > V3 User".

Interface Description

V3 user interface as follows:



The main element configuration description of V3 user interface:

Interface Element	Description
User name	SNMP v3 version user name definition, combination of letters and numbers, and support 48 characters input.
Engine ID	SNMP protocol engine identification. There is a one-to-one correspondence between the engine identification and SNMP entity. It is in charge of SNMP protocol operation, providing service for each type of SNMP applications. Note: The main function of SNMP engine includes: send and receive message, authenticate and encrypt message, control access toward managed object.
ZUGRIFF Mode	Acess mode, options as follows: • ReadOnly: Read-only mode. • ReadWrite: ReadWrite mode.
Authentifizieren Mode	Authentication method and authentication password information, two authentication methods are optional: • Md5: Information abstract algorithm 5; • Sha: Secure hash algorithm.
Verschlüsselung Mode	Corresponding authentication password information in authentication mode

Interface Element	Description
Verschlüsselung Mode	V3 user data encryption algorithm and encryption password information, encryption algorithm options are as follows: • Des: Adopt data encryption algorithm; • Aes: Adopt advanced encryption standard; • None: No encryption.
Add	Click "Add" button to add the related configuration of V3 users.

7.4 RMON Configuration

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

7.4.1 Event

Function Description

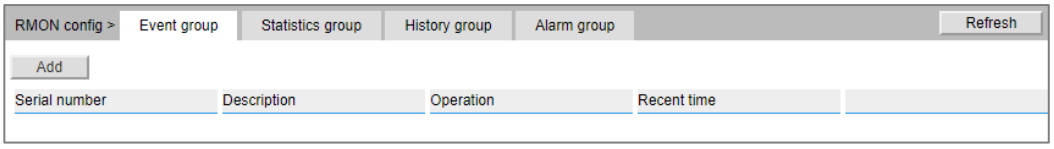
On the "Event" page, user can add, delete or check the configuration information of event.

Operation Path

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

Interface Description

Check event interface as below:



The main element configuration description of event interface:

Interface Element	Description
Serial number	Triggered event serial number when monitoring MIB object exceeds threshold value, the value range is 0-1024. Note: This serial number corresponds to the rising event index and falling event index set in RMON alarm configuration information.
Description	Some description information for describing the event.
Operation	Event dealing method, options as below: • None: No dealing; • log: Record the event in the log table when the event is triggered; • trap: Send Trap information to management station for informing the occurring of event when the event is triggered; • Log, trap: Record the event in the log table and produce a trap information when the event is triggered.
Recent Time	The time when the event occurred.
Add	Click "Add" button to add the related configuration of the event group.

7.4.2 Statistical

Function Description

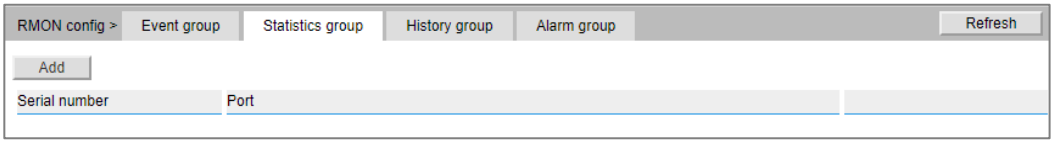
On the "Statistical" page, user can add, delete or check the configuration information of statistical.

Operation Path

Open in order: "Main Menu > RMON Config > Statistical".

Interface Description

Statistical interface as below:



The main element configuration description of statistical interface:

Interface Element	Description
Serial number	Serial number is used to identify a special application interface, when the serial number is same to the application interface serial number set before, previous configuration will be replaced.
Port	Set a port number (physical interface) as the receiving end of monitoring data information.
Add	Click "Add" button to add the related configuration of the statistics group.

7.4.3 History

Function Description

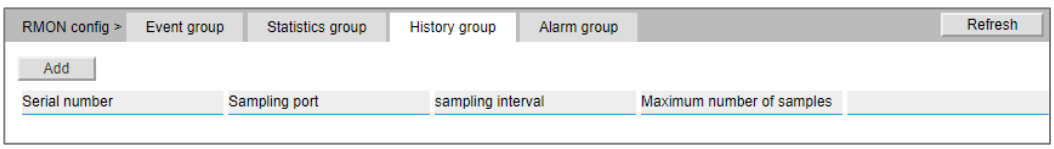
On the "History" page, user can add, delete or check the configuration information of history.

Operation Path

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

Interface Description

History interface as below:



The main element configuration description of history interface:

Interface Element	Description
Serial number	Serial number is used to identify a special application interface, when the serial number is same to the application interface serial number set before, previous configuration will be replaced.
Sampling port	Set a physical interface as the receiving end of monitoring information.
Sampling interval	The interval time of gaining statistics data each two times.
Maximum number of samples	Table entries needed to be reserved.
Add	Click "Add" button to add the related configuration of the history group.

7.4.4 Alarm Group

Function Description

On the "Alarm Group" page, user can add, delete the alarm or check the alarm configuration information.

