5 100M Ethernet Ports + 2 Serial Ports Managed Industrial Ethernet Switch

User Manual

Document Version: 03

Issue Date: 12/26/2022

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

Note

The screenshoot reference model of this manual is 5 100M copper ports + 2 serial ports, except the supported Ethernet port, serial port and power supply number and type, its interface function and operation is same to other models products.

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

Text Format Convention

Format	Description
" "	Words with “” represent the interface words. 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’.

Format	Description
About this chapter	The section 'about this chapter' provide links to various sections of this chapter, as well as links to the Principles Operations Section of this chapter.

Symbols

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

Revision Record

Version No.	Date	Revision note
01	2016-01	Product release
02	2019-10-25	Layout optimization
03	2022-12-26	Product upgrading

Contents

1 Log in the Web Interface

1.1 System Requirements for WEB Browsing

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

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

1.2 Setting IP Address of PC

The switch default management as follows:

IP Settings	Default Value
IP Address	192.168.1.254
Subnet mask	255.255.255.0

While configuring the switch via Web:

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

the same subnet to the one of switch.

Note:

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

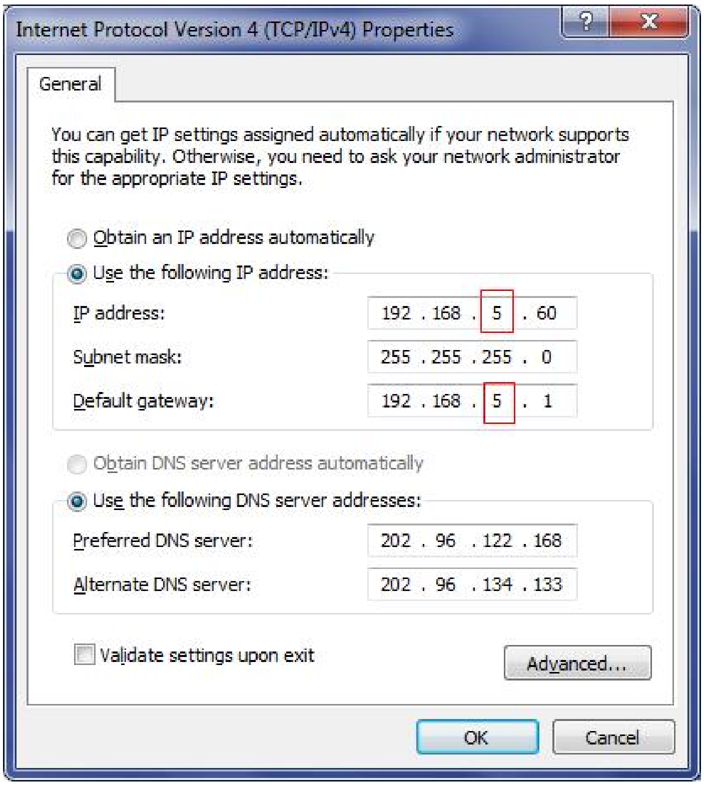
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follow:

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

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



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

Step 4 End.

1.3 Log in the Web Configuration Interface

Operation Steps

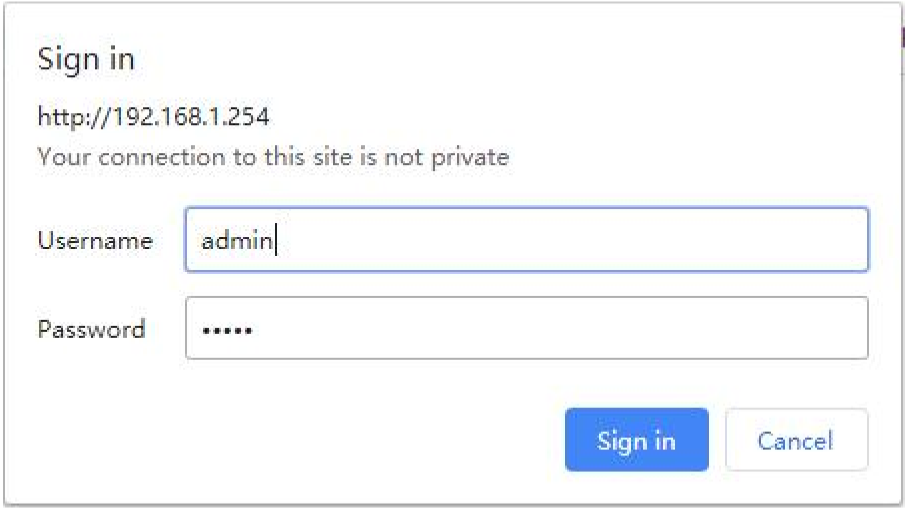
Login in the web configuration interface as follow:

Step 1 Run the computer browser.

