6 100M Copper Ports + 2/3 100M Fiber Ports Series

Managed Industrial Ethernet Switch

User Manual

Document Version: 01

Issue Date: 03/06/2023

Preface

Managed 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.

Button Operation Convention

Format	Description
Logout	There is a logout button in the upper right corner of the webpage. After clicking it, the webpage returns to the login page.
Reboot	There is a restart button in the upper right corner of the webpage. After clicking, a restart confirmation box pops up. After confirmation, the device will restart.
Save	There is a Save button in the upper right corner of the webpage. Click it to save the current device configuration.
Add	Click the Add button to add a line of configuration. Note that repeated configuration may result in data overwrite.
Delete	Check the line to be deleted, and then click the Delete button to delete the configuration.
Config	Check the line to be configured, and then click the configure button to enter the configuration page.
	Click the right side of the switch to enable the function, as shown in figure:  . Click the left side of the switch to disable the function, as shown in the figure:  .
Apply	Click the Set button to submit the current configuration.

Revision Record

Version No.	Date	Revision note
01	03/06/2023	Product release

Contents

1 Log in 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 Setting IP Address of PC

The switch default management as follows:

IP Settings	Default Value
IP Address	192.168.1.254
Subnet mask	255.255.255.0

While configuring the switch via Web:

- Before remote configuration, please make sure the route between computer and switch is reachable.
- Before local configuration, please make sure the IP address of the computer is on

the same subnet to the one of switch.

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

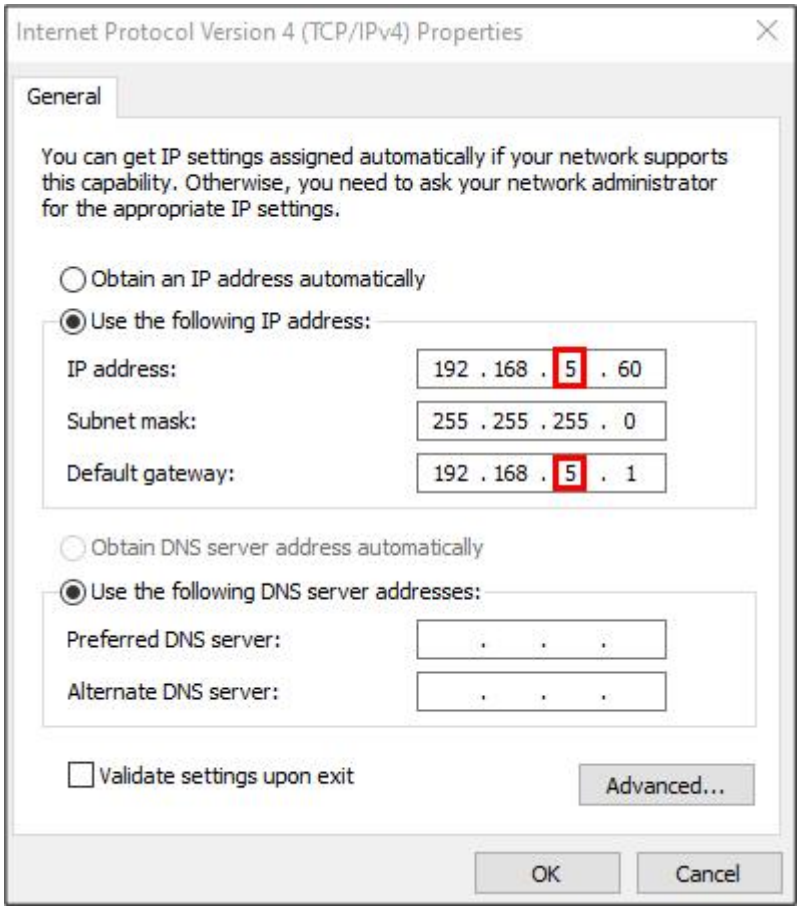
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follow:

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

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



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

Step 4 End.

1.3 Log in the Web Configuration Interface

Operation Steps

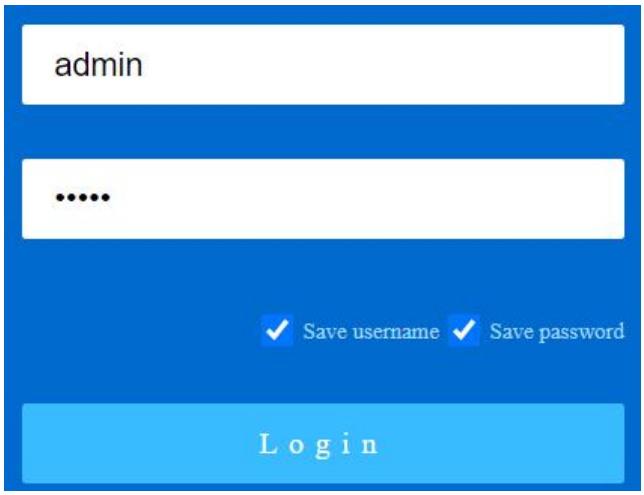
Login in the web configuration interface as follow:

Step 1 Run the computer browser.

Step 2 Enter the address of the switch "http://192.168.1.254" in the address bar of the browser.

Step 3 Click the Enter key.

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



Note:

- The default user name and password are “admin”, please strictly distinguish capital and small letter while entering.
- The default user password is with administrator privileges.
- WebServer will provide 3 opportunities to enter username and password. If you enter the error 3 times in succession, the browser will display "Access denied" to deny access to the information. Please refresh the page and try again.

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

View port status such as port type and connection status.

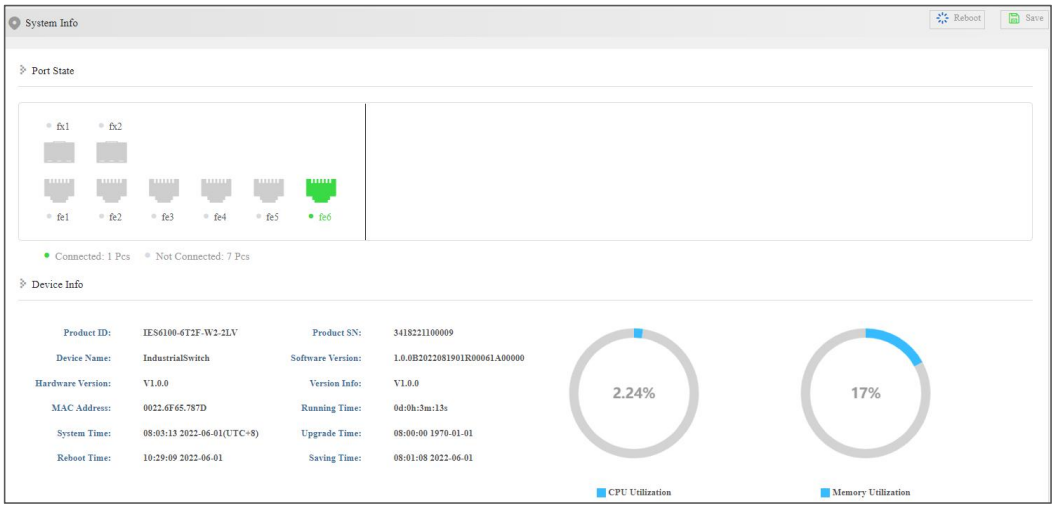
Check device information such as product model, software and hardware version, etc.

Operation Path

Open in the navigation bar: “System Information”.

Interface Description

System information interface screenshot:



The main element configuration description of state information interface:

Interface Element	Description
Port State Bar	Display port icon and port connection status of the device:

Interface Element	Description
	•  Copper port icon, grayed out indicates that the device is not connected. •  Copper port icon, highlighting indicates that the device is connected. •  Fiber port icon, grayed out indicates that the device is not connected. •  Fiber port icon, highlighting indicates that the device is connected.
Device information column	Basic information of software, hardware and operation of the device. • Product ID • Device Name • Hardware Version • Mac Address • System Time • Reboot Time • Product SN • Software Version • Version Info • Running Time • Upgrade Time • Saving Time • CPU Utilization • Memory Utilization

3 Login Configuration

3.1 IP Address Configuration

Function Description

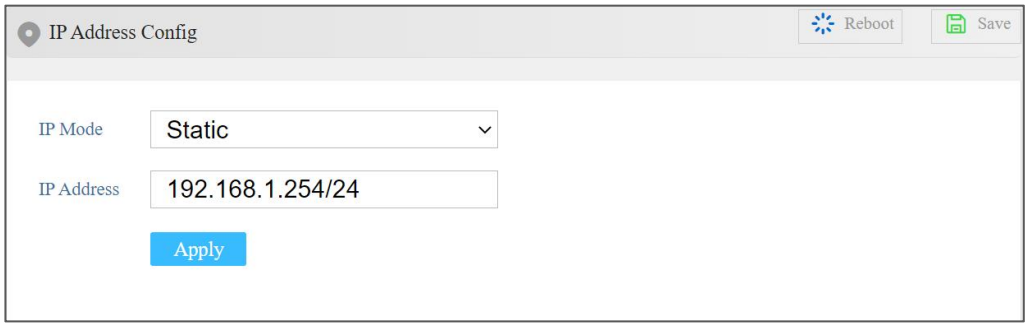
Configure the static or dynamic IP address.

Operation Path

Open on the navigation bar: "Login Configuration > IP Address Config".

Interface Description

Interface screenshot of IP address configuration:



The main elements configuration description of IP address configuration interface:

Interface Element	Description
IP Mode	Set the IP address acquisition mode, which can be set to: • Static: System IP address configured by default or manually. • Dynamic: system automatically acquired IP address of the device.

Interface Element	Description
	Note Default configured IP address is 192.168.1.254/24.
IP Address	Display the IP address of the device.

3.2 User Configuration

Function Description

Add/delete users accessing the network management system.

Operation Path

Open in the navigation bar: “Login Configuration” > “User Configuration”.

Interface Description

The screenshot of user configuration interface:

The main element configuration description of state information interface:

Interface Element	Description
Username	User name for accessing the network management system. Note: • The user name is a combination of letters, numbers and symbols not more than 20 bytes. Please be case-sensitive. • Up to 5 groups of users are supported.
Password	User name for accessing the network management system. Note: The password is a combination of letters, numbers and symbols not more than 20 bytes. Please be case-sensitive.

Notice

Please keep the modified login name and password in mind. If you forget it, you can restore it to factory setting via DIP switch. Default login name and password of logging in to the WEB configuration interface are “admin”.

3.3 Protocol Authorization

Function Description

Open the access security protocols Telnet and SSH for the remote login service.

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. After SSH function is enabled, users can enter the command line configuration interface to manage devices.

Telnet is the standard protocol and main mode of Internet remote login service. It provides users with the ability to complete the remote host work on the local computer. After the TELNET function is enabled, users can enter the command line configuration interface to manage devices.

Operation Path

Open in the navigation bar: “Login Configuration > Protocol Authorization”.

Interface Description

Screenshot of protocol authorization interface:

Configuration description of main elements of the protocol interface:

Interface Element	Description
Telnet Switch	After opening, users can access the command line configuration interface through Ethernet port.
SSH Switch	After opening, users can access the command line configuration interface through the Console port.

4 Port Configuration

4.1 Port Settings

Function Description

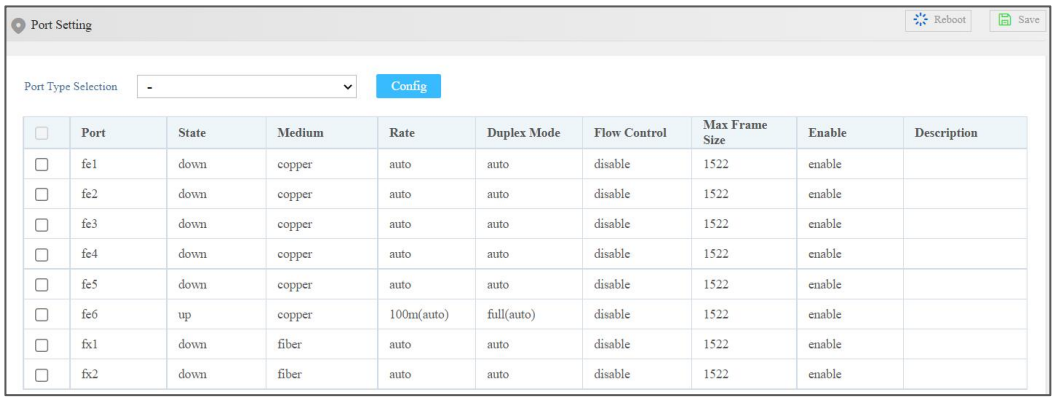
Set port parameters individually or in batches.

Operation Path

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

Interface Description

Port setting interface as follows:



Port	State	Medium	Rate	Duplex Mode	Flow Control	Max Frame Size	Enable	Description
fe1	down	copper	auto	auto	disable	1522	enable	
fe2	down	copper	auto	auto	disable	1522	enable	
fe3	down	copper	auto	auto	disable	1522	enable	
fe4	down	copper	auto	auto	disable	1522	enable	
fe5	down	copper	auto	auto	disable	1522	enable	
fe6	up	copper	100m(auto)	full(auto)	disable	1522	enable	
fx1	down	fiber	auto	auto	disable	1522	enable	
fx2	down	fiber	auto	auto	disable	1522	enable	

Main elements configuration description of port settings interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
State	Ethernet port connection status, display status as follows: • down: represent the port is disconnected; • up: represent the port is connected.

Interface Element	Description
Medium	Ethernet port connection type, display medium as follows: • copper: copper port • fiber: fiber port
Rate	Ethernet port working speed, optional speed as follows: • auto • 10m • 100m
Duplex Mode	Under current Ethernet working mode, optional mode as follows: • Auto: Auto-negotiation • Full: full duplex • Half: half-duplex
Flow Control	Port flow control status, options as follows: • disable • enable
Max Frame Size	Display the maximum data frame length that the Ethernet port transmitted.
Enable	Enable Ethernet port. Notice: If “disable” is selected, the port won't be connected to use.
Description	Support entering port description of no more than 40 characters.

4.2 Link Aggregation

The link aggregation technology can increase link bandwidth by bundling multiple physical interfaces into one logical interface without hardware upgrade. While increasing the bandwidth, link aggregation adopts the mechanism of backup link, which can effectively improve the reliability of link between devices.

Link aggregation technology has the following three advantages:

- Increase bandwidth

  The maximum bandwidth of link aggregation interface can reach the sum of the bandwidth of each member interface.
- Improve the reliability

  When an active link fails, traffic can be switched to other available member links, thus improving the reliability of link aggregation interface.

- Load sharing

  Within a link aggregation group, load sharing can be achieved on the active links of each member.

Function Description

Binding multiple physical ports into one logical channel.

Operation Path

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

Interface Description

Screenshot of Link Aggregation interface:

The main element configuration description of Link Aggregation interface:

Interface Element	Description
Group Name	Aggregation group number, support two groups of ports of the same type.
Port Member	Ports that join the trunking group.

Note

- The attributes of all member ports in trunking group should be the same, including medium, rate and duplex mode, etc.
- Setting one port as both ring network port and trunking port is not supported.
- One port can only join a trunking group.

4.3 Port Speed Limit

Function Description

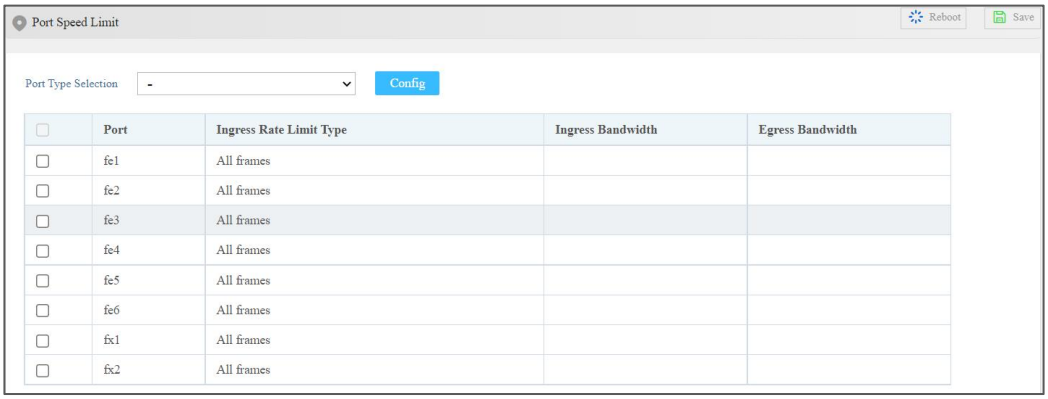
Single or batch limit the ingress bandwidth and egress bandwidth of broadcast, multicast and unicast received by the port.

Operation Path

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

Interface Description

Port speed limit interface is as follows.



Main elements configuration description of bandwidth management interface:

Interface Element	Description
Port Type Selection	Select the port type, and check the ports of the same type in batches: • 100M port (fe) • 100M fiber port (fx)
	Check box, you can check multiple ports for simultaneous configuration.
Port	Port number of the device.
Ingress Rate Limit Type	The data packets type of receiving bandwidth needs to be limited, options of drop-down list as follows: • All frames: all kinds of data packets; • Broadcast, Multicast and flood unicast frames • Broadcast and Multicast only; • Broadcast only.

Ingress Bandwidth	Limit the transmission rate of all ingress data, and select the rate range: • 128/256/512Kbps • 1/2/4/8/16/64Mbps
Egress Bandwidth	Limit the transmission rate of all egress data, and select the rate range: • 128/256/512Kbps • 1/2/4/8/16/64Mbps

Note

Port speed limit has high requirements on network cable quality. If the cable quality is not up to the standard, lots of conflict packets and broken packet would appear.

4.4 Port Mirroring

Function Description

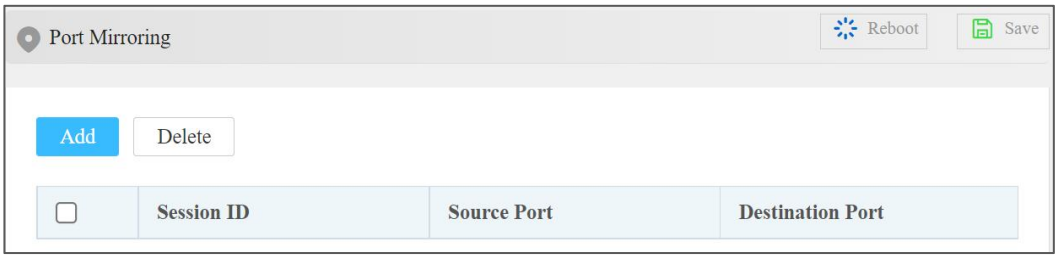
Copy the data from the source port to the appointed port for analysis and monitoring.

Operation Path

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

Interface Description

Port mirror interface as follows:



The main element configuration description of port mirror interface:

Interface Element	Description

Interface Element	Description
Session ID	Device mirror ID number, value is 1. Note: Support only 1 mirror session. If mirroring is configured multiple times, only the data of the last configuration will be retained.
Source Port	Monitored ports, from which the device will collect input or output messages. There can be one or more mirror ports.
Destination Port	Monitoring port, used to copy and analyze messages from source port.
Add	Click “Add” to reconfigure the mirror and configure the data direction of the mirror. Data direction options are as follows: • transmit tx: egress data, the message sent by the source port will be mirrored to the destination port; • receive rx: ingress data, the message received by the source port will be mirrored to the destination port; • Both: all data, mirror the source port receiving and sending packets at the same time.