Alarm type adopts absolute to directly monitor MIB object value; Alarm type adopts delta to monitor changes in MIB object values between two samples;

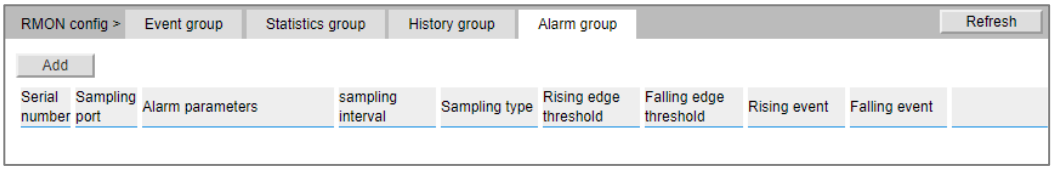
- When monitoring MIB object reaches or surpasses the rising threshold value, it will trigger corresponding event of rising event index;
- When monitoring MIB object reaches or surpasses declining threshold value, it will trigger corresponding event of declining event index;

Operation Path

Open in order: "Main Menu > Advanced Config > RMON Config > Alarm Group".

Interface Description

Alarm group interface as below:



The main element configuration description of alarm group interface:

Interface Element	Description
Serial number	Serial number is used to identify a specific alarm configuration information, when the serial number is same to the application interface serial number set before, previous configuration will be replaced.
Sampling port	Set a physical interface as the receiving end of monitoring information.
Alarm parameters	Alarm parameters, options as follows: • DropEvents: Falling edge event; • Octets: Byte. • Pkts: Data packet. • BroadcastPkts: Broadcast packet; • MulticastPkts: Multicast packet; • CRCAlignErrors: CRC alignment errors; • UndersizePkts: Ultra short packet number, less than 64 bytes; • OversizePkts: Ultra-long packet number, more than 1518 bytes; • Fragments: Fragment frame data; • Jabbers: Invalid huge frame data, more than 1518 bytes; • Collisions: Conflicts occur; • Pkts64Octets: 64 bytes data packet; • Pkts65to127Octets: 65-127 bytes data packet; • Pkts128to255Octets: 128-255 bytes data packet; • Pkts256to511Octets: 256-511 bytes data packet; • Pkts512to1023Octets: 512-1023 bytes data packet; • Pkts1024to1518Octets: 1024-1518 bytes data packet.
Sampling interval	Sampling time interval value, value range is 5-65535, unit: second.
Sampling Type	Two sampling methods, options as follows: • Absolute: When alarm variable value reaches alarm

Interface Element	Description
	threshold value, an alarm is triggered; If the second sampling is same to last sampling alarm type, alarm isn't triggered again; • Delta: When alarm variable value reaches alarm threshold value during each sampling, an alarm is triggered.
Rising edge threshold	Alarm variable value, upper limit alarm, threshold value is 0-4294967295. Note: In the rising process of alarm variable value, when the variable value surpasses rising threshold, an alarm occurs at least one time.
Falling edge threshold	Alarm variable value, lower limit alarm, threshold value is 0-4294967295. Note: In the falling process of alarm variable value, when the variable value reaches falling threshold, an alarm occurs at least one time.
Rising Event	Event index, when alarm variable value reaches or surpasses the rising event threshold value, it will activate corresponding event in event group, value range is 0-1024.
Falling Event	Event index, when alarm variable value reaches or is less than the falling threshold value, it will activate corresponding event in event group, value range is 0-1024.
Add	Click "Add" button to add the related configuration of the alarm group.

7.5 DHCP Server Configuration

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

7.5.1 DHCP Server

Function Description

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

Operation Path

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

Interface Description

The DHCP server interface as follows:

The main element configuration description of DHCP Server configuration interface:

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

7.5.2 DHCP address pool

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

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

DHCP server adopts tree structure: Tree root is the address pool of natural network segment. Branch is the subnet address pool of the network segment. Leaf node is the manually binding client address. The order of address pool at the same level is decided by the configuration order. This kind of tree structure has realized the inheritance of configuration, that is, subnet configuration inherits the configuration of natural network segment, and client configuration inherits the subnet configuration.

Therefore, as for some common parameters (such as DNS server address), user only needs to configure in the natural network segment or subnet. Specific inheritance situation as follows:

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

Function Description

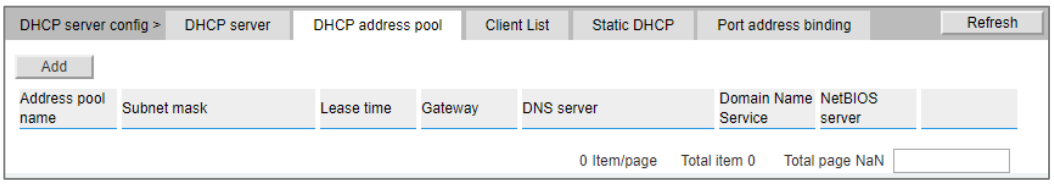
On the "DHCP Pool Address" page, user can add, delete the address pool and look over the configuration information of address pool.