Step 2 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 in the device, modify the switch IP address for usage convenience.

2 System Status

Function Description

On the page of "System Information", user can check "Device Information" and "Port Information".

Operation Path

Open in order: "Main Menu > System Status > Overview".

Interface Description

Device information interface as follows:

Device Information

Name	IndustrialSwitch	Hardware Ver	1.0.0
Module	ManagedSwitch	Firmware Ver	1.1.0 B20220420E1R0A00000
Description	5PORT	MAC Address	00-22-6F-01-05-1D
Serial No	sw12345656877	Contact	

Port Information

Port	Connection	Duplex	Speed	Type
01	LINK	FULL	100M	TX
02	LOS	HALF	10M	TX
03	LOS	HALF	10M	TX
04	LOS	FULL	10M	FX
05	LOS	FULL	10M	FX

Main elements configuration description of state information interface:

Interface Element	Description
Device information	**Device information status bar.**

Interface Element	Description
Name	Display the device name.
Module	Display the device model.
Description	Display characters description of the device.
Device No.	SN code, product serial number.
Hardware Ver	Current hardware version information.
Software Ver	Current software version information.
MAC address;	Hardware address of device factory configuration.
Contact	Display the contact information of the device maintenance personnel.
Port Information	**Port Information Status Bar.**
Port	Number of device port.
Connection	Port connection state, display state as follows: • "LINK" represents connected port; • "LOS" represents disconnected port.
Duplex	Port work state, display state as follows: • "HALF" represents the corresponding port is in the state of half-duplex; • "FULL" represents corresponding port is in full duplex state.
Speed	When a port is connected, the current rate of port link is displayed.
Type	Interface type. • FX: fiber port; • TX: copper port.

Note

“Device model”, “Device name”, “Device description”, “Device number” and “Contact information” can be modified in "Main Menu > System Manage > System Info".

3 Serial Server

3.1 COM Settings

Serial server can extend the transmission distance of serial terminal device via Ethernet, at the same time user can manage the device centrally. The Ethernet data of serial server is transmitted on the TCP and UDP protocol, which has realized the transparent transmission of serial data. The device supports multiple work modes and meets various demands.

Basic Mode

- TCP Server

  In the TCP server mode, the serial device server is assigned an IP port number, passive waiting for the host connection. When the host initiates a connection request and establishes a connection with the serial device server, the host can realize bidirectional transparent data transmission through the network connection and the serial port.
- TCP Client

  In the TCP client mode, the serial server can automatically establish a network connection with the host specified by the user when the serial data arrives.
- UDP.

  In UDP server mode, the serial server through the UDP protocol and user-specified host for serial data transmission. Compared with TCP protocol, UDP protocol is faster and more efficient.
- TCPAuto

  In this mode, the serial server could be the TCP server or host. Before setting this mode, please make sure the relevant parameters are correctly set. When the server mode is enabled, the client mode would be disconnected automatically.

Advanced Mode

- TCP Server

  In the TCP server mode, the serial device server is assigned an IP port number, passive waiting for the host connection. The TCP server mode supports up to four session connections simultaneously, allowing multiple hosts to simultaneously read or send Ethernet data to a serial device.

- UDP(UDP section)

  When the routers and switches and other devices do not support multicast, but also need to achieve the multicast function, you can make the serial server in UDP rang mode. In this mode, the serial server through the UDP protocol with the user specified the same network segment of the host advance serial data transmission, to achieve point to multipoint data communication.