4.5 Port Statistics

4.5.1 Port Statistics-Overview

Function Description

Check the data information of each port:

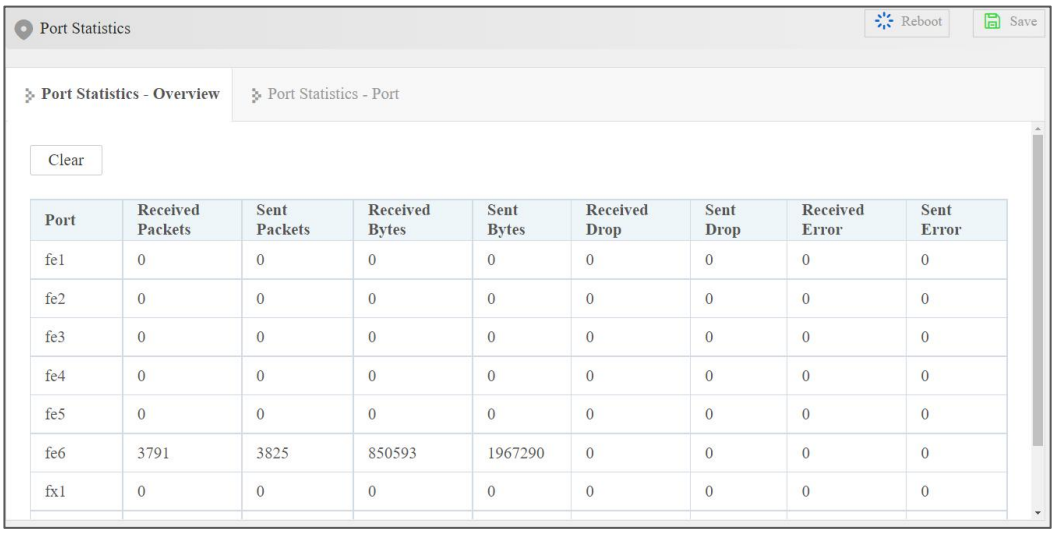
- Number of messages sent and received and number of message bytes
- Number of dropped and error messages

Operation Path

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

Interface Description

Port Statistics-Overview interface as follows:



Port	Received Packets	Sent Packets	Received Bytes	Sent Bytes	Received Drop	Sent Drop	Received Error	Sent Error
fe1	0	0	0	0	0	0	0	0
fe2	0	0	0	0	0	0	0	0
fe3	0	0	0	0	0	0	0	0
fe4	0	0	0	0	0	0	0	0
fe5	0	0	0	0	0	0	0	0
fe6	3791	3825	850593	1967290	0	0	0	0
fx1	0	0	0	0	0	0	0	0

4.5.2 Port Statistics-Port

Function Description

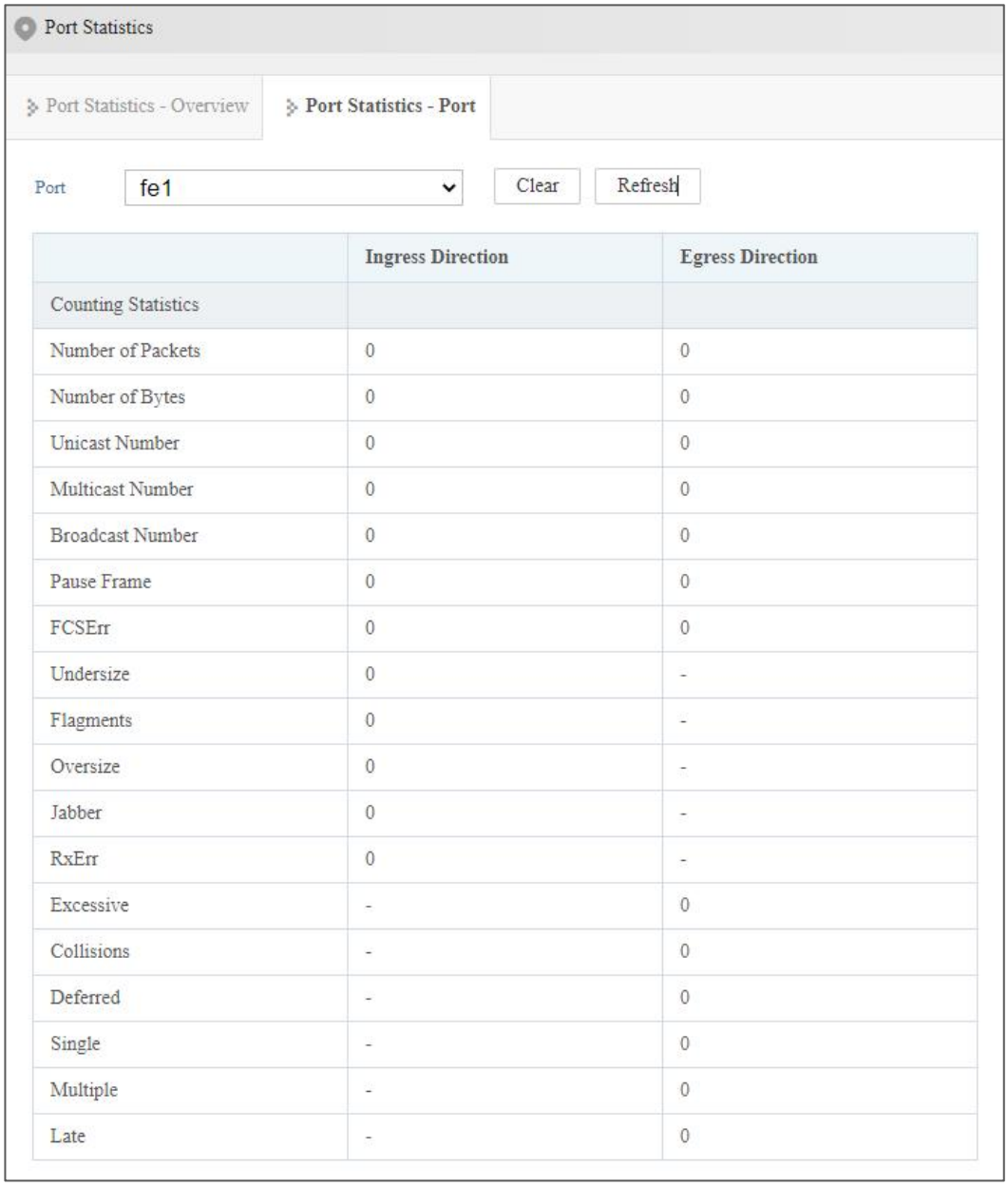
Check the classification statistics of the total number of messages sent and received by the designated port and the number of bytes of messages.

Operation Path

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

Interface Description

Port Statistics-Port interface as follows:



	Ingress Direction	Egress Direction
Counting Statistics		
Number of Packets	0	0
Number of Bytes	0	0
Unicast Number	0	0
Multicast Number	0	0
Broadcast Number	0	0
Pause Frame	0	0
FCSErr	0	0
Undersize	0	-
Flagments	0	-
Oversize	0	-
Jabber	0	-
RxErr	0	-
Excessive	-	0
Collisions	-	0
Deferred	-	0
Single	-	0
Multiple	-	0
Late	-	0

5 Layer 2 Configuration

5.1 VLAN Configuration

VLAN (Virtual Local Area Network) is a communication technology that logically divides a physical LAN into multiple broadcast domains. Hosts in VLAN can directly communicate with each other, but two VLAN can't directly communicate with each other, which can limit the broadcast message in a VLAN. Using VLAN can bring following benefits to users.

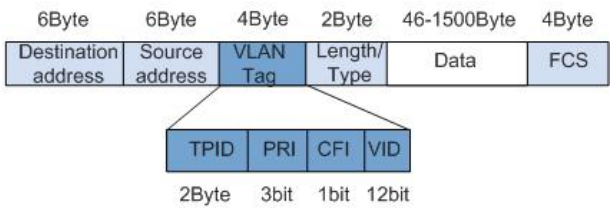
- Limit the broadcast domain;
- Increase the security of LAN;
- Improve the network stability;
- Flexibly construct virtual working team.

Port VLAN

Port VLAN adopts different identifications to distinguish different VLAN. Adopting the same ID identification will cause internal member groups being replaced, new ID identification will establish new forwarding rules, and all ports must belong to one or more VLAN.

IEEE802.1Q VLAN

Under the provisions of IEEE 802.1Q protocol, the device can add 4 bytes VLAN tag (Tag for short) between Source address and Length/Type fields of Ethernet data frame, identifying the VLAN information. As the picture below.



- TPID: Tag Protocol Identifier represents the data frame type, when the value is 0x8100, it represents the VLAN data frame of IEEE 802.1Q.
- PRI: Priority represents the 802.1p priority of data frame. Value range is 0-7, larger value represents higher priority. During network congestion, the switch will preferentially send data frame with higher priority.
- CFI: Canonical Format Indicator represents whether MAC address is packaged in standard format in different transmission media. 0 represents that MAC address is packaged in standard format.
- VID: VLAN ID represents the VLAN number of the data frame. The value range of VLAN ID is 0-4095. 0 and 4095 are reserved values of the protocol, so the valid value range of VLAN ID is 1-4094.

5.1.1 Global Configuration

Function Description

Global Configuration could realize:

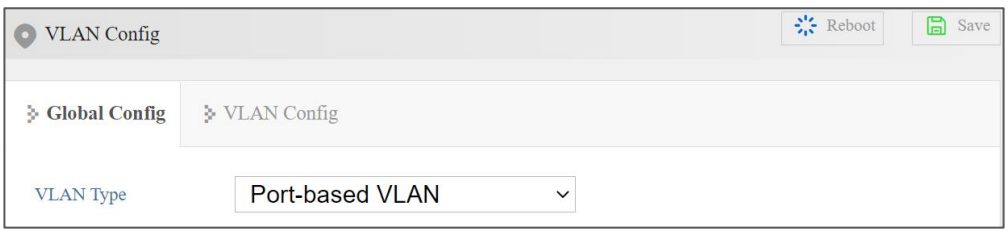
- Set VLAN type
- Set the PVID of CUP
- Set the default PVID of the port
- Set port type

Operation Path

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

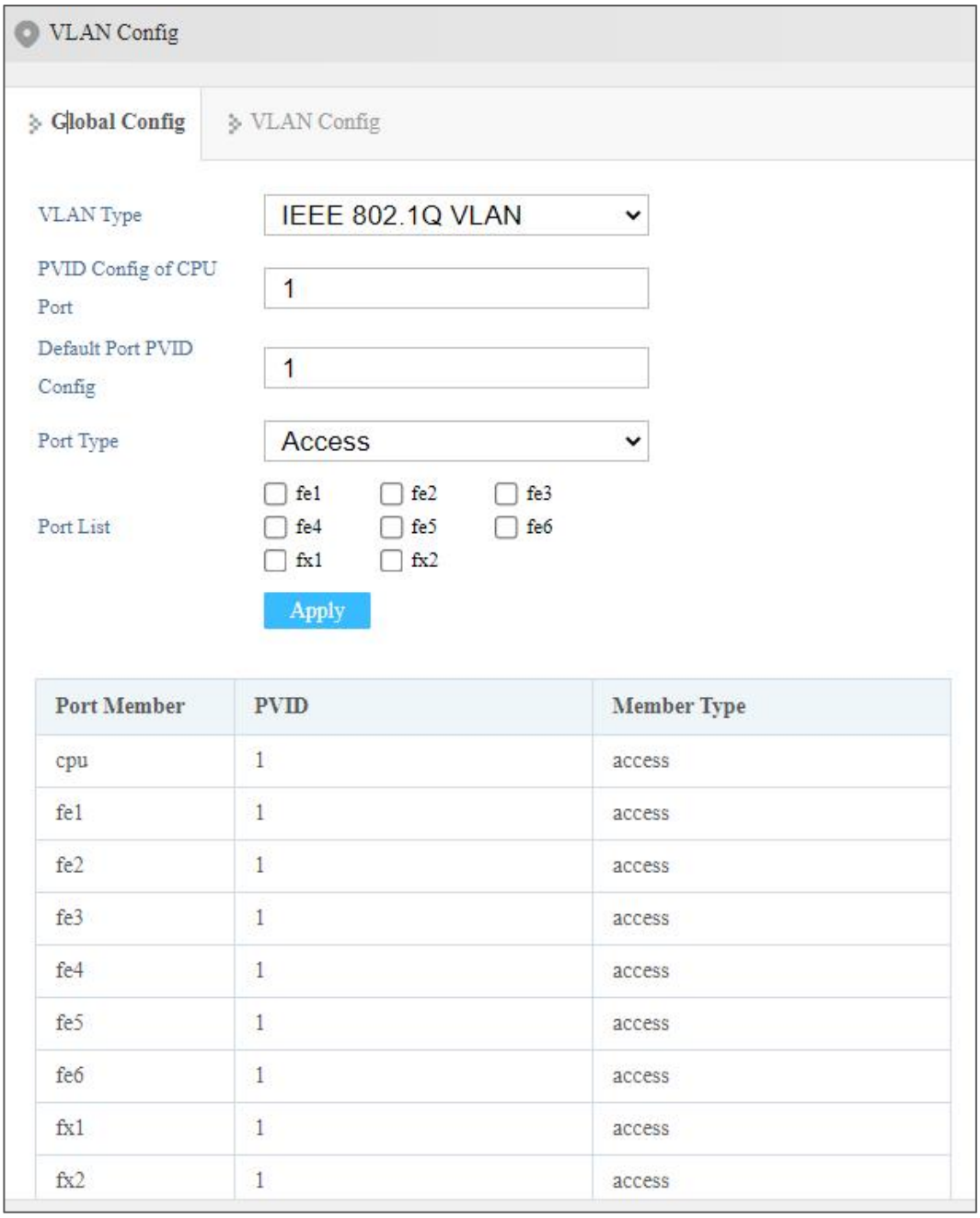
Interface Description 1: Port-based VLAN

Port-based VLAN interface as follows:



Interface Description: 802.1Q VLAN

Interface screenshot of 802.1Q VLAN:



The main element configuration description of global configuration interface:

Interface Element	Description
VLAN Type	VLAN can be configured in two types: • Port-based VLAN • 802.1Q VLAN
PVID Config of CPU Port	The default configuration is 1, and the optional range is 1-4094.
Default Port PVID Config	The default configuration is 1, and the optional range is 1-4094.

Interface Element	Description
Port Type	Configure the link type of port, there are two types as follows: • Access: The message entering the switch from the Access port, which is forced to use the PVID of the port as the VLAN ID. • Trunk: the message entering the switch from Trunk port. If there is already a VLAN TAG, use the VLAN ID in the VLAN TAG of the message; Otherwise, use the PVID of this port as VLAN ID.
Port List	Device port number check box to configure the port type of the selected port in batch.

5.1.2 VLAN Configuration

Function Description

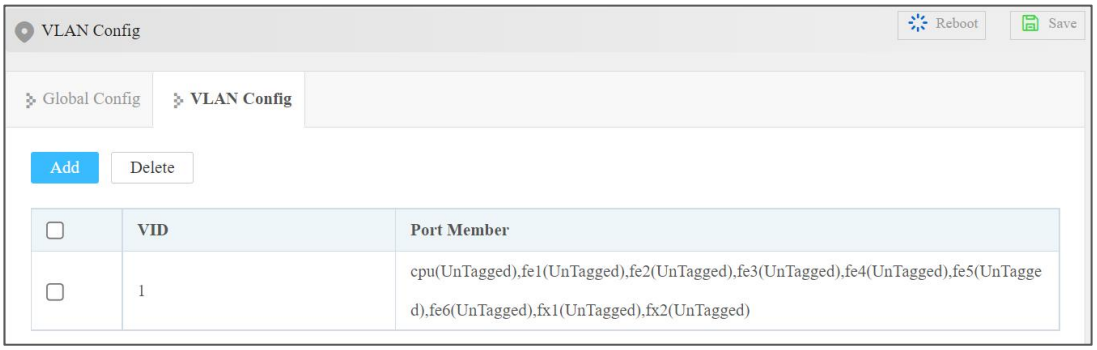
Add VLAN based on port or 802.1Q.

Operation Path

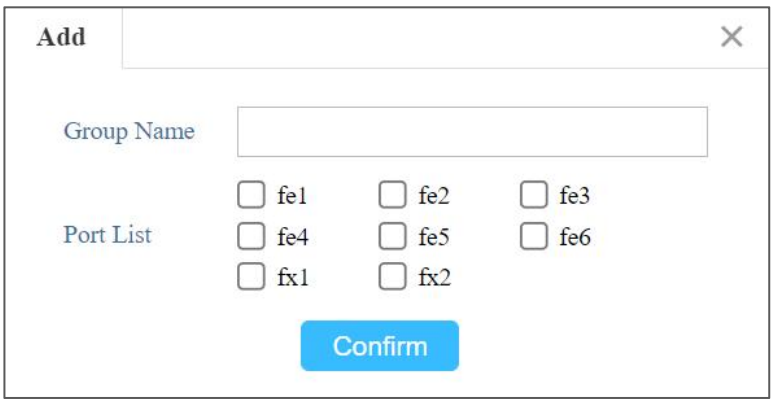
Open in order: "Layer 2 Config > VLAN Configuration > VLAN-config".

Interface Description: View VLAN Configuration

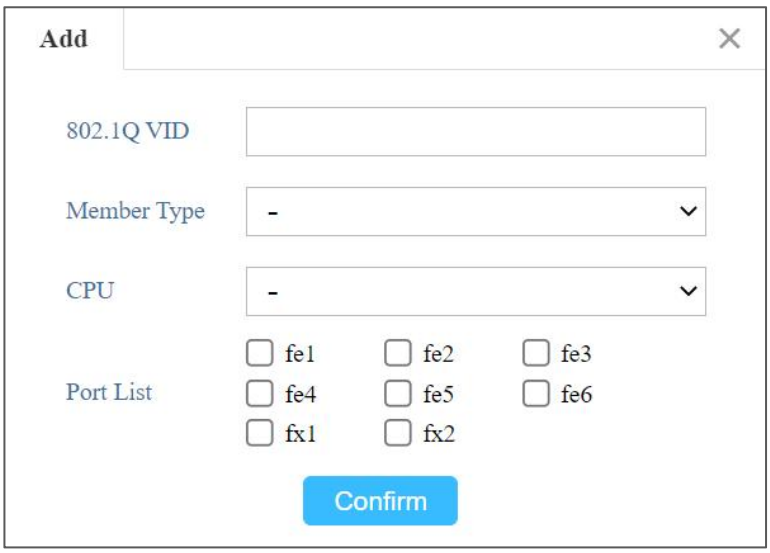
View port-based VLAN interface screenshot:



Interface Description: Add Port-based VLAN



Interface Description: Add 802.1Q-based VLAN



The main element configuration description of Add 802.1Q-based VLAN interface:

Interface Element	Description
802.1Q VLAN	Enter the ID to add the VALN. Note: If the VLAN ID already exists, the original VLAN ID configuration will be overwritten after saving.
Member Type	There are three types of “VLAN ID” for data frames sent out by the port: • Unmodified: when the data frame is sent out from the port, it will recover the “VLAN ID” of accessing to the switch. • Untagged: remove the “VLAN ID” fields when the data frame is sent out from the port,

Interface Element	Description
	• Tagged: reserve “VLAN ID” fields when the data frame is sent out from the port.
CPU	There are three types of “VLAN ID” for data frames sent out by CPU: • Unmodified: when the data frame is sent to CPU, it will recover the “VLAN ID” of accessing to the switch. • Untagged: remove the “VLAN ID” fields when the data frame is sent to CPU. • Tagged: reserve “VLAN ID” fields when the data frame is sent to CPU.
Port List	The device port number check box can be used to configure the port type of the selected port in batch.

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 Address Table

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

View the MAC address, including:

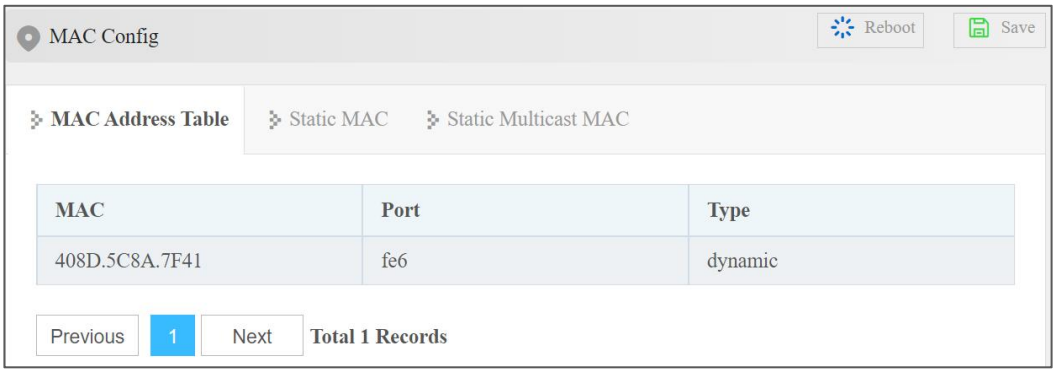
- The data source MAC of the access device learned by the device
- Static unicast MAC
- Static Multicast MAC.