Operation Path

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

Interface Description

DHCP address pool interface as follow:



The main elements configuration description of DHCP address pool interface:

Interface Element	Description
Address pool name	Address pool name, length range is 1-31.
Subnet mask	Address pool distributes the IP address network segment of client, for example: 192.168.0.1/24.
Lease time	IP address utilization valid time of client, range is 0-999 days.
Gateway	Default gateway address of client.

Interface Element	Description
DNS server	DNS server IP address of client.
Domain Name Service	DNS server domain address of client.
NetBIOS Server	NetBIOS server IP address of client.
Add	Click "Add" button to add the related configuration of DHCP address pool.

7.5.3 Client List

Function Description

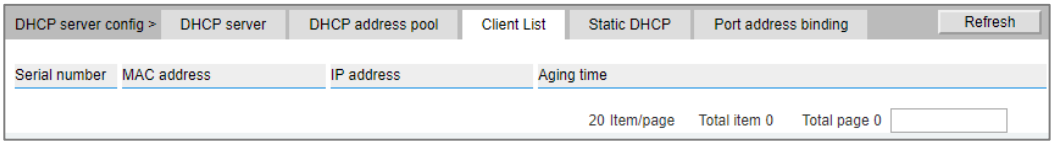
On the "Client List" page, user can look over the information of DHCP client.

Operation Path

Open in order: "Main Menu > Advanced Config > DHCP Server Config > Client List".

Interface Description

Client list interface as follows:



The main element configuration description of client list interface:

Interface Element	Description
Serial number	Serial number name of DHCP client.
MAC address;	MAC address of DHCP client device.
IP address	IP address of DHCP client-side device.
Aging Time	Ageing time of the client address.

7.5.4 Static DHCP

Function Description

On the page of "Static DHCP", user can add, delete, and view the configuration information of static clients.

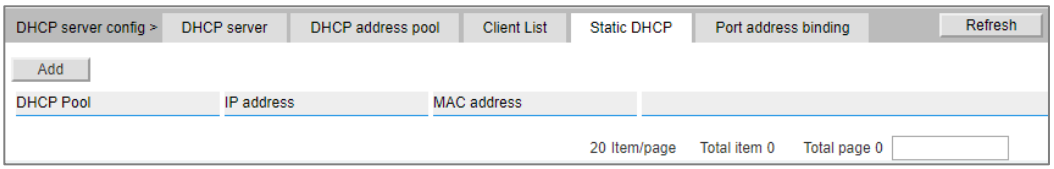
The client MAC address is bound to the address assigned by DHCP server; therefore, each address obtained by the client from server is a binding IP address.

Operation Path

Open in order: "Main Menu > Advanced Configuration > DHCP Server Configuration > Static DHCP".

Interface Description

Static DHCP configuration interface as follows:



The main element configuration description of static DHCP configuration interface:

Interface Element	Description
DHCP Pool	Corresponding list name of DHCP address pool.
IP Address	IP address that DHCP address pool distributes, client needs to gain the static IP address.
MAC Address	MAC address of DHCP client.
Add	Click "Add" button to add the related configuration of Static DHCP.

7.5.5 Port Address Binding

Function Description

On the “Port Address Binding” page, users can bind the relationship of IP addresses assigned by ports.

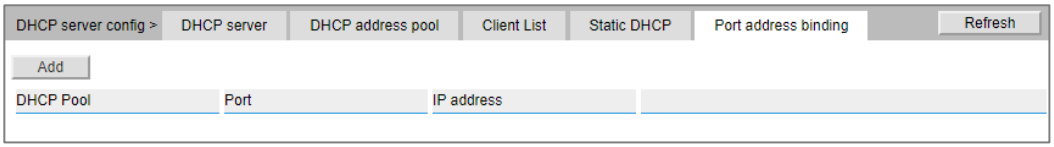
Device A enables DHCP Server function and sets 2 static distribution address tables: 192.168.1.19 corresponding port is 1; 192.168.1.20 corresponding port is 2. After device B enables IP address automated acquisition function, if device A is connected to device B via port 1, device B can automatically 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: "Main Menu > Advanced Configuration > DHCP Server Configuration > Port Address Binding".

Interface Description

Port address binding interface as follows:



The main element configuration description of port binding interface:

Interface Element	Description
DHCP Pool	Corresponding list name of DHCP address pool.
Port	The corresponding port name of the device Ethernet port.
IP Address	IP address that DHCP address pool distributes, the IP addresses that client gains in the port.
Add	Click "Add" button to add the related configuration of port address binding.

7.6 DHCP-Snooping Configuration

DHCP Snooping is layer 2 snooping function of DHCP service, after enable DHCP Snooping function, the device can extract and record IP address and MAC address information from received DHCP-ACK and DHCP-REQUEST messages.