Function Description

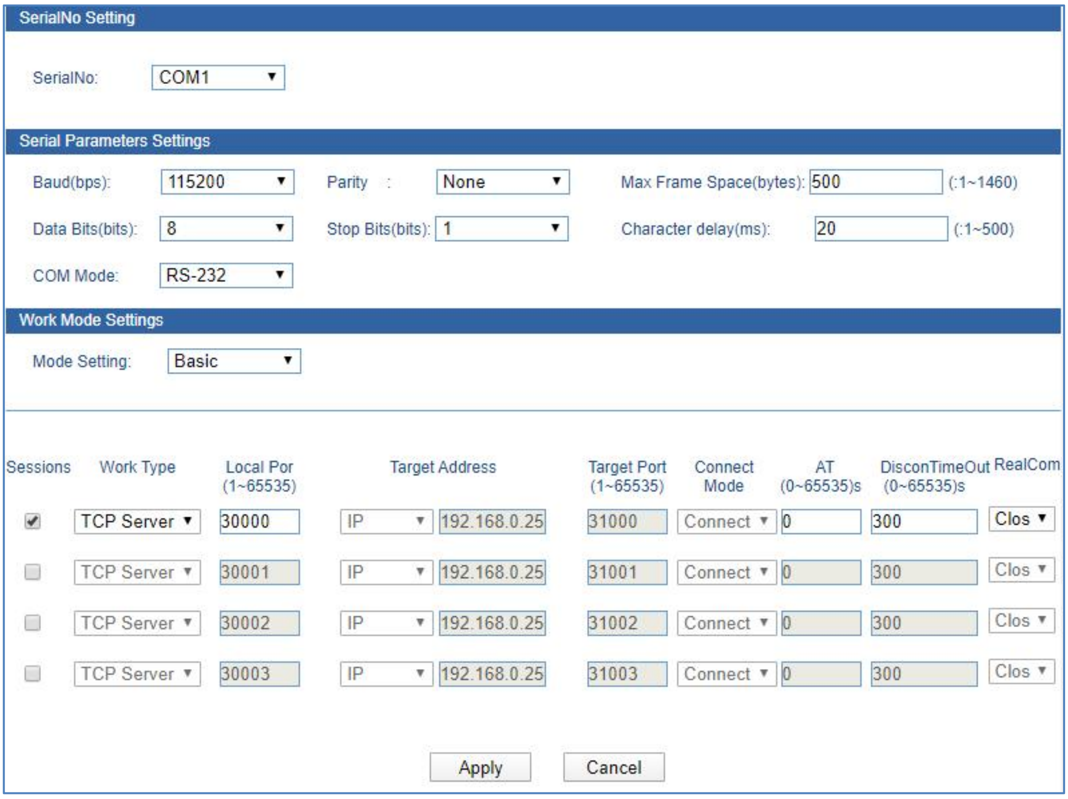
On the page of "COM Settings", user can configure baud rate, data bit, stop bit, parity bit and other basic parameters information of corresponding serial number and the operating mode of serial port.

Operation Path

Open in order: " Main Menu > Serial Server > COM Settings".

Interface Description

COM settings interface as follows:



Main elements configuration description of COM settings interface:

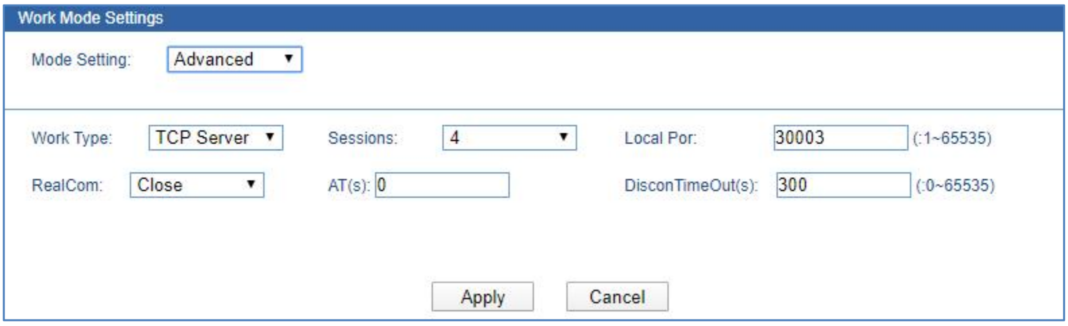
Interface Element	Description
Serial No Setting	**Configuration column of serial number selection**
Serial port number	Select corresponding serial number of the device.
Serial Parameter Settings	**Serial parameter settings column**
Baud Rate(bps)	Select baud rate of corresponding serial number. Options: 1200/2400/4800/9600/19200/38400/57600/115200
Parity	Select parity bits of corresponding serial number. Options: • None; • Odd; • Even.
Max Frame Space (bytes)	Frame length of serial data to Ethernet data, within given time range, data frame that is greater or equal to given frame length should be forwarded; value range is 1-1430bytes.
Data Bits (bits)	Select data bits of corresponding serial number. Options: • 8 bits.
Stop Bit	Select stop bits of corresponding serial number. Options: • 1 bits;