Operation Path

Open in order: "Layer 2 Configuration > MAC Configuration > MAC Address Table".

Interface Description

MAC address table interface is as follows:



Main elements configuration description of MAC address table interface:

Interface Element	Description
MAC	The dynamic MAC that the device have learned or the static unicast or multicast MAC that user has configured.
Port	Access the port number of the source data of the corresponding MAC address.
Type	The type of MAC address, it displays as follows: • Dynamic: dynamic MAC address; • Static: static MAC address.

5.2.2 Static MAC

Function Description

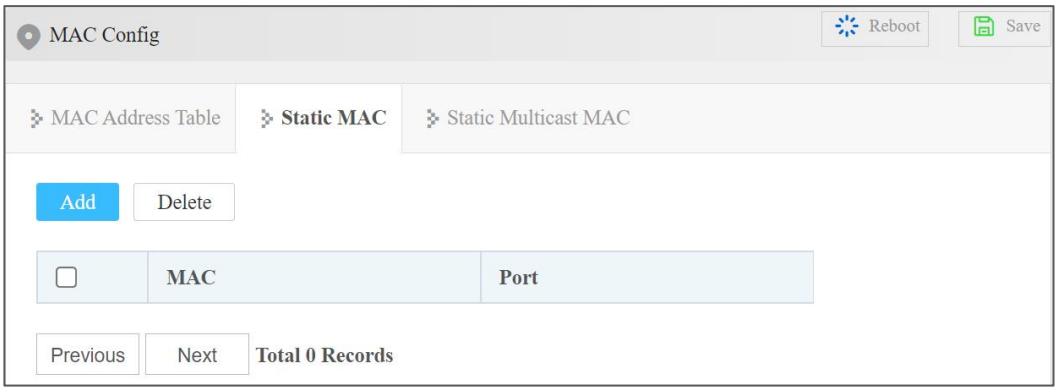
Support manual binding of unicast MAC addresses. The unicast address after binding is static MAC, which will not age.

Operation Path

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

Interface Description

Static MAC interface as follows:



The main element configuration description of static MAC interface:

Interface Element	Description
MAC	Fill in the unicast MAC address that needs to bind the interface, such as 0001.0001.0001.
Port	The Binding Port Number.

Note

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

5.2.3 Static Multicast MAC

Function Description

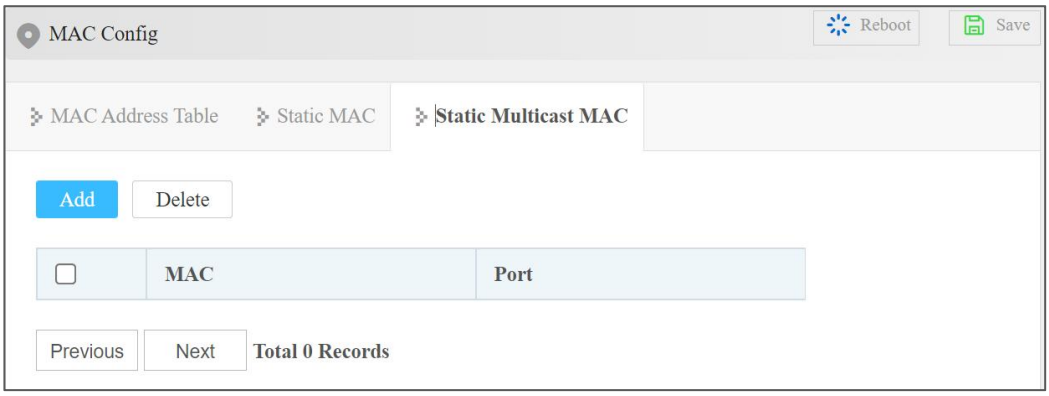
On the static multicast MAC page, you can bind multicast MAC addresses. The bound multicast address is static multicast MAC, which will not age.

Operation Path

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

Interface Description

Static multicast MAC interface as follows:



The main element configuration description of static multicast MAC interface:

Interface Element	Description
MAC	Fill in the multicast MAC address that needs to bind the interface, such as 0100.0001.0001.
Port	The Binding Port Number.

5.3 Spanning-tree Configuration

Notice

Spanning tree and Ring cannot be enabled at the same time. Please disable the enable switch of the Ring before setting the spanning tree.

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

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

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 Global Configuration

Function Description

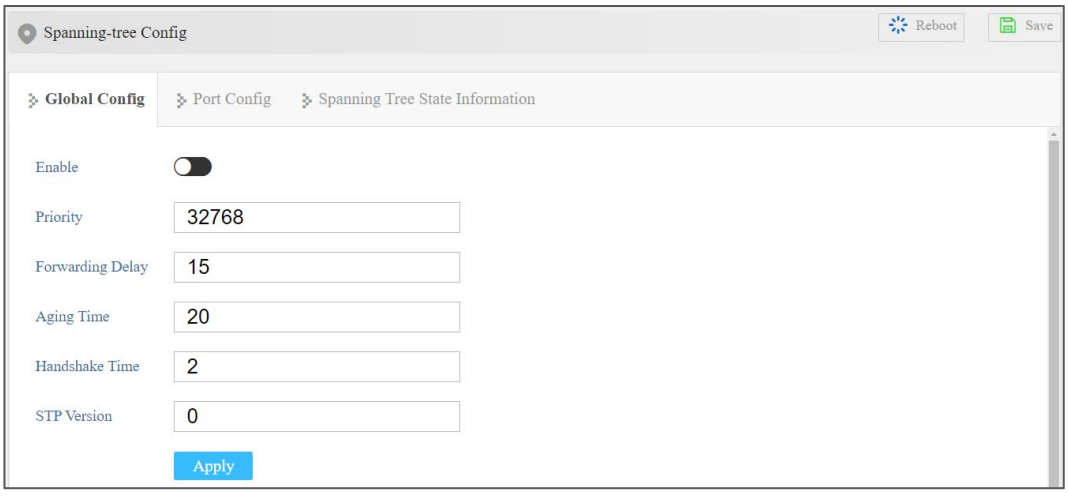
On the "Global Configuration" page, user can configure relative parameters of spanning-tree.

Operation Path

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

Interface Description

Global configuration interface is as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
Enable	Spanning-tree enable switch. Disable by default
Priority	Bridge priority level, defaults to 32768, value range is 0-61440. Note: Smaller the priority level value is, higher the priority level is.

Interface Element	Description
Forwarding Delay	Port state transition delay, defaults to 15S, the value range is 4-30.
Aging Time	The maximum lifetime of the message in the device, defaults to 20S, the value range is 6-40. It's used to determine whether the configuration message times out.
Handshake Time	Message sending cycle,defaults to 2S, the value range is 1-10. Note: The spanning tree protocol sends configuration information every Hello time to check whether the link is faulty.
STP Version	STP revision level, defaults to 0, the value range is 0-1. • 0 means STP Spanning Tree Protocol. • 1 means RSTP (Rapid Spanning Tree Protocol)

5.3.2 Port Configuration

Function Description

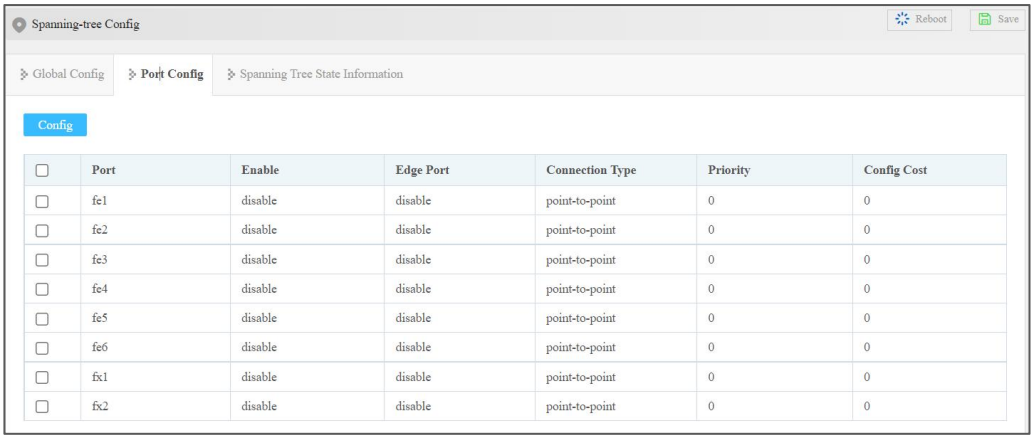
On the "Port Configuration" page, users can enable ports to participate in spanning tree and configure port connection type, path cost, priority and other attributes.

Operation Path

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

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Enable	Status of participating in spanning tree enable switch.
Edge port	Remote port enable switch: • Enable: participate in spanning-tree; • Disable: not participate in spanning-tree.
Connection type	Select port link type: • Auto: Automatic system detection • Point-to-point: Point-to-point link is the connection between switches. • Shared: Non-point-to-point link is the connection between switch and hub.
Priority	Port priority, optional values are: 0/16/32/48/64/80/96/112/128/144/160/176/192/208/224/240. Note: Port priority level in bridge, port priority level is higher when the value is smaller. The higher the priority, the more likely it is to be a root port.
Configuration Cost	The path cost from network bridge to root bridge, defaults to 200000000. Value range: 1-200000000.

5.3.3 State Information of Spanning Tree

Function Description

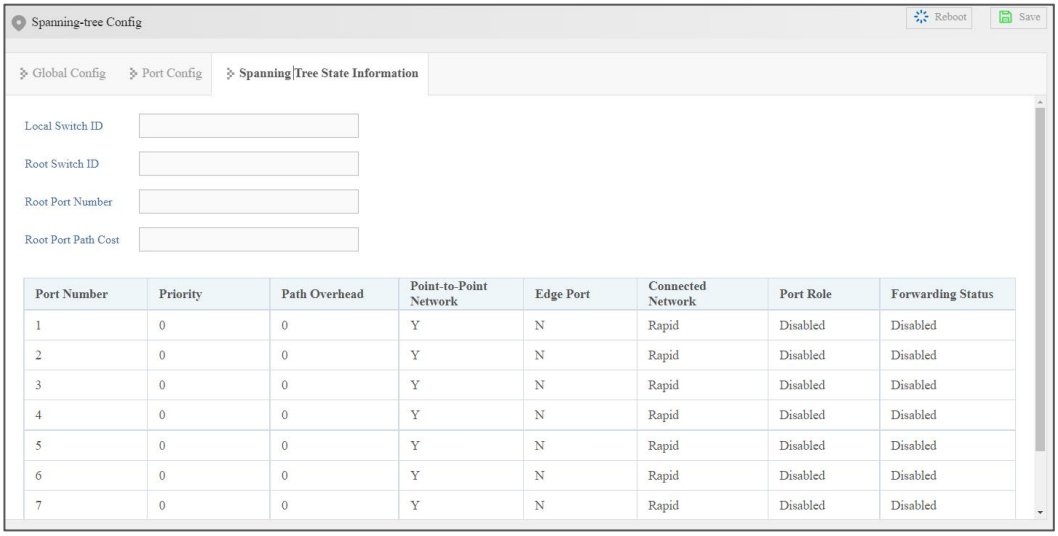
Display information about the root switch and this switch in the spanning tree.

Operation Path

Open in order: "Layer 2 Configuration > Spanning-tree Configuration > Spanning Tree State Information".

Interface Description

The Spanning Tree State Information interface is as follows:



The main element configuration description of Spanning Tree State Information interface:

Interface Element	Description
Local Switch ID	It displays the priority of this switch and MAC address information ID.
Root Switch ID	It displays the priority of the root switch and MAC address information ID.
Root Port Number	The port of the switch, which is not in the root bridge but nearest to it, is in charge of communicating with the root bridge. The path cost from this port to the root bridge is the lowest. When the path costs of multiple ports are the same, the one with the highest priority would be the root port.
Root Port Path Cost	The root cost of a switch is the sum of root port cost and the root cost that data packet goes through all switches. The root cost of root bridge is zero.
Port Number	Display the device port number.
Priority	The priority of ports in network bridge. The values range from 0 to 240. The smaller the value, the higher the port priority. The higher the priority, the more likely it is to be a root port.
Path Overhead	The path cost from network bridge to root bridge.
P2P Network	The directly connected switch port.
Edge Port	The port that directly connects to terminal instead of other switches.

Connected Network	It displays the network protocol of devices with connected ports.
Port Role	Root port, specified port, Alternate port and Backup port.
Forwarding Status	It is divided by whether the port forwards user flow and learns MAC address. • Discarding: neither forward user flow nor learn MAC address; • Learning: doesn't forward user flow but learn MAC address; • Forwarding: forward user flow and learn MAC address; • Listening: neither forward user flow nor learn MAC address; but can receive and send configuration message; • Blocking: port only receives and processes BPDU, doesn't forward user flow; • Disabled: blocked or physically disconnected.

5.4 Ring

Notice

Spanning tree and Ring cannot be enabled at the same time. Please disable the enable switch of spanning tree before setting the Ring.

Ring is an Ethernet Ring network algorithm developed and designed by the company for highly reliable industrial control network applications that require link redundancy backup. Features in Ethernet link redundancy, fast automatic recovery. Ring adopts no master station design. 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 SW-Ring redundant mechanism enables the backup link to quickly recover the network communication.

Function Description

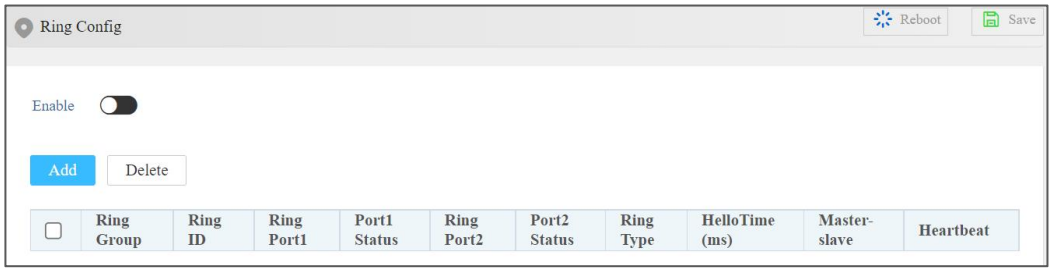
Quickly configure Ring network.

Operation Path

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

Interface Description

Ring network interface as follows:



The main element configuration description of Ring network interface:

Interface Element	Description
Enable	Enable switch, slide to the right to enable the Ring ring network function.
Ring Group	Support ring group 1/2, it can create 2 ring networks at the same time.
Ring ID	When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID. Value range is 1-255. Note: The ring network identification must remain the same in one ring network.
Ring Port 1	The network port 1 on the switch device used to form a ring. Note: When the ring network type is "Couple", port 1 is the "Coupled Port". Coupling port is the port that connects different network identities.
Port1 Status	The current state of Port 1. • block • forward
Ring Port 2	The network port 2 on the switch used to form a ring. Note: • When the ring network type is “Couple”,port 2 is the “console port”. Console port is the port in the chain where two rings intersect. • “Port 1” and “Port 2” cannot be set to the same port, and the port number it sets must be the same as it actually connects

Interface Element	Description
	without sequential order;
Port2 Status	The current state of the port 2. • block • forward
Ring Type	According to the requirement in the scene, user can choose different ring type. • Single: single ring, using a continuous ring to connect all device together. • Couple: couple ring is a redundant structure used for connecting two independent networks. • Chain: chain can enhance user's flexibility in constructing all types of redundant network topology via an advanced software technology. • Dual: Two adjacent rings share a switch; users can carry the same switch on two different networks or two different switching devices on the same network.
HelloTime (ms)	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. Input range is 0~100. Note: When the Hello Time value is 0, it means that no inquiry packet is sent.
Master-slave	Single loop network supports no-master station structure and one-master multi-slave structure. • When all the single-loop devices are slave stations, the single-loop structure is no-master station. • When a single ring device is a master and multiple slave station, one device can be designated as the master device and the other devices as the slave device. One end of the main device of the ring network is the backup link. When the ring network fails, the backup link is enabled from the master station to ensure the normal operation of the network.
Heartbeat	Heartbeat detection mechanism. When this configuration is enabled, the network association will periodically send heartbeat messages to detect whether the corresponding devices are in live state, thus enhancing the reliability of the network. Configurable: • Enable

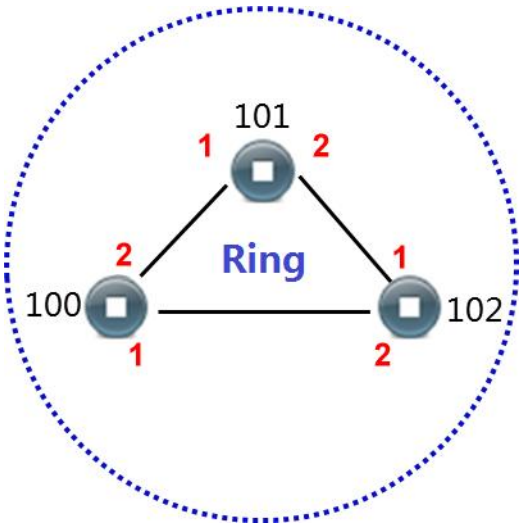
Interface Element	Description
	• Disable

Notice

- The port that has been set to port trunking could not be set as rapid ring port. One port can't belong to multiple ring networks.
- The ID in the same single ring must be the same; otherwise it cannot form a ring and achieve normal communication.
- To ensure the communication of ring network, it's recommended to set the "Type" of ports that have already been set as ring network to "Trunk" and "member relationship" to "Tagged".
- When forming complicated ring networks like tangent ring, please make sure the ID conforms to the unity of single ring network ID. Network ID of different single ring must be different.

5.4.1 Instance: create single ring

For example: create the following single ring:



Instance Analysis

The ring ports of Device 100, 101, and 102 are port 1 and port 2. Therefore, creating single ring is viable. Port 1 and port 2 are set as the ring ports of each device.

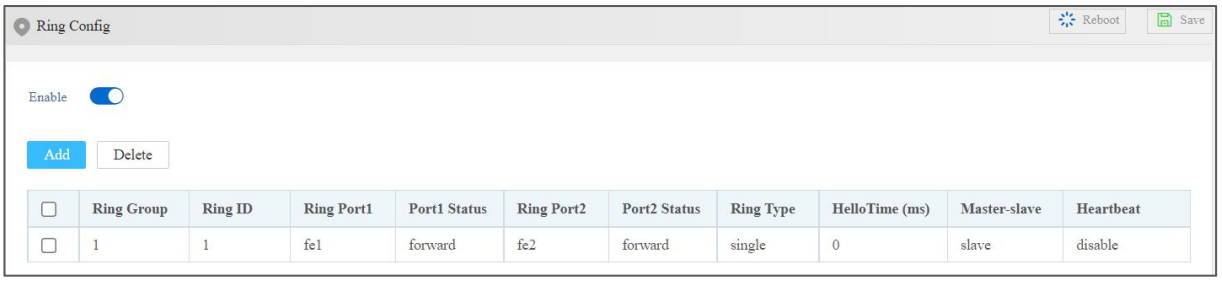
Operation Steps

Configuring Device 100, 101 and 102 in the following steps:

Step 1 Select “Layer 2 Configuration > Ring Configuration”.

Step 2 Turn on the “Enable switch”.

Step 3 Enter “1” into the “Ring ID” textbox of “Group 1”.



Step 4 Set “Port 1” as “fe1” and “Port 2” as “fe2” separately.

Note:

“Port 1” and “Port 2” cannot be set to the same port.