For security reasons, security department needs to record the IP address used by user to access the Internet, and confirm the correspondence between IP address applied by user and MAC address of the host used by user. User can monitor DHCP-REQUEST messages and DHCP-ACK messages via DHCP Snooping function, and record IP address information user obtains.

7.6.1 Global Configuration

Function Description

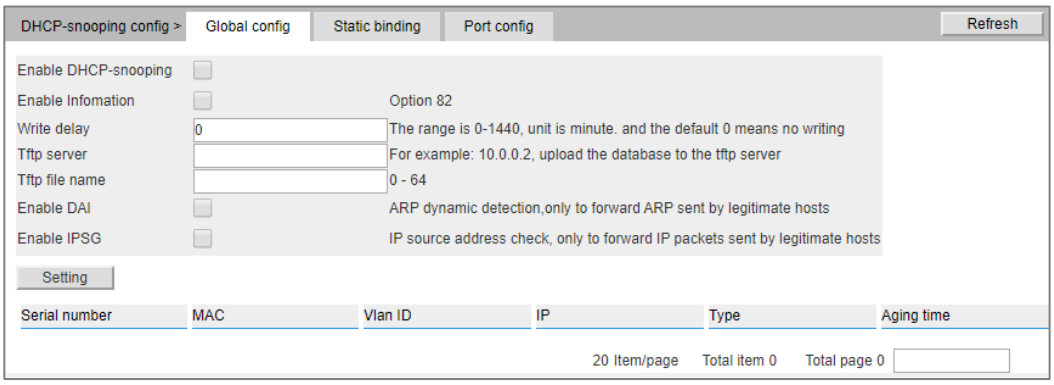
On the "Global Config" page, user can configure DHCP-Snooping parameters information.

Operation Path

Open in order: "Main Menu > Advanced Config > DHCP-snooping > Global Config".

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Enable DHCP-snooping	Enable DHCP-Snooping function checkbox.

Interface Element	Description
Enable Information	Enable information function checkbox, after checking; enable Option 82 relay agent function which records the location information of DHCP client.
Write Delay	Writing delay range is 1-1440; unit is minute, default to 0, which represents not writing.
Tftp Server	Upload database to IP address of TFTP server, for example 10.0.0.2.
Tftp File name	Folder name of database uploading to TFTP server.
Enable DAI	Enable DAI optional box, after checking, forward ARP sent by legitimate host according to DHCP Snooping table items.
Enable IPSG	Enable IPSG optional box, after checking, forward IP message sent by legitimate host via dynamically gaining DHCP Snooping table items.

7.6.2 Static Binding

Function Description

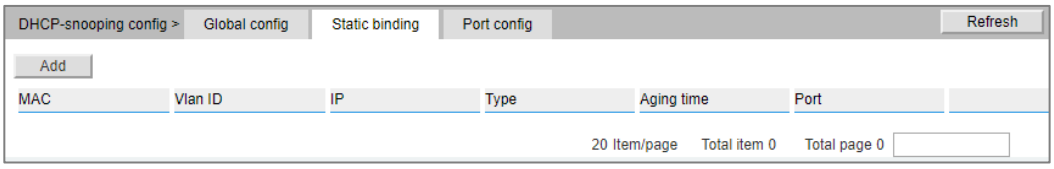
On the "Static Binding" page, user can bind static MAC and port.

Operation Path

Open in order: "Main Menu > Advanced Config > DHCP-snooping > Static Binding".

Interface Description

Static binding interface as follows:



The main element configuration description of static binding interface:

Interface Element	Description
MAC	Binding MAC address, for example: 0001-0001-0001.
Vlan Id	Binding VLAN ID information, for example: 1-4094.

Interface Element	Description
IP	Binding IP address, for example: 192.168.1.1.
Port	The corresponding port name of the device Ethernet port.
Add	Click "Add" button to add the related configuration of static binding.

7.6.3 Port Configuration

Function Description

On the "Port Config" page, user can configure DHCP Snooping port information. The trust function of DHCP Snooping can control the source of the DHCP server reply message to prevent any forged or illegal DHCP server from distributing IP address and other configuration information to other hosts.

The DHCP Snooping trust function divides ports into trust ports and non-trust ports:

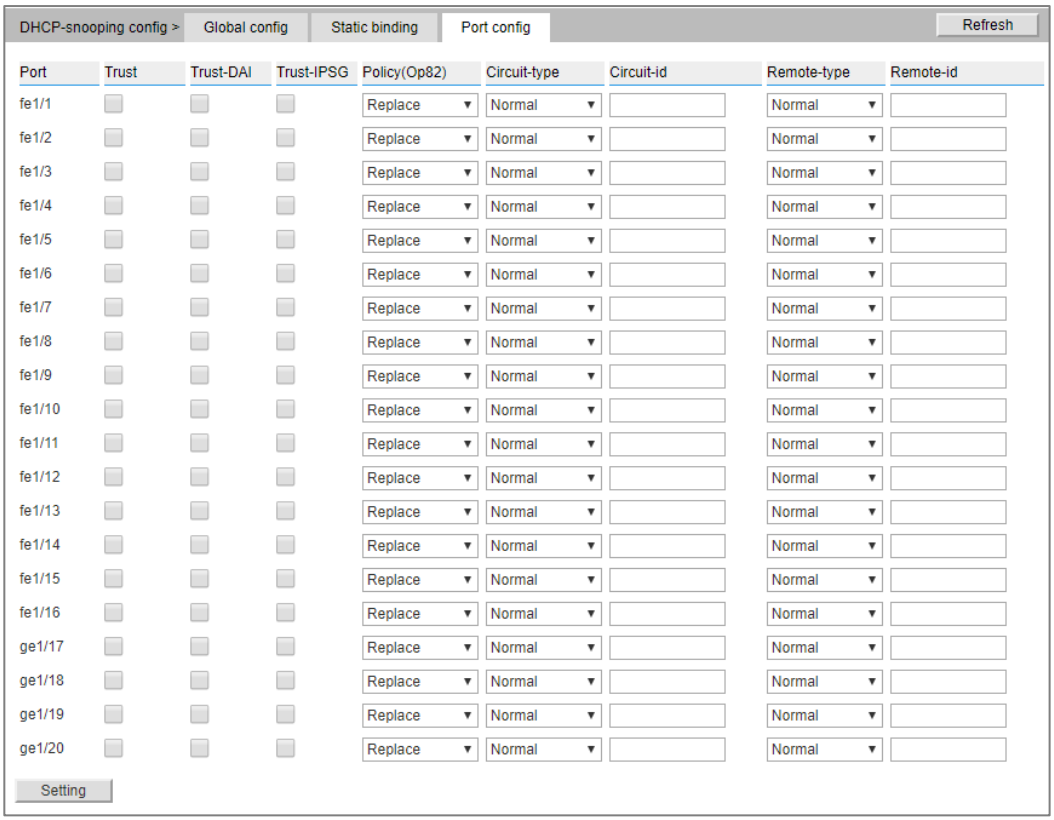
- Trust port is the port that is directly or indirectly connected to legitimate DHCP server. Trust port normally forwards received DHCP messages to ensure that DHCP client can gain correct IP address.
- Distrustful port is the port that isn't connected to legitimate DHCP server. The DHCP-ACK, DHCP-NAK, and DHCP-OFFER packets that receive DHCP server responses from untrusted ports will be discarded, preventing the DHCP client from obtaining the wrong IP address.

Operation Path

Open in order: "Main Menu > Advanced Config > DHCP-snooping > Port Config".

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Trust	Trust checkbox, trust port.
Trust-DAI	Trust-DAI checkbox, trust port ARP dynamic snooping.
Trust-IPSG	Trust-IPSG checkbox, source address examination of trust port IP .
Policy (Op82)	Option 82 dealing strategy, options as follows: • Replace: Keep Option 82 in messages unchanged and forward. • Keep: Adopt different modes to fill Option 82, replace prime Option 82 in message and forward, filling modes will be described as below. • Drop: Discard messages.
Circuit-type	Circuit ID sub-option filling type, options as follows: • Normal: Normal mode; • String: Detailed mode.
Circuit-id	Circuit ID sub-option filling content, support ASCII and HEX mode.

Interface Element	Description
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	Remote ID sub-option filling content, support ASCII and HEX mode.

7.7 DNS Settings

Function Description

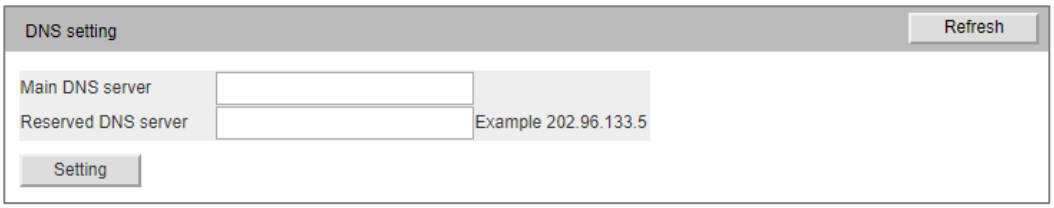
On the “DNS Settings” page, you can configure the IP address information of the DNS server.

Operation Path

Open in order: "Main Menu > Advanced Config > DNS Config".

Interface Description

DNS setting interface as follows:



DNS settings interface main element configuration instructions

Interface Element	Description
Main DNS server	IP address information of the primary DNS server.
Reserved DNS server	IP address information of the backup DNS server, for example: 202.96.133.5.