Step 5 Choose “Single” in the drop-down list of “Type” of “Group 1”.

Step 6 Enter “0” into the “HelloTime” textbox of “Group 1”.

Step 7 (For Device 100 and 101) Choose “Slave” in the drop-down list of “Master-slave” of “Group 1”.

Step 8 (For Device 102) Choose “Master” in the drop-down list of “Master-slave” of “Group 1”.

Step 9 Click “OK”.

Step 10 End.

5.5 IGMP Snooping Configuration

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

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

The ways of IGMP Snooping processing different messages:

- IGMP universal group query message: IGMP universal group query message is sent periodically to all hosts and routers in the local network segment to query which multicast group members are in the network segment.
- IGMP report message: the member receives the IGMP universal group query message and responds by the IGMP report message. The member actively sends an IGMP report message to the IGMP query to declare joining the multicast group.
- IGMP leave message: a member running IGMPv2 or IGMPv3 sends an IGMP leave message to notify the IGMP query that it has left a multicast group.

5.5.1 Global Configuration

Function Description

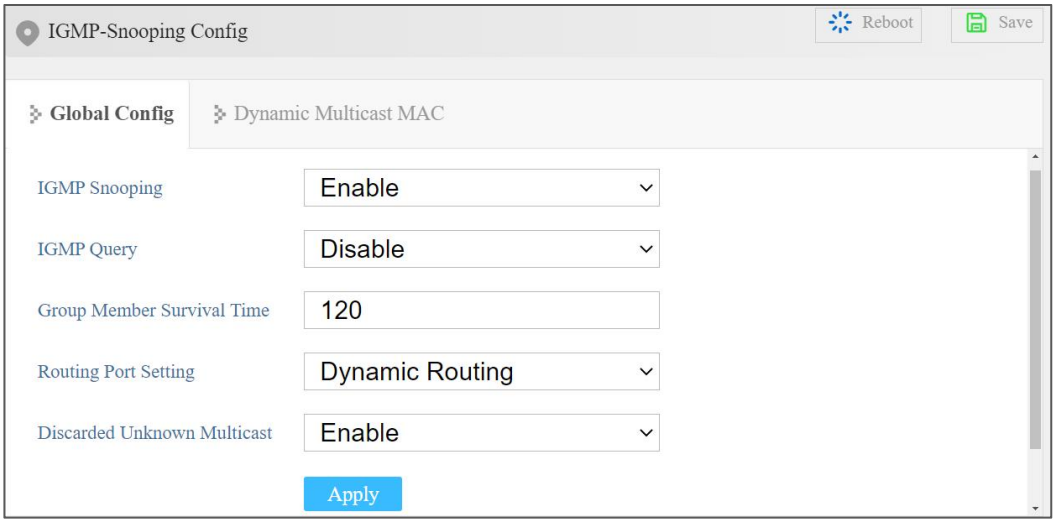
Enable/disable IGMP Snooping; Enable/disable "Drop Unknown Multicast".

Operation Path

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

Interface Description

Global configuration interface is as follows:



The main element configuration description of IGMP Snooping interface:

Interface Element	Description
IGMP Snooping;	The switch of IGMP snooping function, options are: • Enable; • Disable. Note: IGMP snooping means snooping the messages between user host and router, as well as tracking multicast information and the ports that have been applied for.
IGMP Query	The switch of IGMP query, options are: • Enable; • Disable. Note: IGMP query means that router inquiring all hosts in subnet if they join some multicast groups.
IGMP Query Interval	IGMP query interval, unit: second. Note: The time range that can be entered is 60-300s.
Group Member Survival Time	The maximum time that multicast members in device can survive from existence to not receiving any response. Unit: second. Note: • IGMP snooping needs to be enabled before using this function. • The time range of group survival that can be set is 120-300s.
Routing Port Setting	Choose the building mode of routing table, options are: • Dynamic routing, routing ports are dynamically acquired though switch.

	• Static routing, check the box of port in “port list” as routing port.
Port List	All ports of the device. Note: This item is displayed when the routing port is set to static routing.
Discarded Unknown Multicast.	Discard unknown multicast function enable switch, options: • Enable; • Disable. Note: Unknown multicast refers to multicast in which all hosts in the router subnet have not joined.

Note

- You need to set multicast source and port in one VLAN first to enable IGMP Snooping function.
- Multiple IGMP inquirers should be avoided in network lest cause waste of resources. Please choose all ports if the forwarding relationship of unknown multicast group is uncertain.

5.5.2 Static Multicast MAC

Function Description

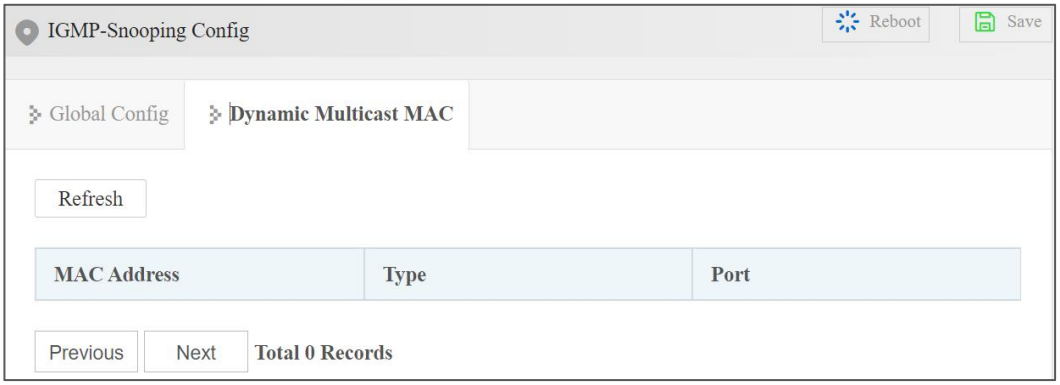
Display the dynamic multicast information received by the device interface.

Operation Path

Open in order: " Layer 2 Configuration > IGMP Snooping Configuration > Dynamic Multicast MAC".

Interface Description

The Dynamic Multicast MAC interface is as follows:



Main element configuration description of Dynamic Multicast MAC interface:

Interface Element	Description
MAC Address	The multicast address received by the interface.
Type	Multicast type: • dynamic • static
Port	Ethernet port.

5.6 Port Loopback Detection

Function Description

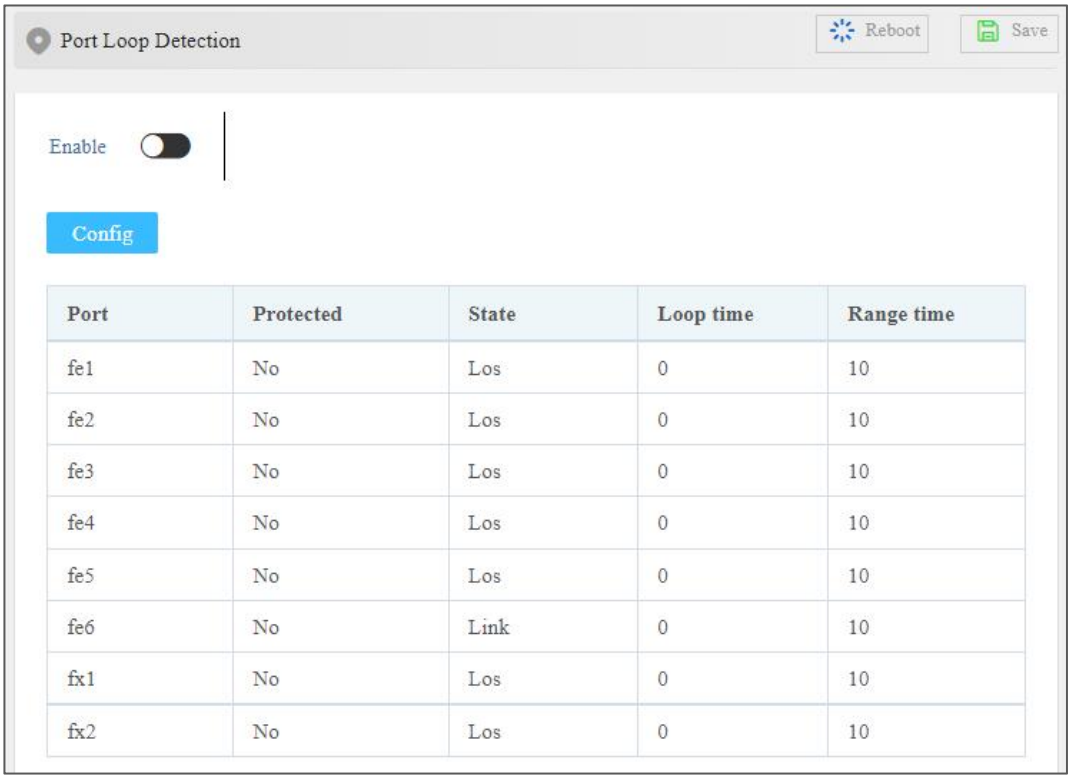
Loop protection can be configured to avoid ring network storm.

Operation Path

Open in order: "Layer 2 Configuration > Port Loop Detection".

Interface Description

Screenshot of Port Loopback Detection interface:



Port	Protected	State	Loop time	Range time
fe1	No	Los	0	10
fe2	No	Los	0	10
fe3	No	Los	0	10
fe4	No	Los	0	10
fe5	No	Los	0	10
fe6	No	Link	0	10
fx1	No	Los	0	10
fx2	No	Los	0	10

Main elements configuration descriptions of Loop Protection interface:

Interface Element	Description
Enable	Enable or disable port loop detection.
Port	Displays the port number of the device.
Protected	The state of the port protected by a loop. After enabled, when there is a port self-loop or a port loop, the loop can be quickly disconnected, and the port status can be set to blocking or forwarding to avoid network storms. Notice: The loop port cannot be set as a loop detection port.
State	The connection status of this port, values are: • Los: the port is physically disconnected • Link: The port is not looped and the port is connected. • Block: The port is enabled with loop protection function, and the loop has been detected, so it has entered the protection state. • Forward: The port is connected, loop protection is enabled and no loop is detected.
Loop Time	Time interval for detection after loop formation. Value range is 1-600, default value: 300, unit: seconds.
Range Time	Time interval before loop formation, ranging from 1-60,

	default value: 10, unit: second.

5.7 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.

5.7.1 MRP Configuration

Function Description

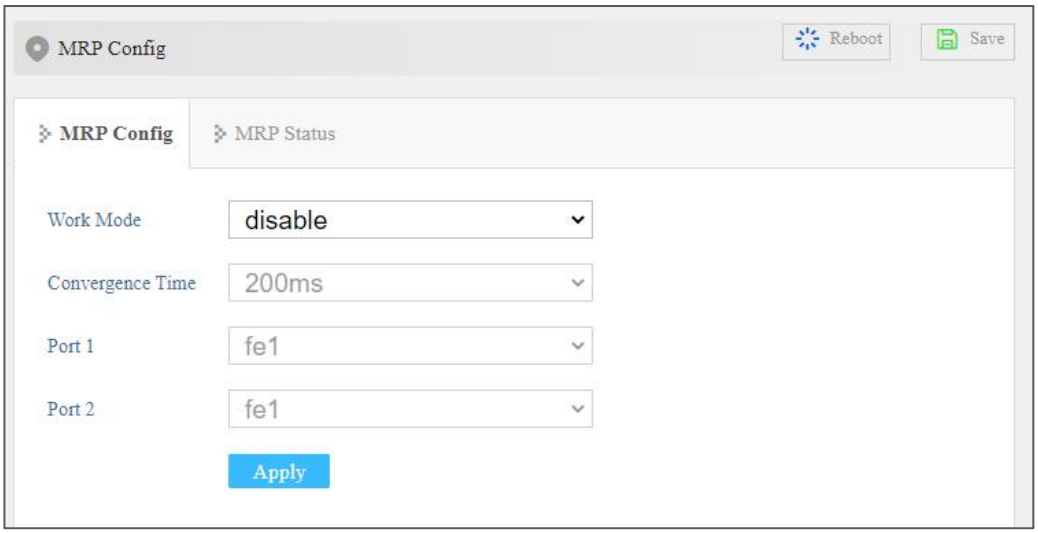
Enable MRP ring network and configure ring network parameters.

Operation Path

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

Interface Description

MRP configuration interface is as follows:



The main element configuration description of MRP configuration interface:

Interface Element	Description

Interface Element	Description
Work Mode	The working modes of the device are as follows: • Disable: disable MRP function • MRM: media redundancy manager • MRC: media redundancy client
Convergence Time	When the MRP ring network is disconnected, the ring network reconfiguration time. The options are as follows: • 200ms • 500ms Note: When the working mode is MRC, the convergence time is fixed at 200ms and cannot be configured at 500 ms.
Port1	Select port as port 1 of MRP ring network.
Port2	Select port as port 2 of MRP ring network.

5.7.2 MRP Status

Function Description

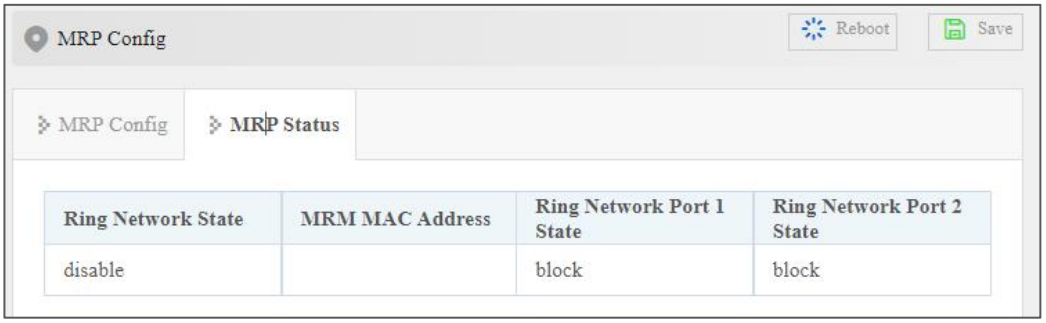
View MRP ring network status.

Operation Path

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

Interface Description

MRP State interface is as follows:



The main element configuration description of ring network state interface:

Interface Element	Description

Interface Element	Description
Ring Network State	The MRP ring network status can be displayed as follows: • Enable • Disable
MRM MAC Address	The MAC address of MRM device in this ring network.
Ring Network Port1 State	The ring network status of device ring network port 1 is displayed as follows: • Forward: port is forwarding • Block: the port is blocking
Ring Network Port2 State	The ring network status of device ring network port 2 is displayed as follows: • Forward: port is forwarding • Block: the port is blocking

6 Wireless

6.1 User List

Function Description

View the wireless clients or wireless devices accessing the wireless network of this device.

Operation Path

Open in order: "Wireless > User List".

Interface Description

User list interface is as follows:

The main element configuration description of user list interface:

Interface Element	Description
MAC	The MAC address of wireless client connected to the wireless network of this device currently.
Signal	The signal strength of wireless client connected to the wireless network of this device currently. The unit is dBm, the larger the value, the stronger the signal.

Interface Element	Description
Upstream	The upload flow of wireless client connected to the wireless network of this device currently.
Downstream	The download flow of wireless client connected to the wireless network of this device currently.
Online Time	The online time of wireless client connected to the wireless network of this device currently.

6.2 Configuration

6.2.1 Network Bridge Settings

Function Description

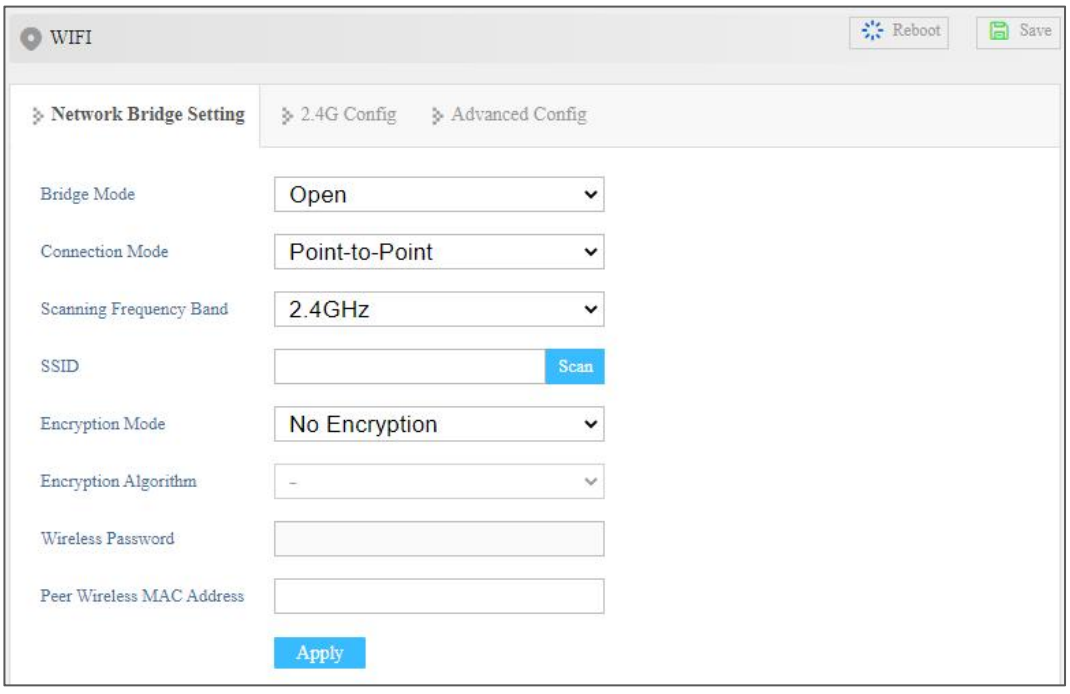
The default state of this device is AP mode. On the network bridge configuration page, select "Bridge Mode" as "On", and the device will switch to bridge mode.

Operation Path

Open in order: " Wireless > Configuration > Network Bridge Setting".

Interface Description

Nerwork bridge settings interface is as follows:



The network bridge setting interface elements are described as follows:

Interface Element	Description
Bridge Mode	Bridge mode is disabled by default and can be selected by enabling or disabling the radio box.
Connection Mode	Connection mode of the device and opposite terminal wireless device, options as follows: • Point to point: it's used for connecting the appointed wireless device; • Roam: Switching among wireless devices with the same SSID.
Roaming signal threshold	Textbox of roaming signal threshold. • When the signal strength RSSI falls below this threshold, roaming will be triggered. • When the signal strength RSSI is higher than this threshold, roaming will not be triggered. Note: This parameter is visible only when the "Connection Mode" is selected as "Roaming".
Scanning Frequency Band	Scanning frequency band. Options are as follows: • 2.4GHz
SSID	SSID name of the opposite device wireless network. Note: You can also select the wireless devices that need to be bridged through the scan button.
Encryption Mode	Encryption mode of opposite wireless network, the options are as follows: • No encryption; • WPA: WiFi Protected Access. When the wireless authentication method is personal edition, encryption method is PSK (pre-shared key); when the wireless authentication method is enterprise edition, encryption method is 802.1X authentication which use RADIUS server and EAP to authenticate. • WPA2: upgrade version of WPA, supports AES (Advanced Encryption Standard), and provides higher security for WLAN. • WPA-MIXED: the mixed-mode of WPA, is compatible with both WPA and WPA2 encryptions.

Interface Element	Description
	• WEP-SHARED: a kind of Wired Equivalent Privacy, it adopts shared key authentication encryption mode. Note: • WPA2 is a more powerful and secure encryption method than WEP-SHARED, and it is recommended to use this encryption method. • Under "WIFI > Configuration > Advanced Configuration", you can switch between personal and enterprise authentication methods.
Encryption Algorithm	Password of opposite wireless network. Wireless network supports different encryption algorithms when it using WPS, WPA2 or WPA-MIXED encryption method, options as follows: • AES(CCMP): CCMP(Counter Mode with CBC-MAC Protocol) uses AES(Advanced Encryption Standard) encryption algorithm. • TKIP: Temporal Key Integrity Protocol, provides more secure protection mechanism than WEP encryption. • TKIP/AES: compatible with both TKIP and AES encryption algorithm.
Wireless Password	Password of opposite device wireless network.
BSSID	MAC address of opposite device wireless network. Note: The parameter is visible when the connection mode is "Point to point".
Bridge information	Display bridging information.
Bridging status	Display bridging status.

6.2.2 2.4G Configuration

Function Description

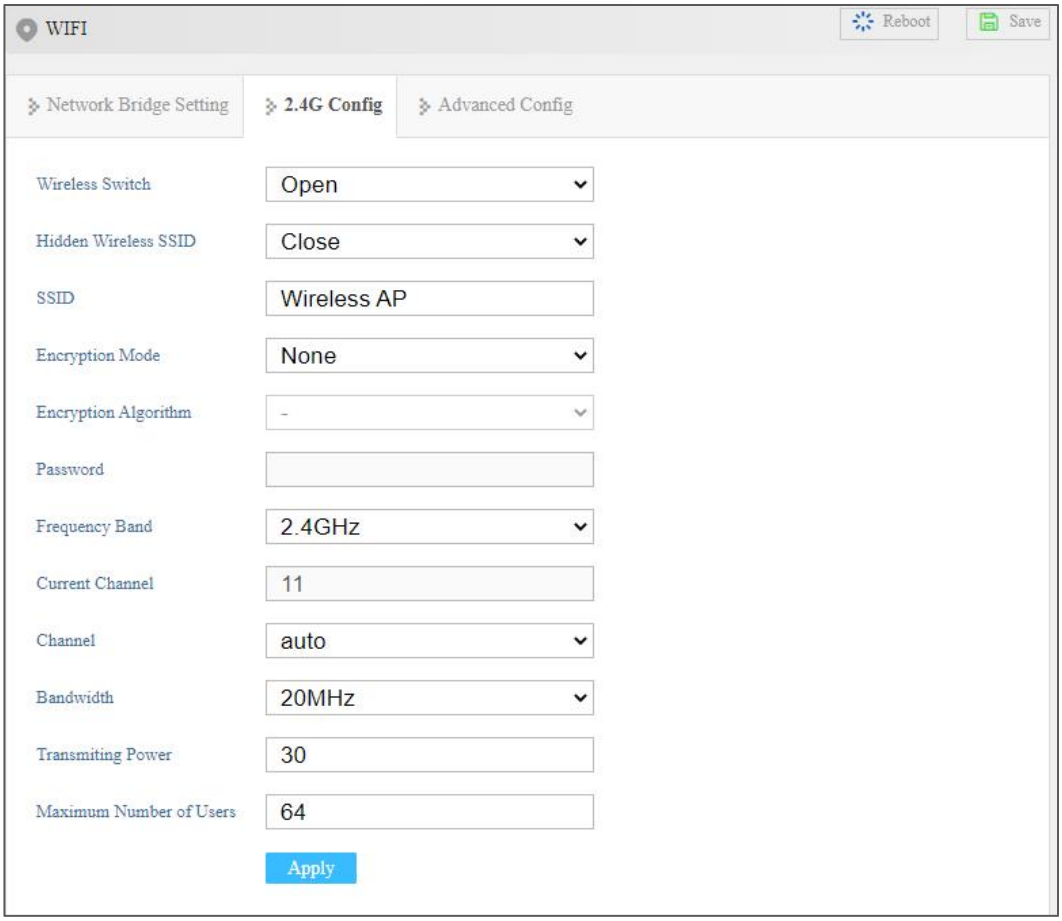
Set 2.4G wireless parameters.

Operation Path

Open in order: "Wireless > Configuration > 2.4G Configuration".

Interface Description

The 2.4G configuration interface is as follows:



Element description of 2.4G configuration interface.

Interface Element	Description
Wireless Switch	Enable/disable the wireless access point in this frequency band.
Hidden Wireless SSID	Enable/disable hidden SSID function. After it is enabled, the wireless client will not be able to automatically search for the WiFi name, and it is necessary to manually add the WiFi name for access authentication.
SSID	SSID name of wireless network of this device, it supports 1-32 characters.
Encryption Mode	The encryption method of wireless network of this device. Options are as follows: • No encryption; • WPA: WiFi Protected Access. When the wireless

Interface Element	Description
	authentication method is personal edition, encryption method is PSK (pre-shared key); when the wireless authentication method is enterprise edition, encryption method is 802.1X authentication which use RADIUS server and EAP to authenticate. • WPA2: upgrade version of WPA, supports AES (Advanced Encryption Standard), provides higher security for WLAN. • WPA-MIXED: the mixed-mode of WPA, is compatible with both WPA and WPA2 encryptions. • WEP-SHARED: a kind of Wired Equivalent Privacy, it adopts shared key authentication encryption mode. Note: • WPA2 is a more powerful and secure encryption method than WEP-SHARED, and it is recommended to use this encryption method. • Under WIFI > Configuration > Advanced Configuration, you can configure personal and enterprise authentication methods.
Encryption Algorithm	Encryption algorithm of wireless network of this device. Wireless network supports different encryption algorithms when it using WPS, WPA2 or WPA-MIXED encryption method, options as follows: • AES(CCMP): CCMP(Counter Mode with CBC-MAC Protocol) uses AES(Advanced Encryption Standard) encryption algorithm. • TKIP: Temporal Key Integrity Protocol, provides more secure protection mechanism than WEP encryption. TKIP/AES: compatible with both TKIP and AES encryption algorithm.
Password	Password of wireless network of this device, it supports 5 or 8-32 characters. Note: Wireless password doesn't support blanks. It represents no encryption for wireless network if no password is filled in.
Current Xhannel	Displays the current working channel of this device. Note: If the working mode of the device is AP, the current channel is the working channel of the opposite wireless network.
Channel	Working channel of wireless network, default "auto"

Interface Element	Description
	self-adaptation, options as follows: • Auto: channel self-adaptation; • 1: main frequency band 2412Hz, frequency range 2401~2423Hz; • 2: main frequency band 2417Hz, frequency range 2406~2428Hz; • 3: main frequency band 2422Hz, frequency range 2411~2433Hz; • 4: main frequency band 2427Hz, frequency range 2416~2438Hz; • 5: main frequency band 2432Hz, frequency range 2421~2443Hz; • 6: main frequency band 2437Hz, frequency range 2426~2448Hz; • 7: main frequency band 2442Hz, frequency range 2431~2453Hz; • 8: main frequency band 2447Hz, frequency range 2436~2458Hz; • 9: main frequency band 2452Hz, frequency range 2441~2463Hz; • 10: main frequency band 2457Hz, frequency range 2446~2468Hz; • 11: main frequency band 2462Hz, frequency range 2451~2473Hz; • 12: main frequency band 2467Hz, frequency range 2456~2478Hz, this frequency band is not open in America, so it's temporarily unavailable; • 13: main frequency band 2472Hz, frequency range 2461~2483Hz, this frequency band is not open in America, so it's temporarily unavailable; Note: • In order to improve the network performance, please choose unused channel in the device working environment. • If the working mode of the device is AP, the channel is grayed out and cannot be edited.
Bandwidth	Wireless network channel bandwidth, options are as follows: • 20MHz

Interface Element	Description
Transmitting Power	The wireless signal transmission power of device ranges from 1 to 1~25dBm. Note: • The larger the transmission power, the stronger the transmission ability and the farther the transmission distance, but the excessive transmission power is easy to produce other interference. • Different device has different transmitted power range.
Maximum Number of Users	Maximum client number of the device wireless signal, value range 1-64, when the value is 64, it represents the unlimited connected clients number.

6.2.3 Advanced Configuration

Function Description

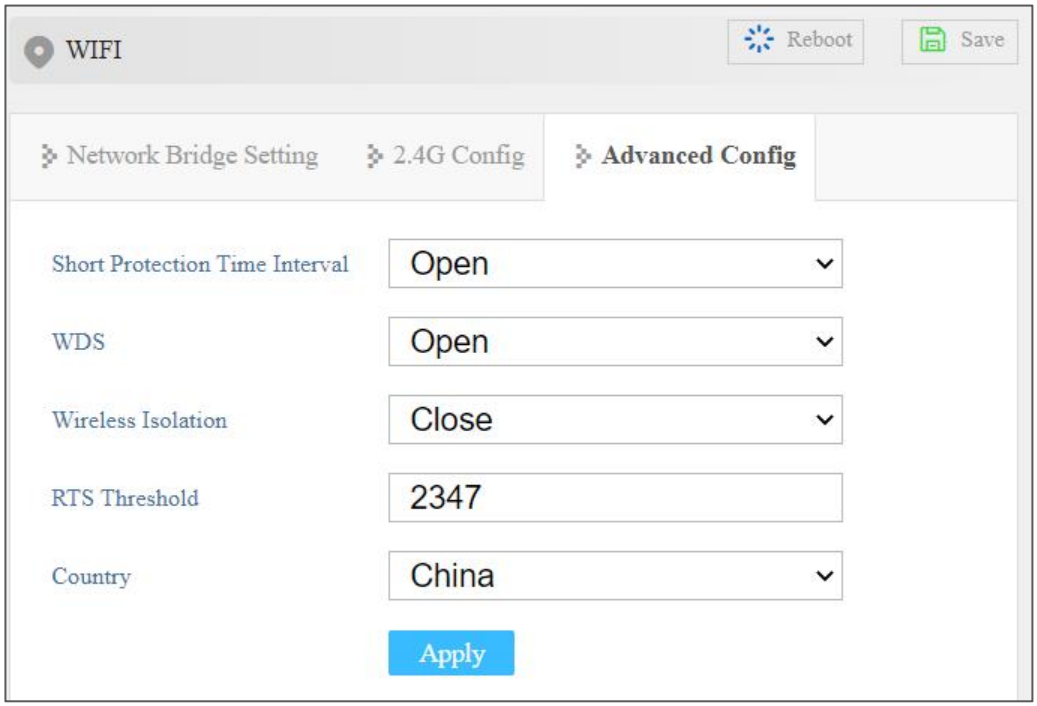
Functions such as Short Guard Interval, wireless multimedia, WDS and wireless isolation can be enabled.

Operation Path

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

Interface Description

The Advanced Configuration interface is as follows:



The advanced configuration interface is described as follows:

Interface Element	Description
Short Protection Time Interval	Check box for Short GI(Short Guard Interval) protection interval. Enabling the function can reduce the gap between two data packets to 400ns, and improve the data transmission speed. Uncheck: after disabling the function, the transmission interval of data packet defaults to 800ns. Note: Under high signal strength and low latency, this function can be enabled to improve nearly 10% handling capacity.
WDS	WDS (Wireless Distribution System), this function is used for bridging multiple WLAN.
Wireless Isolation	Wireless user isolation, it's used for isolating the wireless clients connected to the device wireless network with same SSID, defaults to disabled. After enabling the wireless isolation function, two wireless clients connected to the same SSID can't mutually access, and this function can further enhance the wireless network security.
RTS Threshold	Data packet RTS (Request to Send) threshold, value range 0-2347, defaults to 2347. • RTS threshold = 0: it needs to detect whether there exists collision only if the data packet is sent out; AP will

Interface Element	Description
	send RTS signal; • 0 < RTS threshold < 2347: when the length of data packet surpasses RTS threshold, the device wireless terminal will send RTS signal to avoid signal conflict; • RTS threshold = 2347: the device wireless terminal won't send RTS signal. Note: • As for the wireless nodes in different wireless detection range of AP range, collision will occur when the nodes send out signals; RTS function can avoid the collision. • The device will send RTS to destination station for negotiation when the length of data packet surpasses RTS threshold. After receiving RTS frame, the wireless station will send a CTS (Clear to Send) frame to response the device, which represents the two stations can conduct wireless communication.
Country	Applied countries and regions of wireless network, the options are as follows: • China • USA Note: Different country opens different channels.

6.3 Update Driver

Function Description

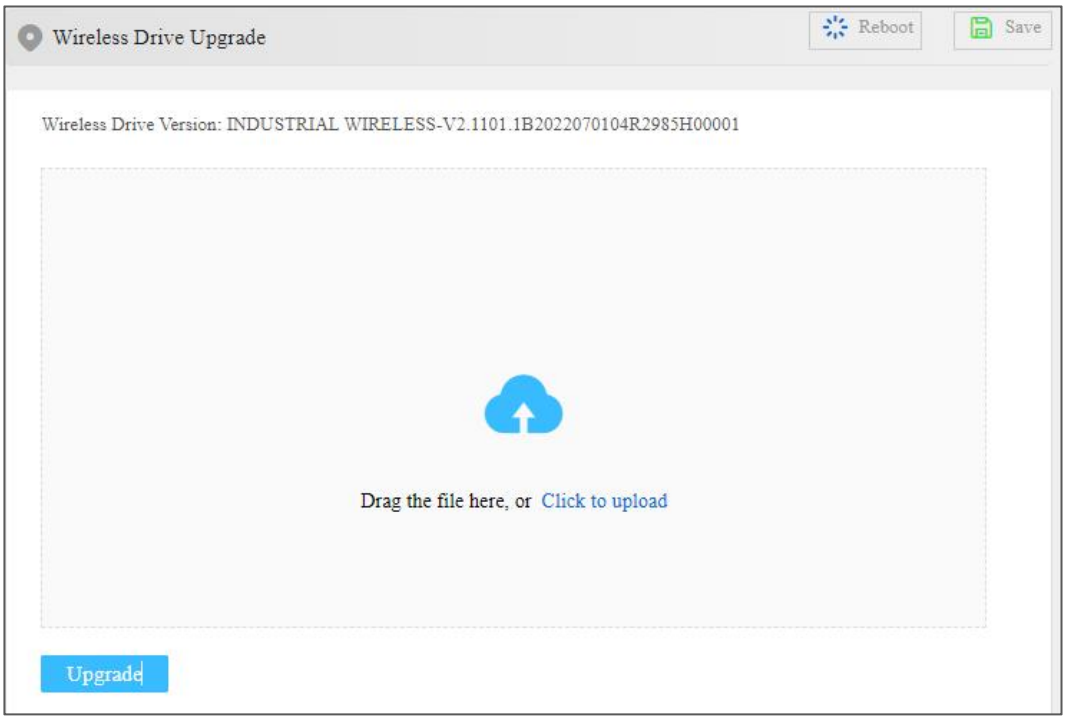
Update and upgrade the device's wireless driver through the web page, and the configuration of the device after successful upgrade will remain unchanged, but the firmware version information will change.

Operation Path

Open in order: “Wireless > Update Driver”.

Interface Description

The driver upgrade interface is as follows.



Main elements configuration descriptions of driver upgrade interface:

Interface Element	Description
Upgrade	Drag the upgrade file into the upgrade box or click "Upgrade" to select the upgraded file in the format of ".bin". Notice: It takes a while during the upgrade process. Do not power off the device.

7 Network Configuration

7.1 SNMP Configuration

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

7.1.1 View

Function Description

Add/delete SNMP view.

Operation Path

Open in order: “Network Configuration > SNMP Configuration > View”.

Interface Description

View interface as below:

The main element configuration description of view interface:

Interface Element	Description
Name	SNMP view name definition, support 32 characters input including a-z and 0-9.
OID	Node location information of MIB tree where the device resides. Note: • OID object identifier, a component node of MIB, uniquely identified by a string of numbers that represent the path. • The information of OID could be viewed via the third-party software MG-SOFT MIB Browser.
Mode	Node OID dealing method, options as below: • Included: It contains all objects under the node subtree; • Excluded: Eliminate all objects beyond the node subtree.

7.1.2 Community

Function Description

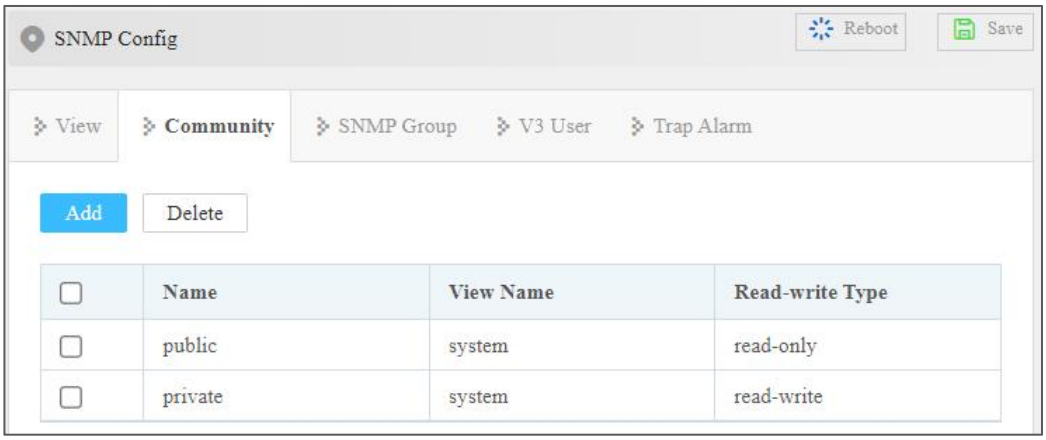
Add SNMP community, and define MIB view that community can access, set MIB object access privilege of community as write privilege or read privilege.

Operation Path

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

Interface Description

Community interface as below:



The main element configuration description of community interface:

Interface Element	Description
Name	Group name, including numbers or letters, with a length of no more than 32 characters.
View Name	SNMP view name definition, which has been configured in the View page.
Read-write Type	Read-write privilege view name selection, options:. • Read-only • Read-write

7.1.3 SNMP Group

Function Description

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

Operation Path

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

Interface Description

SNMP Group interface as follows:

Main elements configuration description of SNMP Group interface:

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

7.1.4 V3 User

Function Description

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

between NMS and Agent to prevent eavesdropping. It adopts authentication and encryption function to provide higher security for the communication between NMS and Agent.

Operation Path

Open in order: "Network Configuration > SNMP Configuration > V3 Users".

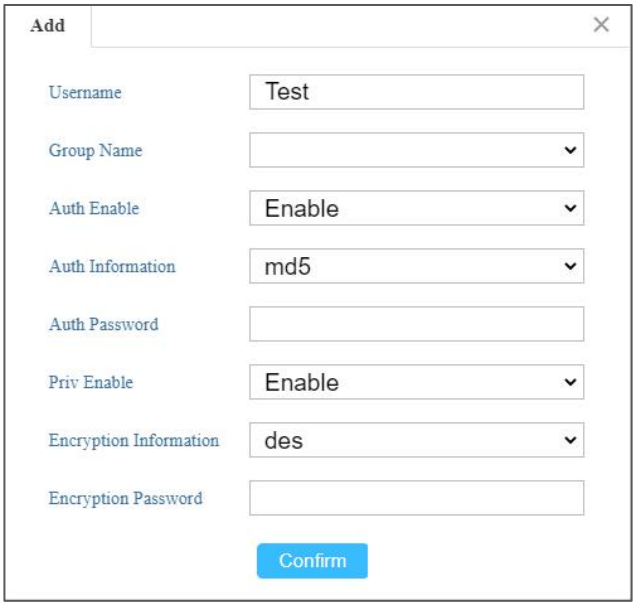
Interface Description

V3 user interface as follows:

The main element configuration description of V3 user interface:

Interface Element	Description
Username	SNMP v3 user name definition, can only contain numbers, letters, or @_! , no longer than 32 characters.
Group Name	Group name, ranging from 1 to 32 bytes. Note: Group name must be created snmp group, and only created group can create SNMP v3 users.
Security Mode	Whether to authenticate and encrypt the message, values: • auth: indicates that the message is authenticated but not encrypted; • noauth: indicates that the message is neither authenticated nor encrypted; • priv: indicates that the message is authenticated and encrypted.
Authentication Mode	Authentication mode type, acceptable value: • Md5: Information abstract algorithm 5; • Sha: Secure hash algorithm.
Encryption Mode	V3 user data encryption algorithm, options as follows: • Des: Adopt data encryption algorithm; • Aes: Adopt advanced encryption standard.