7.8 NTP Settings

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

Function Description

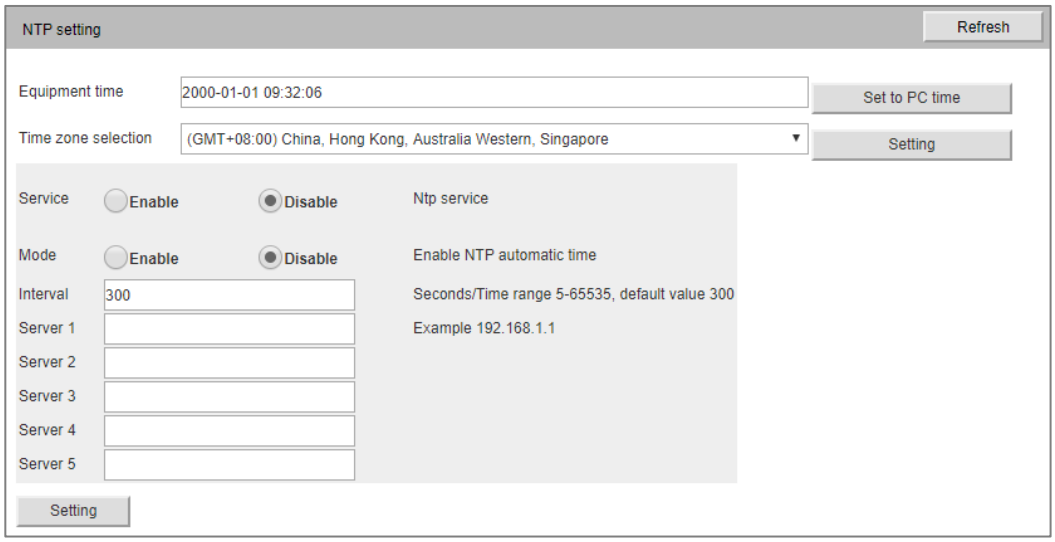
On the "NTP Config" page, user can configure the device time and NTP server information.

Operation Path

Open in order: "Main Menu > Advanced Config > NTP Config".

Interface Description

NTP configuration interface as follows:



The main element configuration description of NTP configuration interface:

Interface Element	Description
Equipment time	The device own time, which can be synchronized to current computer time.
Timezone	Time standard of different global regions.

Interface Element	Description
selection	
Service	The options of enabled status of the server: • Enable; • Disable.
Mode	The status of NTP automatic time synchronization function, options as follows: • Enable; • Disable.
Interval	Time hack interval, values range from 5 to 65535, the default value is 300 seconds/time.
Server 1	IP address of NTP-sync server 1, for example: 192.168.1.1.
Server 2	IP address of NTP-sync server 2, for example: 192.168.1.1.
Server 3	IP address of NTP-sync server 3, for example: 192.168.1.1.
Server 4	IP address of NTP-sync server 4, for example: 192.168.1.1.
Server 5	IP address of NTP-sync server 5, for example: 192.168.1.1.

8 System Maintenance

8.1 Configuration File Management

8.1.1 View Launch Configuration

Function Description

On the "View launch config" page, user can view current configuration information.

Operation Path

Open in order: "Main Menu > System Management > Configuration File Settings > Global Configuration".

Interface Description

Global configuration interface is as follows:

8.1.2 Manage Configuration File

Function Description

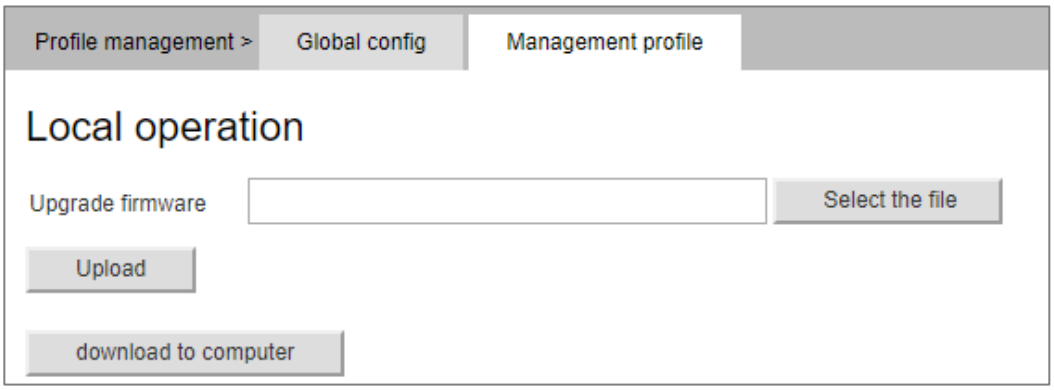
On the "Manage Configuration File" page, user can download and upload configuration file.

Operation Path

Open in order: "Main Menu > System Management > Profile Management > Manage Profile".

Interface Description

Manage Profile interface as follows:



The main element configuration description of Manage Profile interface:

Interface Element	Description
Local operation	**Local operation configuration bar**
Upgrade firmware	Click the "Select the File" button to select the configuration upgrade file locally.
Upload	Click the "Upload" button to upload the configuration file.
Download to computer	Download the configuration file from the device to the PC.

Note

- After the update is completed, a new page will be automatically opened to "system status". The device needs to be restarted before the uploaded profile will take effect.