V3 User: “Add” Interface Description



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

Interface Element	Description
Username	SNMP v3 user name definition, can only contain numbers, letters, or @_! , no longer than 32 characters.
Group Name	The drop-down list of SNMP group name.
Auth Enable	Indicate that security mode requires authentication. If “disable” is selected, the default is no authentication, no encryption mode.
Auth Information	Authentication information type, acceptable values: • Md5: Information abstract algorithm 5; • Sha: Secure hash algorithm.
Auth Password	Authentication password, character string, length greater than or equal to 8 bytes.
Priv Enable	Indicate that security mode requires encryption.
Encryption Information	V3 user data encryption algorithm, options as follows: • Des: Adopt data encryption algorithm; • Aes: Adopt advanced encryption standard.
Encryption Password	Encrypted password, character string, length greater than or equal to 8 bytes.

7.1.5 Trap Alarm

Function Description

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

Operation Path

Open in order: "Network Configuration > SNMP Configuration > Trap Alarm".

Interface Description

Trap alarm interface is as follows:

The main element configuration description of Trap alarm interface:

Interface Element	Description
Address	IP address of SNMP management device, used for receiving alarm information, such as PC.
Mode	Managed device that sends an active alert to the NMS. After the inform alarm is sent out, it will wait for the confirmation message from NMS, and if no confirmation message is received, it will resend the Inform message; Trap message has no confirmation process. The types of alarm messages include:

Interface Element	Description
	• trapV1: send snmpV1 trap • trapV2c: send snmpV2c trap • trapV3: send snmpV3 trap • informV2c: send snmpv2 inform • informV3: send snmpV3 inform
Group Name	Community name or snmpv3 user name.

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.

7.2.1 Current Configuration

Function Description

Enable LLDP and configuration.

Operation Path

Open in order: “Network Configuration > LLDP Configuration > Global Configuration".

Interface Description

The current configuration interface is as follows:

Main elements configuration description of the current configuration interface:

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

7.2.2 Port Configuration

Function Description

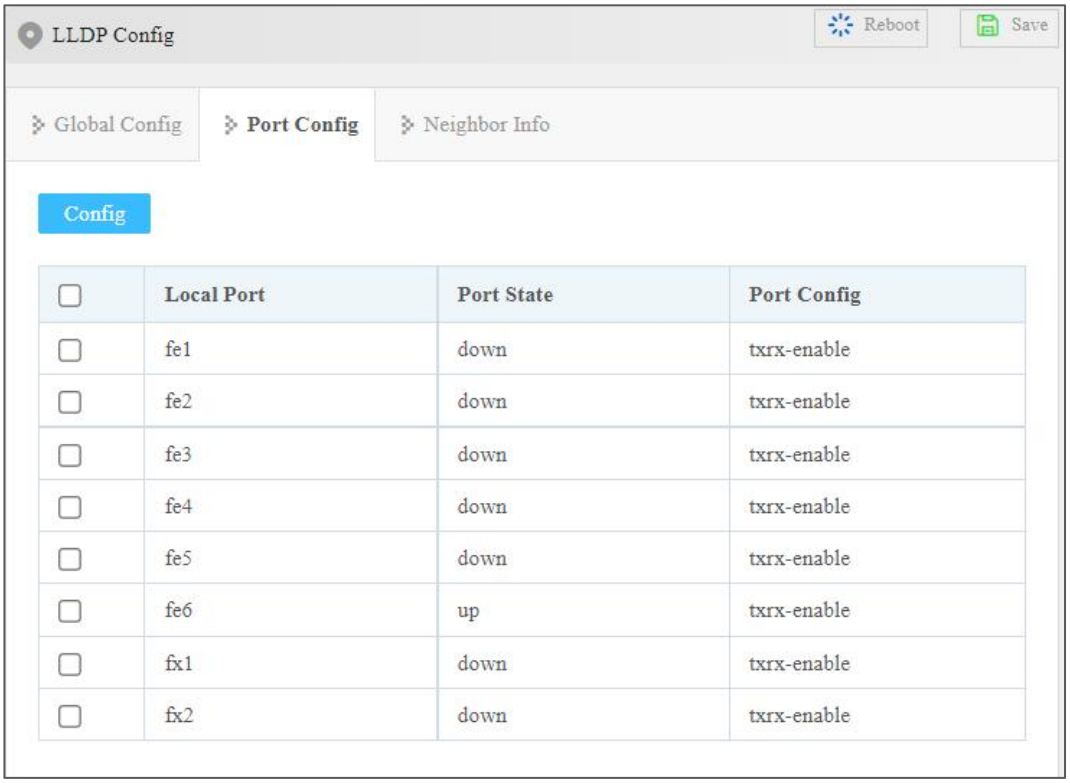
Configure the LLDP work mode of the port.

Operation Path

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

Interface Description

Check port configuration interface as below:



The main element configuration description of port configuration interface:

Interface Element	Description
Local Port	The corresponding port name of the device Ethernet port.
Port State	Port connection status: • UP • down
Port Configuration	The options of LLDP working modes of device port are as follows: • tx-enable: working mode is Tx, only sending and not receiving LLDP message. • rx-enable: working mode Rx, only receiving and not sending LLDP message. • txrx-enable: working mode is TxRx, both sending and receiving LLDP message. • disable: working mode Disable, neither receiving nor sending LLDP message. Note: When global LLDP is enabled, the work mode of LLDP is TxRx by default.

7.2.3 Neighbor Information

Function Description

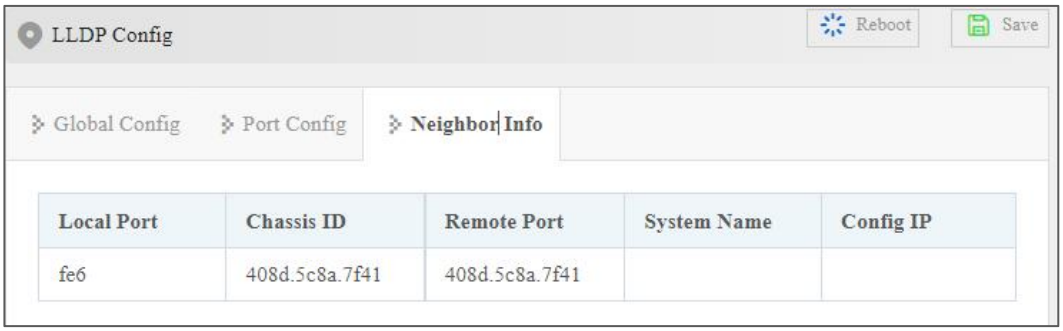
On the "Neighbors Information" page, user can look over the relative information of neighbors.

Operation Path

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

Interface Description

Neighbor information interface as follows:



Main elements configuration description of neighbor information interface:

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

7.3 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.

7.3.1 DHCP Switch

Function Description

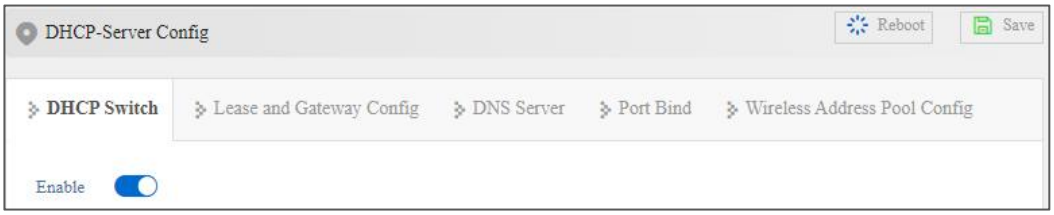
On the "DHCP Switch" page, user can enable/disable DHCP.

Operation Path

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

Interface Description

DHCP switch interface is as follows:



The main element configuration description of DHCP switch configuration interface.

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

7.3.2 Lease and Gateway Configuration

Function Description

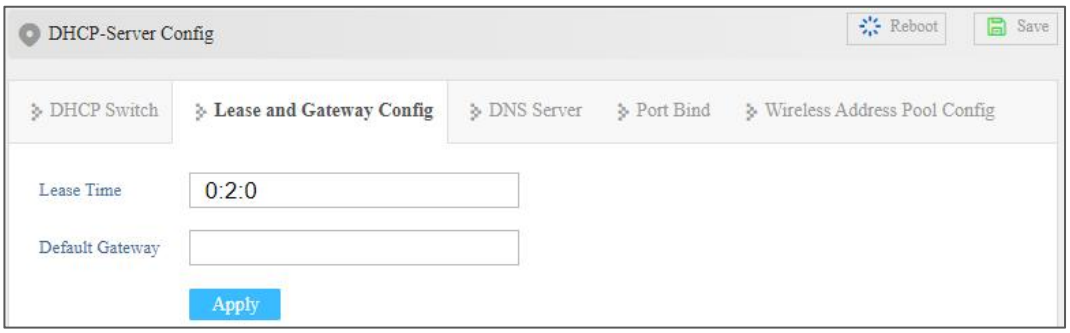
Set the valid time and default gateway for the IP address of the client.

Operation Path

Open in order: “Network Configuration > DHCP-Server Configuration > Lease and Gateway Configuration".

Interface Description

The Lease and Gateway Configuration interface is as follows:



The main element configuration description of Lease and Gateway Configuration interface:

Interface Element	Description
Lease time	IP address utilization valid time of client, format: day, hour, minute, range is 0-30 day, 0-24h and 0-60m, which are separated by ":". Note: When the time of ip address obtained by dhcp client reaches the lease time, it needs to renew it otherwise the ip address would be invalid and dhcp client needs to request ip address again.
Default Gateway	Default client gateway address, example: 255.255.255.0.

7.3.3 DNS Server

Function Description

Configure the DNS server address. Parse the domain name to be visited to an IP address, realizing domain name access network.

Operation Path

Open in order: "Network Configuration > DHCP-Server Configuration > DNS Server".

Interface Description

Server configuration interface as follows:

The main element configuration description of server configuration interface:

Interface Element	Description
DNS Server 1	IP address of domain name resolution server 1.
DNS Server 2	IP address of domain name resolution server 2.

7.3.4 Port Binding

Function Description

Bind the relationship of IP addresses assigned by ports.

Take Device A and Device B as examples.

If DHCP Server function is enable on Device A and two static address allocation tables are set:

- 192.168.1.19 corresponds to Port 1;
- 192.168.1.20 corresponds to Port 2.

After the function of automatically obtaining the IP address is enabled on Device B,

- If Device A is connected to Device B through port 1, Device B can automatically obtain the IP address of 192.168.1.19;
- If Device A is connected to Device B through port 2, Device B can automatically obtain the IP address of 192.168.1.20.

Operation Path

Open in order: “Network Configuration > DHCP Server Configuration > Port Binding".

Interface Description

Port binding configuration interface as follows:

The main element configuration description of port binding interface:

Interface Element	Description
IP Address	IP address that DHCP address pool distributes, the IP addresses that client gains in the port.
Port	The corresponding port name of the device Ethernet port.

7.3.5 Wireless Address Pool Configuration

Function Description

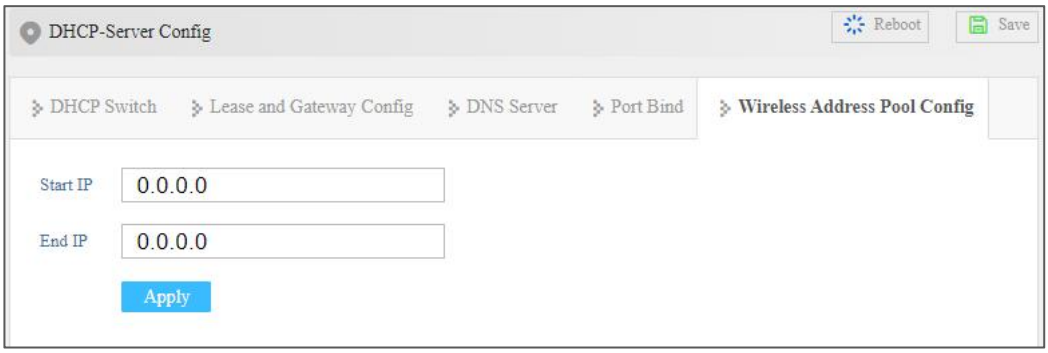
Set the IP address range assigned to wireless clients.

Operation Path

Open in order: “Network Configuration > DHCP-Server Configuration > Wireless Address Pool Configuration".

Interface Description

Wireless Address Pool interface is as follows:



The main element configuration description of client list interface:

Interface Element	Description
Start IP	Start IP address allocated to wireless client.
End IP	End IP address allocated to wireless client.

7.4 Access Control

7.4.1 Port Authentication

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

Function Description

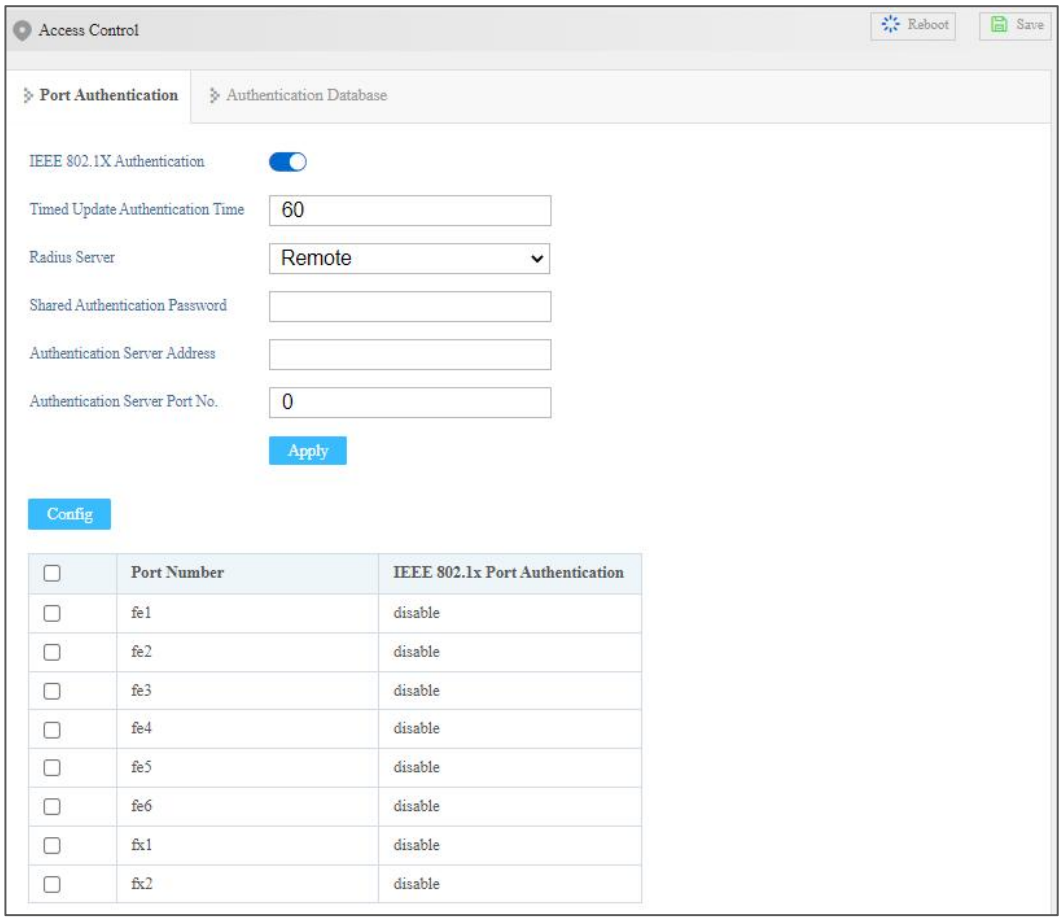
Enable and configure 802.1X Authentication parameter.

Operation Path

Open in order: “Network Configuration > Access Control > Port Authentication".

Interface Description

The screenshot of Port Authentication interface is as follows:



The main element configuration description of port authentication interface:

Interface Element	Description
IEEE802.1X Authentication	Enable/disable IEEE802.1X authentication.
Timed Update Authentication Time	The range of authentication upgrade interval is 60~4095, unit: second. The reauthentication interval of 802.1x used for strengthening the security of authentication.
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, port number and shared password for authentication of the authentication server if using external Radius

Interface Element	Description
	server.
Shared Authentication Password	The shared password character string used for device accessing Radius server. Supports combinations of letters, numbers and symbols with a length of no more than 50 characters.
Authentication Server Address	IP address of Radius server
Authentication Server Port No.	The port number of the Radius server. The default is 1812, value range is 1-65535.
Port Number	Switch port number.
IEEE 802.1x Port Authentication	IEEE802.1X authentication state of the port: • Enable; • Disable.

7.4.2 Authentication Database

Function Description

Set the username and password locally authenticated by 802.1X, and add, delete and save users.

Operation Path

Open in order: “Network Configuration > Access Control > Port Authentication > Authentication Database”.

Interface Description

Screenshot of database authentication interface:

The main element configuration description of database authentication interface:

Interface Element	Description
Username	Username of logging into local authentication.
Password	Password of logging into local authentication

7.5 QoS

7.5.1 QoS Classification

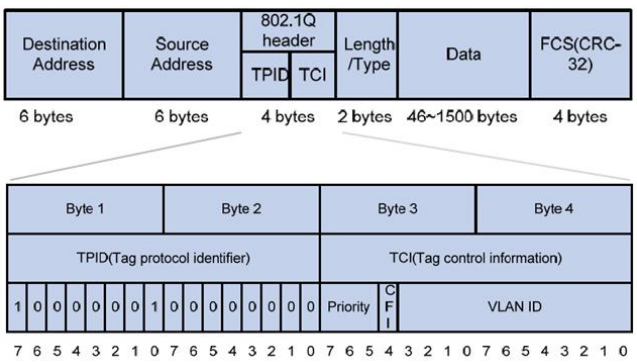
QoS (Quality of Service) is used to evaluate the ability of the service provider to meet the service needs of customers. As for network business, service quality includes transmission bandwidth, transfer delay, data packet loss rate and so on.

The service quality issues that traditional network faces are caused by network congestion. The so-called congestion refers to the phenomenon that the forwarding rate decreases and extra delays are introduced due to the relative shortage of supply resources, thus leading to the decline of service quality. As for congestion management, queue technology is generally adopted. It uses a queue algorithm to classify flow, then uses some priority algorithm to send these flow.

Priority is used to tag the priority of message transmission.

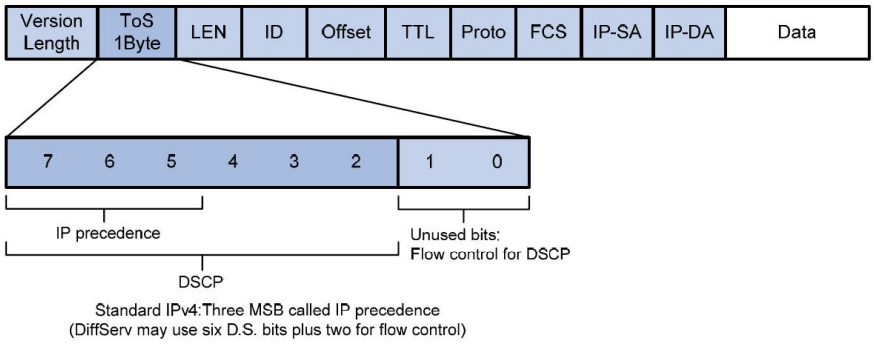
- CoS

  Ethernet defines 8 business priorities (CoS, Class of Service) in the VLAN TAG of Ethernet frame head. The 802.1Q label head of 4 bytes has included 2-byte TPID （Tag Protocol Identifier) and 2-byte TCI （Tag Control Information), TPID's is 0x8100, the following graph has displayed the details of 802.1Q label head, priority field is 802.1p priority.



- ToS

The ToS (Type of Service) domain in the head of IP message is called DS (differential Services) domain, in which the priority of DSCP is represented by the first 6 digits (0 ~ 5 digits) of this domain, with a value range of 0-63, and the last 2 digits (6 and 7 digits) are reserved. The greater the priority level value, the higher the priority level.



Function Description

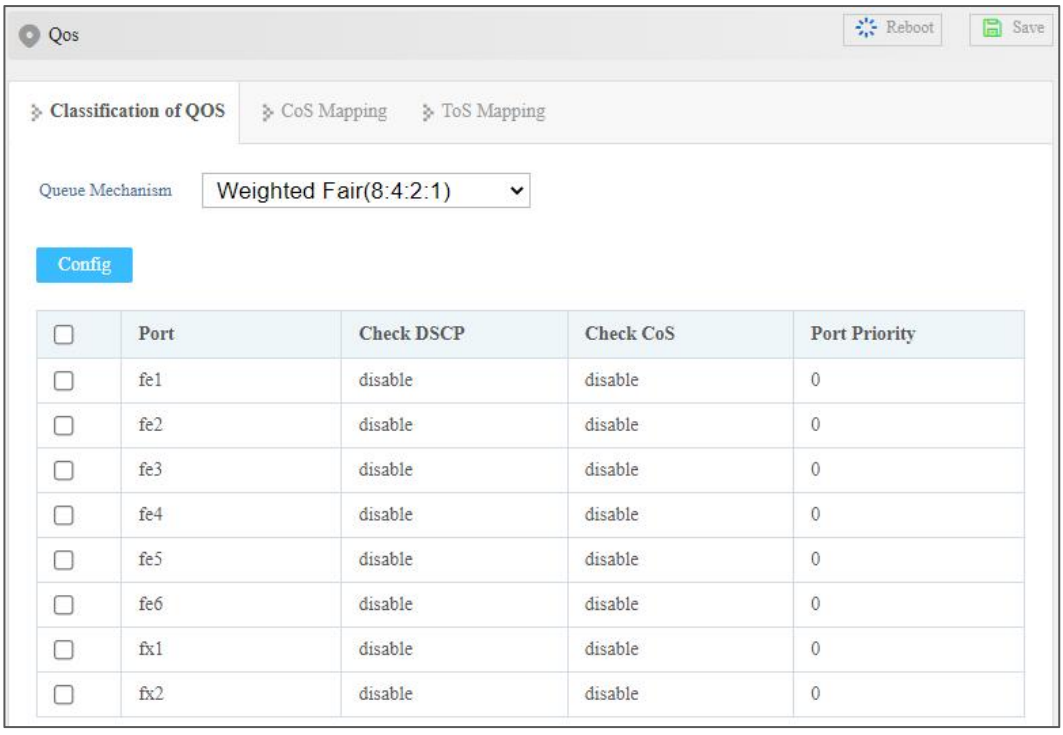
Set the queue mechanism of the device and the priority parameters of each port.

Operation Path

Open in order: “Network Configuration > QoS > Classification of QoS”.

Interface Description

Screenshot of Classification of QoS interface:



The main element configuration description of QoS classification interface:

Interface Element	Description
Queue Mechanism	Queuing scheduling setting, options are: • Weighted Fair (8:4:2:1): according to the queue's weighted value 8:4:2:1, weighted round-robin queue scheduling algorithm would schedule queues in turn to ensure that each queue can get some service time. • Strict (Strict Priority): Strict priority queue scheduling algorithm includes 4 queues and schedules in the decreasing order of priority. When the queue with fairly high priority is empty, then it would send groupings of queue with fairly low priority.
Port	The switch port number.
Check DSCP	After checking the checkbox, the priority of ToS would be inspected during queue scheduling.
Check CoS	After checking the checkbox, the priority of CoS would be inspected during queue scheduling.
Port Priority	To configure default port priority for ports that haven't enabled ToS and CoS priority. The value range is 0-7. The higher the value, the higher the priority. Note: By default, switch would use port priority in place of the 802.1p priority the port comes with when receiving message to control the quality of service the messages deserve.

Note

- When the ToS and CoS are not enabled, queuing and scheduling are in the order of port priority.
- When the ToS or CoS are enabled, queuing and scheduling according to ToS or CoS instead of considering port priority.
- If the ToS and CoS are enabled at the same time, queuing according to ToS priority. When the ToS values are the same, queuing according to CoS priority.

7.5.2 CoS Mapping

Function Description

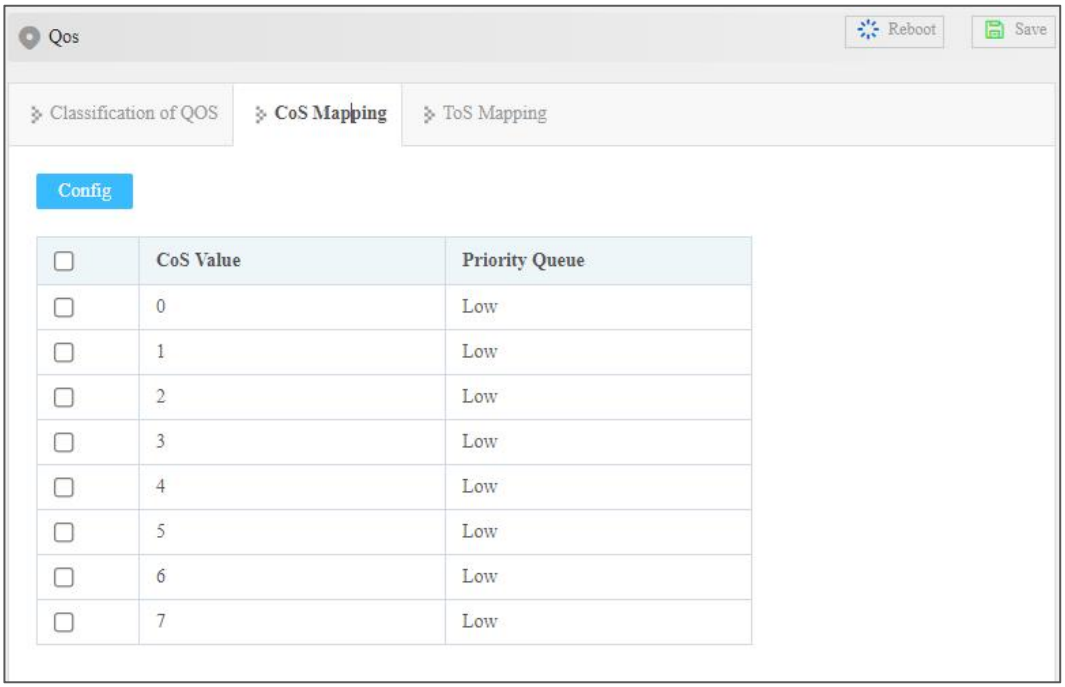
On the page of “CoS Mapping”, user can configure mapping between CoS value and priority queues.

Operation Path

Open in order: “Network Configuration > QoS > QoS Mapping”.

Interface Description

Screenshot of QoS Mapping interface:



The main element configuration description of QoS mapping interface:

Interface Element	Description
CoS Value	Display CoS value.
Priority Queue	Set mapping between CoS value and priority queue, priority queue is as follows: • Low: low priority queue • Normal: normal priority queue; • Medium: medium priority queue • High: high priority queue

7.5.3 ToS Mapping

Function Description

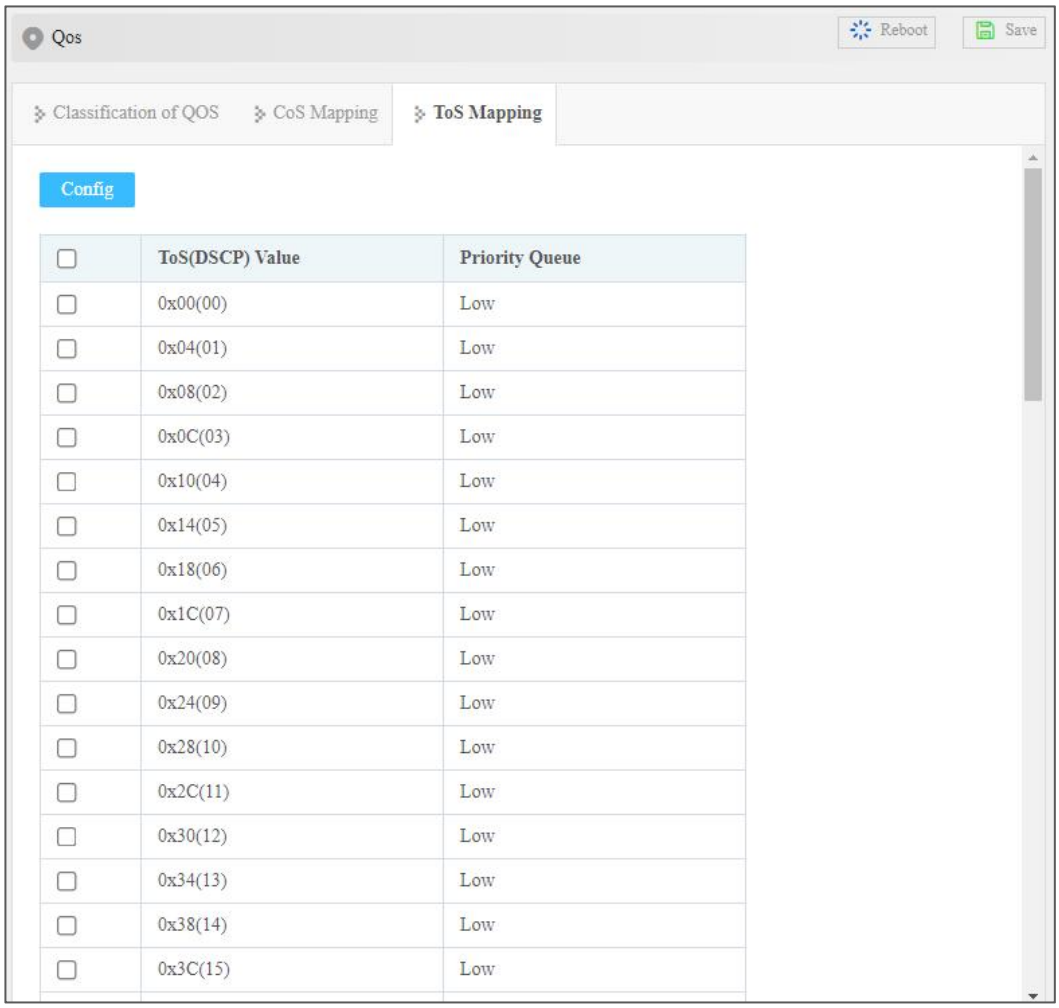
On the page of “ToS Mapping”, user can configure mapping between CoS value and priority queue.

Operation Path

Open in order: “Network Configuration > QoS > ToS Mapping”.

Interface Description

Screenshot of ToS Mapping interface:



The main element configuration description of ToS mapping interface:

Interface Element	Description

ToS (DSCP) Value	It displays ToS (DSCP) in hexadecimal and decimal format simultaneously. The value in the bracket is decimal.
Priority Queue	Set mapping between ToS value and priority queue, options are as follows: • Low: low priority queue • Normal: normal priority queue • Medium: medium priority queue • High: high priority queue

7.6 Modbus TCP

Function Description

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

Note

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

Operation Path

Open in order: “Network Configuration > Modbus TCP".

Interface Description

Modbus_TCP screenshot:

The main element configuration description of Modbus_TCP interface:

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

Modbus_TCP Data Sheet

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

Note

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

Information Type	Address (HEX)	Data Type	Description
System Information	0x0000	2 Words	Device ID (reserved)
	0x0002	16 Words	Name (ASCII display)
	0x0012	16 Words	Description (ASCII display)
	0x0022	3 Words	MAC Address (HEX display)
	0x0025	2 Words	IP address
	0x0027	16 Words	Contact Information
	0x0037	16 Words	Firmware Ver (ASCII display)
	0x0047	16 Words	Hardware Ver (ASCII display)
	0x0057	16 Words	Serial No.
	0x0067	1 Word	Power supply 1 status: • 0x0000: OFF • 0x0001: ON
	0x0068	1 Word	Power supply 2 status: • 0x0000: OFF • 0x0001: ON
Port Information	0x1000-0x101B	1 Word	Port connection status: • 0x0000: Link down • 0x0001: Link up • 0x0002: Disable

Information Type	Address (HEX)	Data Type	Description
			• 0xFFFF: No port
	0x101D-0x1038	1 Word	Port operating mode: • 0x0000: 10M-Half • 0x0001: 10M-Full • 0x0002: 100M-Half • 0x0003: 100M-Full • 0x0004: 1G-Half • 0x0005: 1G-Full • 0xFFFF: No port
	0x1039-0x1054	1 Word	Port flow control status: • 0x0000: OFF • 0x0001: ON • 0xFFFF: No port
	0x1056-0x1071	1 Word	Port interface type: • 0x0000: Copper port • 0x0001: Fiber port • 0x0002: Combo port • 0xFFFF: No port

Example: MODBUS_TCP Configuration

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

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

Operation Steps

First, configure the switch Modbus_TCP monitoring enable.

Step 1 Log into Web configuration interface.

Step 2 Select “Network Configuration > Modbus_TCP".

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

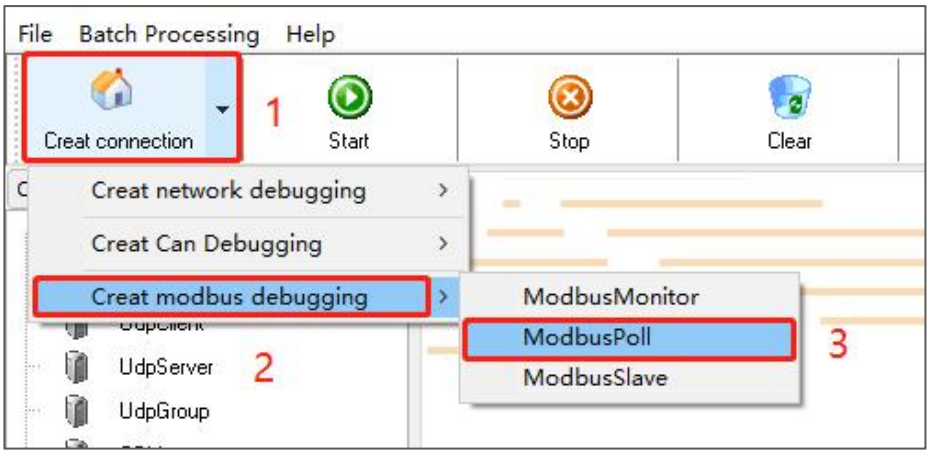
Step 4 End.

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

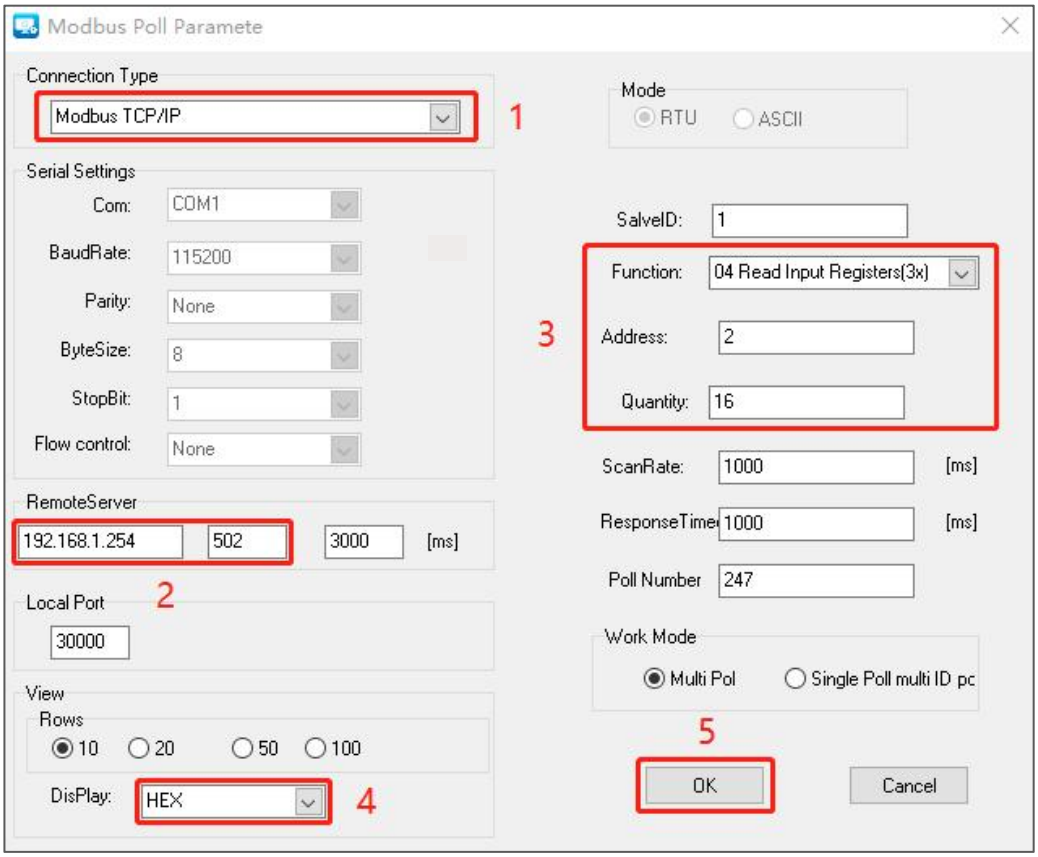
Step 1 Open "Debug Tool".

Step 2 Click the drop-down list of "Create connection".

Step 3 Select "Create Modbus debugging > ModbusPoll", as the picture below.



Step 4 Configuration window of ModbusPoll parameters pops up, the configuration as the picture below:



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

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

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

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

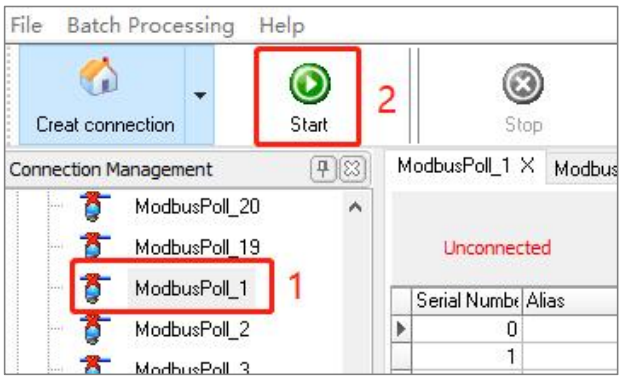
Notice:
Here the start address is decimal format, so hexadecimal register address should be converted into decimal format.

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

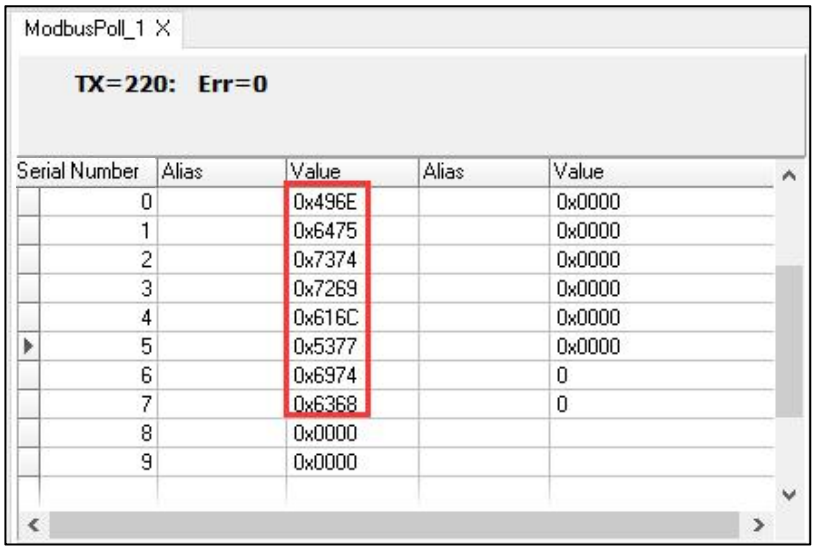
5 Select "HEX" on the drop-down list of "Display";

6 Click "OK".

Step 5 On the page of Debug Tool, select created ModbusPoll, and then click "Start";



Step 6 Check responsive data, and convert the hexadecimal value read by register into ASCII code, displayed as "Industrial Switch";



Step 7 End.