- When uploading a profile, if the static IP of the profile and the IP of the computer are not in the same network segment, the web page will not open.
- While uploading configuration file, if dynamic IP is used in the configuration file and there is no DHCP server in the network segment, relative IP portion won't be updated.
- In the process of uploading configuration files or upgrading software, please don't click or configure other WEB page of the switch, not even reboot the switch; otherwise, it will lead to failure of configuration files uploading or software upgrading, or even cause system breakdown of the switch.

8.2 Restore Factory Defaults

Function Description

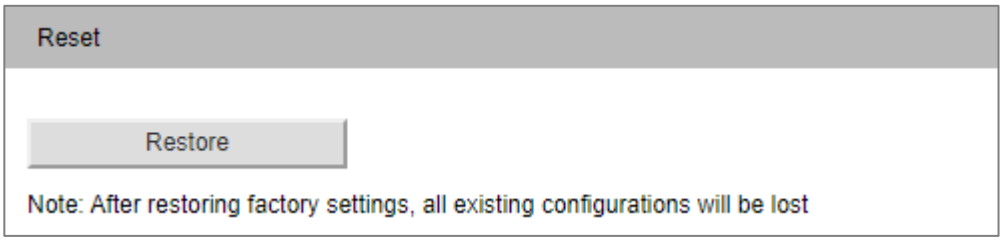
On the "Restore" page, user can restore the device to default settings.

Operation Path

Open in order: "Main Menu > System management > Restore".

Interface Description

Restore Factory Settings interface is as follows:



The main element configuration description of restore factory settings interface:

Interface Element	Description
Restore	Click this button and the device will lose all existing configurations and reverts to factory settings.

Note

Restoring factory value settings will cause all configurations to be in the factory state, where the IP address is configured via CLI or management software, and the user name and password default to "admin".

8.3 Upgrade

Function Description

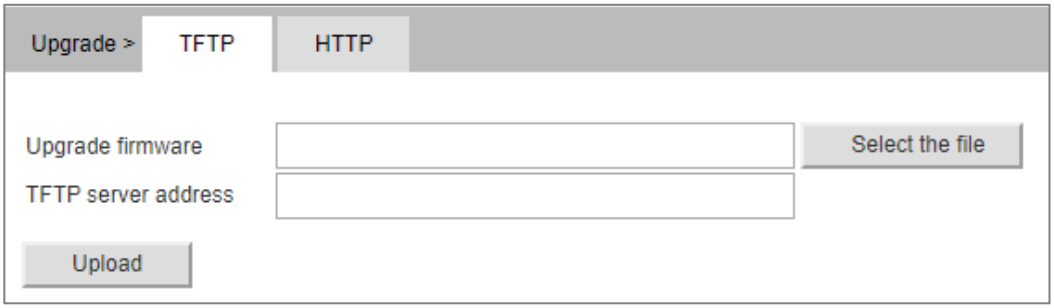
On the "Online Upgrade" page, user can update and upgrade the device procedure via TFTP server.

Operation Path

Open in order: "Main Menu > System Maintenance > Upgrade".

Interface Description: TFTP

TFTP interface as below:

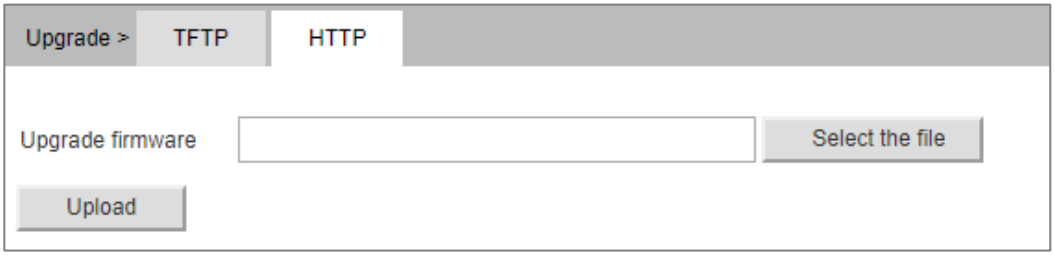


Main elements configuration descriptions of TFTP interface:

Interface Element	Description
Upgrade firmware	Select the upgrade file on TFTP server
TFTP server address	The IP addresses of TFTP server that stores upgrade files.

Interface Description: HTTP

Upload interface is as below:



Main elements configuration descriptions of HTTP interface:

Interface Element	Description
Upgrade firmware	Select local upgrade file
Upload	The upgrade file is uploaded to the device, and the device program can be locally updated and upgraded.

Note

- Do not click on or configure other WEB pages of the device or restart the device or power off the device when upgrading software. Otherwise, the software update will fail, or the device system will crash.
- Keep a reliable wired connection when upgrading.
- When the online upgrade is complete, the device will restart automatically.

The Second Part: Frequently Asked Questions

9 FAQ

9.1 Sign in Problems

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

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

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

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

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

   Both configurations are the same, without conflict.