Note

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

8 System Configuration

8.1 Network Diagnosis

8.1.1 Ping

Function Description

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

Operation Path

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

Interface Description

The Network diagnosis interface is as follows:

The main element configuration description of Ping 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.

8.2 Time Configuration

8.2.1 NTP Configuration

The full name of NTP protocol is Network Time Protocol. Its purpose is to deliver uniform, standardized time on the 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

Enable and configure NTP server.

Operation Path

Open in order: “System Configuration > NTP Configuration > Time Configuration".

Interface Description

NTP configuration interface as follows:

The main element configuration description of NTP configuration interface:

Interface Element	Description
Enable	Enable/Disable NTP configuration.
NTP Server	IP address of NTP server, for example: 192.168.1.1. Note: As NTP client, the system will synchronize time with NTP server every 11 minutes.

8.3 Alarm Configuration

After enabling alarm, when the device port is in an abnormal state, the administrator can be informed in time, and the device state can be quickly repaired to avoid excessive loss.

8.3.1 Global Settings

Function Description

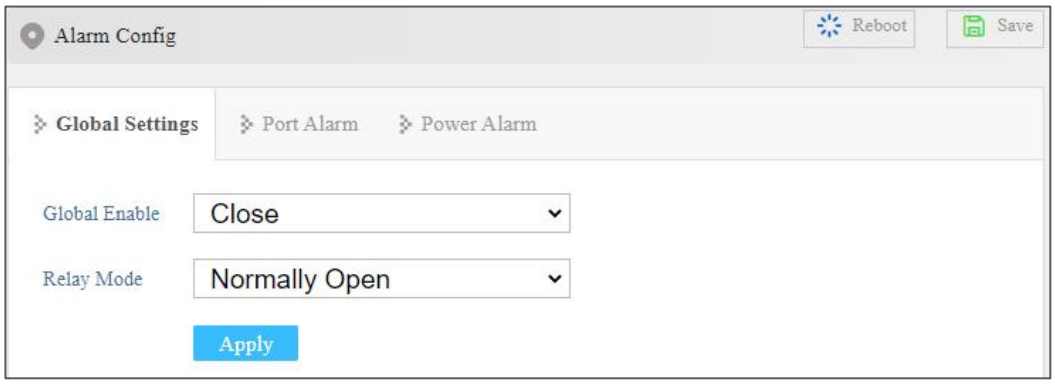
Enable/disable the alarm item of this device globally. Set the circuit mode of the relay.

Operation Path

Open in order: “System Configuration > Alarm Configuration > Global Settings".

Interface Description

Global configuration interface is as follows:



The main element configuration description of port configuration interface:

Interface Element	Description
Global Enable	Enable/disable all enabled alarm items.

Interface Element	Description
Relay Mode	Set the circuit state of the relay: • Normally closed: when the relay is normal without alarm, it is in closed status; when alarm occurs, the relay is in open status; • Normally open: when the relay is normal without alarm, it is in open status; when alarm occurs, the relay is in closed status.

8.3.2 Port Alarm

Function Description

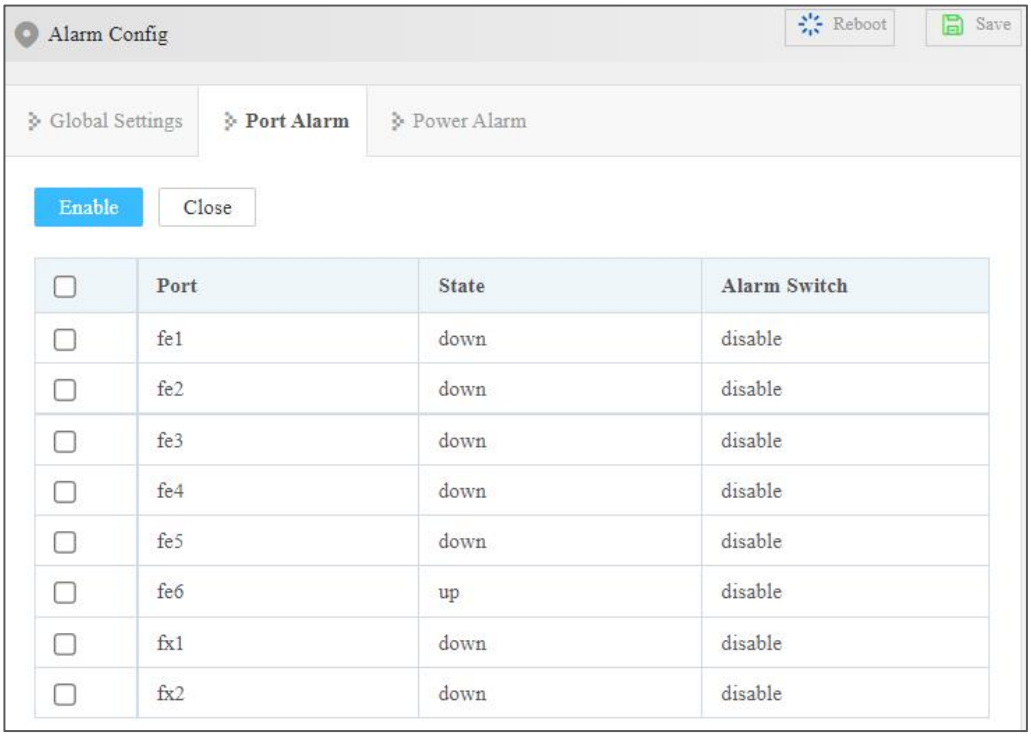
After enabling alarm, when the device port is in an abnormal state, the administrator can be informed in time, and the device state can be quickly repaired to avoid excessive loss.

Operation Path

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

Interface Description

Global configuration interface is as follows:



The main element configuration description of port configuration interface:

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

8.3.3 Power Alarm

Function Description

Enable/disable the power alarm function.

Note

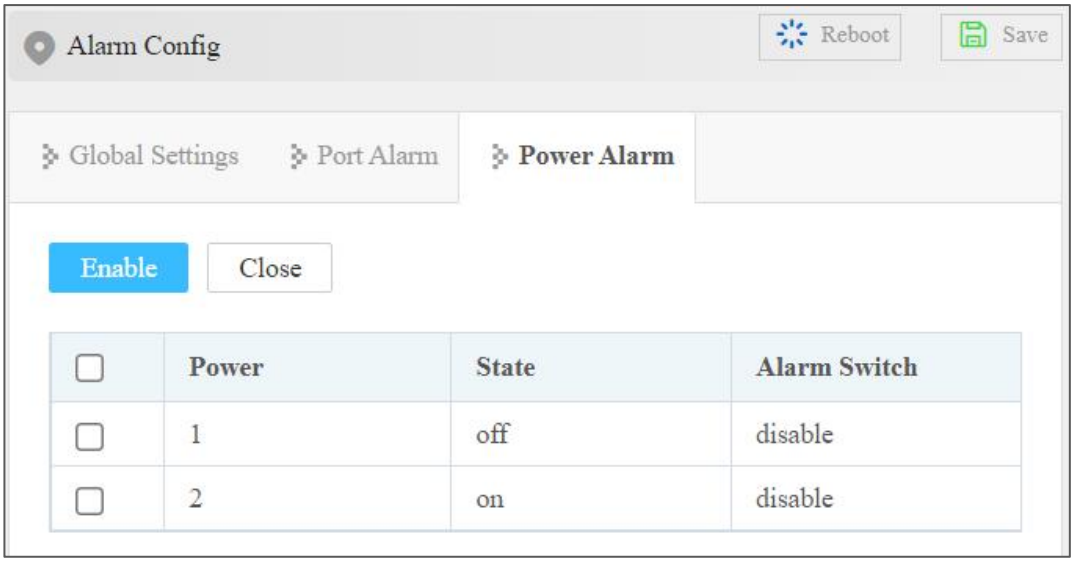
Only DC dual power supply supports power alarm, and AC current does not support power alarm.

Operation Path

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

Interface Description

Power alarm interface as below:



Main elements configuration description of power alarm interface:

Interface Element	Description
Power	The corresponding name of this device’s power supply
State	Device power link status, display items as follows: • On: connected • Off: disconnected
Alarm Switch	Port alarm function status, options as follows: • Enable: alarm has been enabled. • Disable: the alarm is not enabled
Enable	Check the port that needs to enable power alarm, and click enable to enable this function.
Close	Check the port that needs to disable power alarm, and click disable to disable this function.

8.4 Configuration File Management

8.4.1 Configuration File Update

Function Description

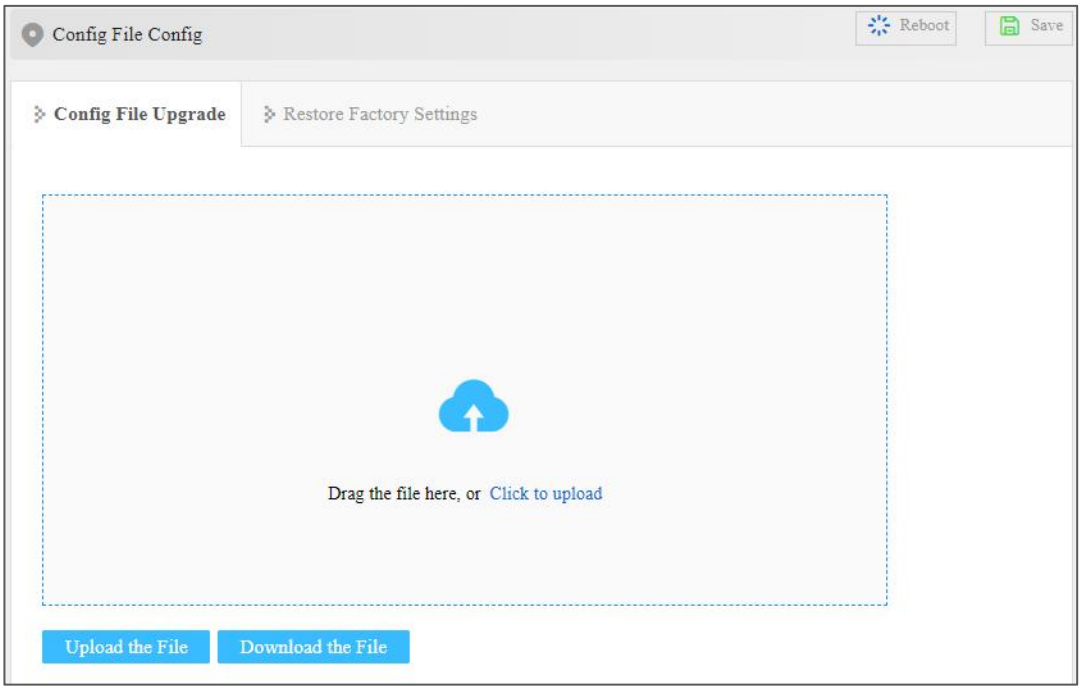
Upload and download configuration files

Operation Path

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

Interface Description

Configuration file upgrade interface as follows:



The main element configuration description of System File interface:

Interface Element	Description
Download the File	Download the configuration information files of current switch. Tips: Downloaded configuration files can be uploaded to other homogeneous devices, achieving repeated usage after one-time configuration.
Upload Configuration	The format of the configuration file is ".conf". Drag the profile into the upgrade box, or click "Click to Upload" to select the

	profile.

Warning

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.

8.4.2 Restore Factory Settings

Function Description

Restore the device firmware to the factory configuration.

Operation Path

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

Interface Description

The Restore Factory Settings interface is as follows.

The main element configuration description of management file interface:

Interface Element	Description
One-Key Reset	Restore factory defaults of the switch. Note: Restore factory defaults will cause all devices to be in the factory status, default IP address is "192.168.1.254".

8.5 Upgrade

Function Description

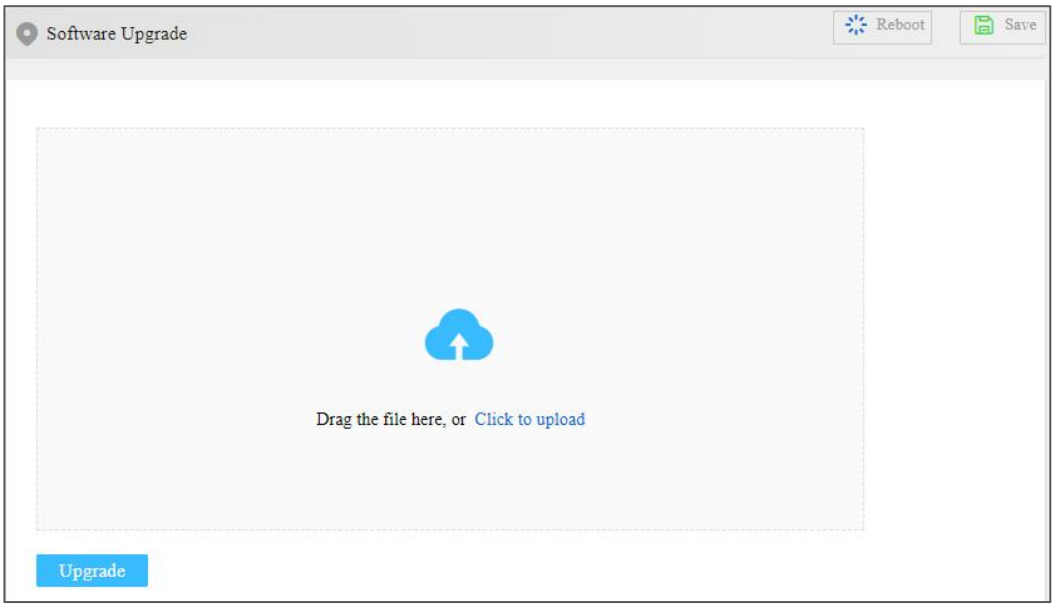
Update and upgrade the device program via web page.

Operation Path

Open in order: “System Configuration > Software Upgrade".

Interface Description

The software update interface is as follows.



The main elements configuration description of software update interface:

Interface Element	Description
Upgrade	Drag the upgrade file into the upgrade box or click "Click to Upload" to select the upgraded file in the format of ".bin".

8.6 Log Information

8.6.1 Log Information

Function Description

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

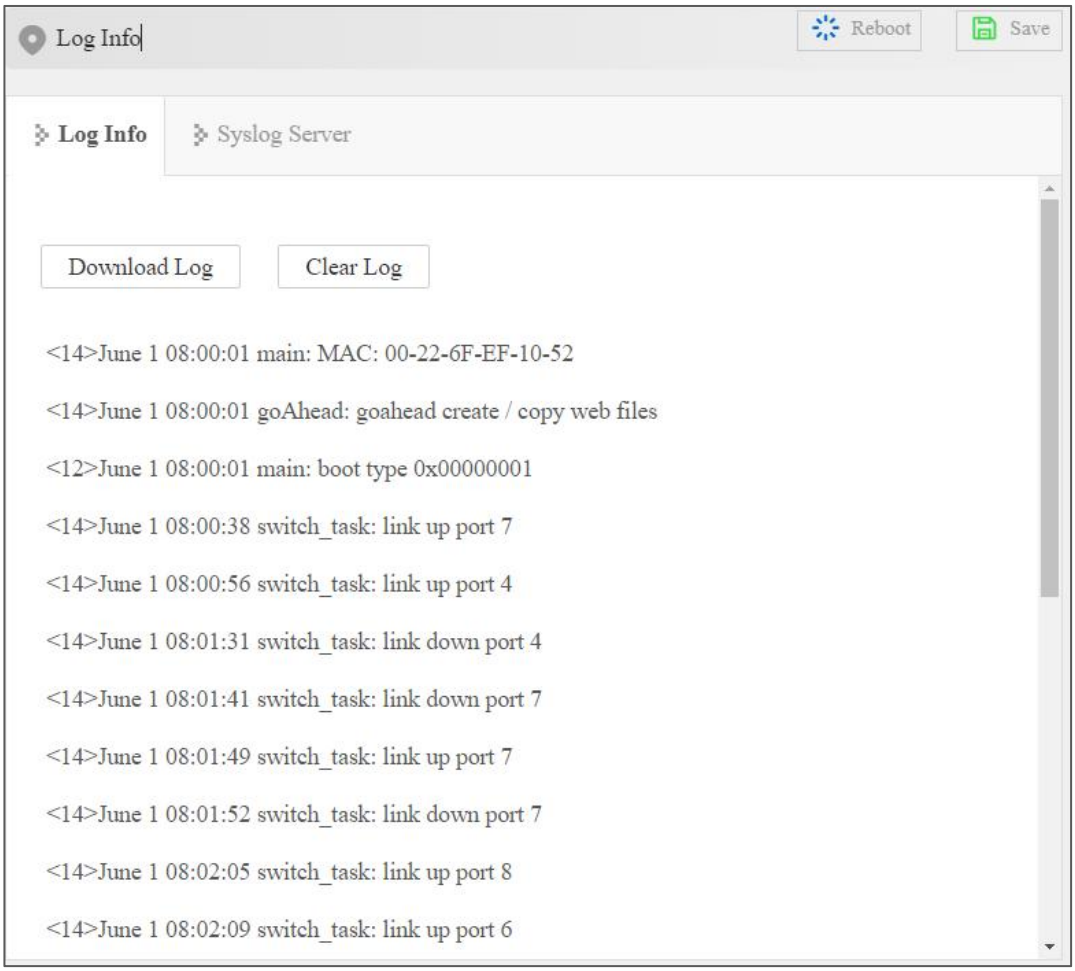
- User log: records user operations and system operation information.
- Security log: records information including account management, protocol, anti-attack and status.
- Diagnostic log: records information that assists in problem identification.

Operation Path

Open in order: “System Configuration > Log Information > Log Information".

Interface Description

The Log Information interface is as follows:



Main elements configuration description of log information interface:

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

8.6.2 Syslog Server

Function Description

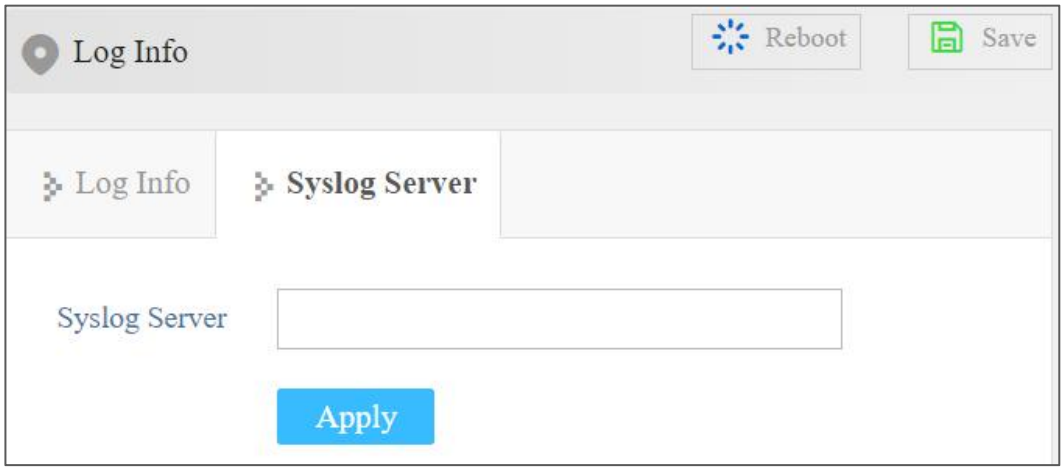
Configure the Syslog server IP address, and the system log information can be sent to the configured syslog server.

Operation Path

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

Interface Description

The Syslog server interface as follows:



Syslog server interface main elements configuration instructions:

Interface Element	Description
Syslog Server	IP address of Syslog server

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. **How to configure the device restore default setting via DIP switch?**

   Turn the DIP switch 2 to ON position, and restore default setting after power on again.

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

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

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

9.3 Alarm Problem

1. **When the device alarms, except BlueEyes_II software nether alarm information display area will display alarm information, is there any other way to notify technical staffs?**

   When the device alarms, monitoring host computer buzzer will continue to emit alarm sounds.

9.4 Indicator Problem

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

Possible reasons include:

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

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

Possible reasons include:

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

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

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

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

Reasons may include:

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

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