9.2 Configuration Problem

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

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

2. **What's the difference between RING V2 and RING V3?**

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

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

   When some ports on the switch are impassable, it may be network cable, network adapter and switch port faults. User can locate the faults via following tests:

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

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

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

9.3 Indicator Problem

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

Possible reasons include:

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

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

Possible reasons include:

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

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

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

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

Reasons may include:

- Surrounding environment disturbs the product; troubleshooting, product grounding adopts shielding line or shields the interference source.
- Site wiring is not normative; Troubleshooting, optical fiber, network cable, optical cable cannot be arranged with power line and high-voltage line.

- Network cable is disturbed by static electricity or surge; Troubleshooting, change the shielded cable or install a lightning protector.
- High and low temperature influence; troubleshooting, check the device temperature usage range.

10 Maintenance and Service

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

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

- Internet Service;
- Call technical support office;
- Product repair or replacement;

10.1 Internet Service

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

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

10.2 Service Hotline

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

10.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company's technical staff, and then contact the salesmen to solve the problem. According to the company's handling procedure, customers should negotiate with our company's technical staff and salesmen to complete the product maintenance, replacement or return.

Appendix

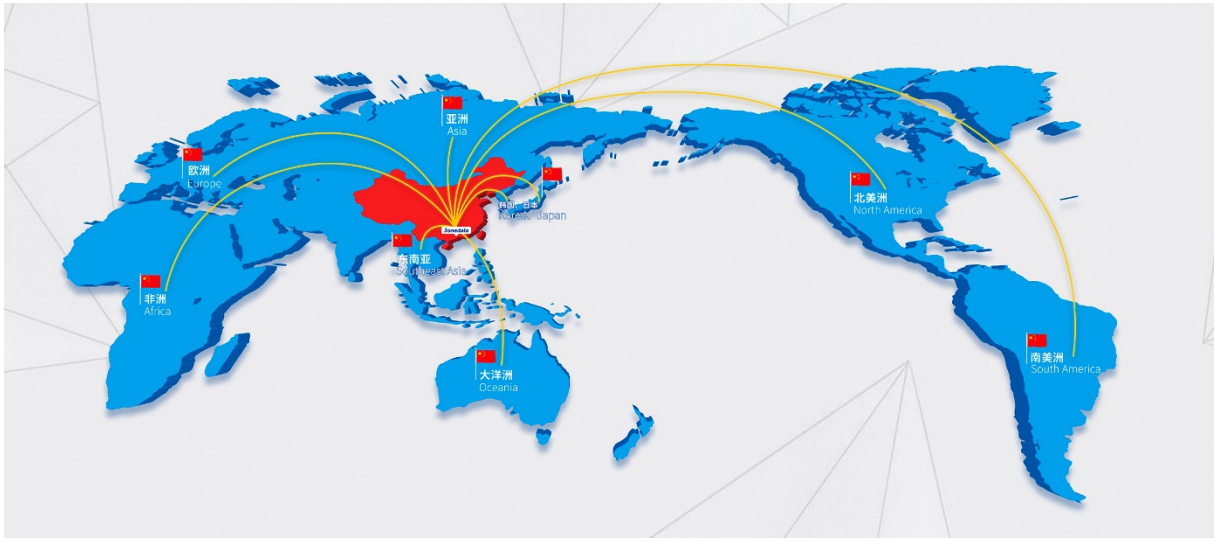
The detailed description and corresponding level of the code are as follows:

ID	Note	Level
1	Power Alarming	Error
2	Port Alarming	Error
3	Temperature Alarming	Error
4	Mrp Alarming!ring state open.	Error
5	Leakage Current Alarming	Error
6	Netload Alarming	Error
7	Warning Neigborhood Alarming	Error
8	Sdcard Alarming!SD card can not detect. Alarming	Error
9	DSP warning!	Error
10	AR Disconnect!	Error
11	Upgrade form Web TFTP mode	Notice
12	Upgrade form Web HTTP mode	Notice
13	Upgrade form sdCard	Notice

14	Download configuration to Web TFTP mode	Notice
15	Download configuration to SD card	Notice
16	Upgrade configuration by Web TFTP mode	Notice
17	Upgrade configuration by SD card	Notice
18	System reboot	Notice
19	System restore	Notice
20	Save running configuration	Notice
21	AR Connect	Notice
22	Time sync form server	Notice
23	User log clear	Notice
24	Test Mail send failed	Notice
25	Netload reset	Notice
26	Leakage current reset	Notice
27	DSP self-Saving	Notice
28	Dhcp server offering.	Notice
29	Dhcp server no offering.	Notice
30	Function Port mirror enable	Information
31	Function IGMP-Snooping enable	Information
32	Function STP enable	Information

33	Function MRP enable	Information
34	Function ACL enable	Information
35	Function NTP enable	Information
36	Function NTP disble	Information
37	Function NTP server enable	Information
38	Function NTP server disable	Information
39	Port Up	Information
40	Port Download	Information
41	Power on	Information
42	Power off	Information

3onedata



3onedata Co., Ltd.

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

Technology Support: tech-support@3onedata.com

Service Hotline: 4008804496

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