Interface Element	Description
	• 2 bits.
Character delay	Interval time of serial data to Ethernet data, value range is 1-500ms.
COM Mode	It's decided by software and hardware, there are RS232, RS485 and RS422 modes.
Work Mode Settings	**Work Mode Settings Column**
Mode Setting	Optional modes of the device as follows: • Basic: TCP Client, TCP Server, UDP, TcpAuto; • Advanced: TCP Server, UDP.
Sessions	1-4, each serial port of the device supports 1-4 sessions. Session refers to the process that serial server transmits data received from serial port to Ethernet via socket connection.
Local port	1-65535, a TCP port provided by the device that can be connected to other TCP/IP nodes and is associated with the corresponding serial port of the serial port server. System will automatically distribute local port number when it's "0", fixed local port number will be used when it's not "0".
Destination Address	IP address or domain name address to be connected to serial server, both can be corresponding to the host address in Internet.
Destination port	1-65535, TCP port number to be connected to serial port.
Connection mode	• Connect Now: the device is connected after being powered on, it will be connected soon after the connection is broken. • Data Trigger: the device will initiate connection when the corresponding serial port receives the data.
AT	0-65535s, the device sends out heartbeat packet according to given time interval, session will be disconnected if there is no reply for 3 times in succession.
DisconTimeOut	0-65535s, set the idle time of automatic disconnection, and the device will disconnect the session connection if there is no data transmission within given time. If it's set to "0", the device won't forwardly disconnect the session connection no matter

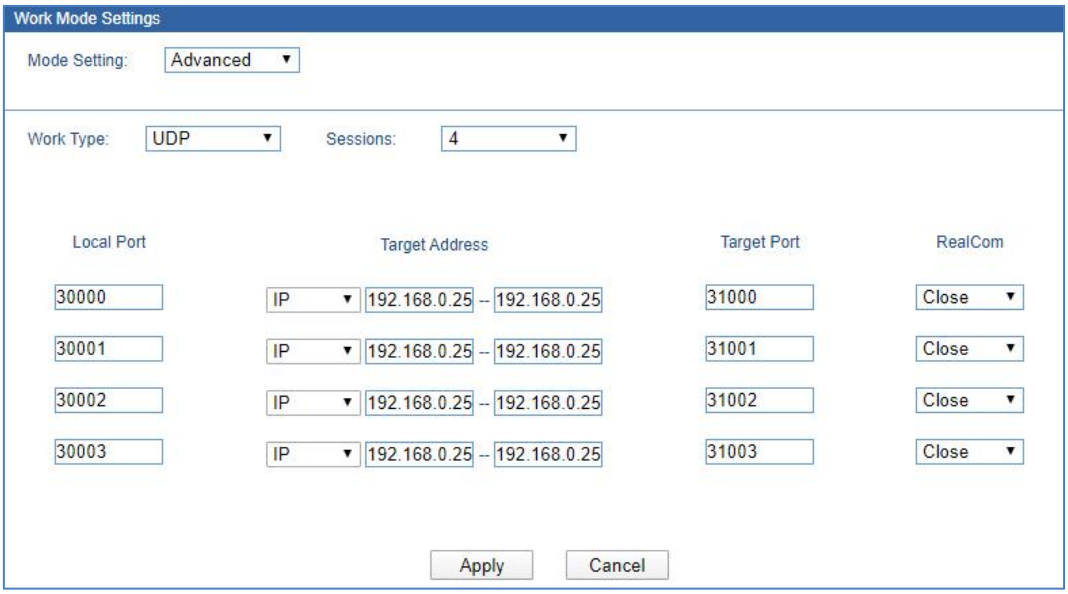
Interface Element	Description
	how long the idle time is.
RealCom	After enable RealCom, the device will work together with Windows/Linux operation system installed with the driver procedure of real serial port. Note: RealCom COM / TTY driver establishes a transparent network transmission connection between the host and the serial device in the operating system. Map the serial port of the serial port server to the local COM/TTY device of the host according to the user configured serial server IP address and serial port number and other parameters. The original serial device software or communication module without modification can be used directly without modification.

Interface Description: Advanced Mode

TCP Server interface of advanced mode as follows:



UDP interface of advanced mode as follows:



Notice

- Address pool only supports IP address of B and C class.
- The value of start and end address of address pool should be in the same network segment.
- The value of start address of address pool must be less than or equal to one of the end address.

3.2 Serial Port Information

Function Description

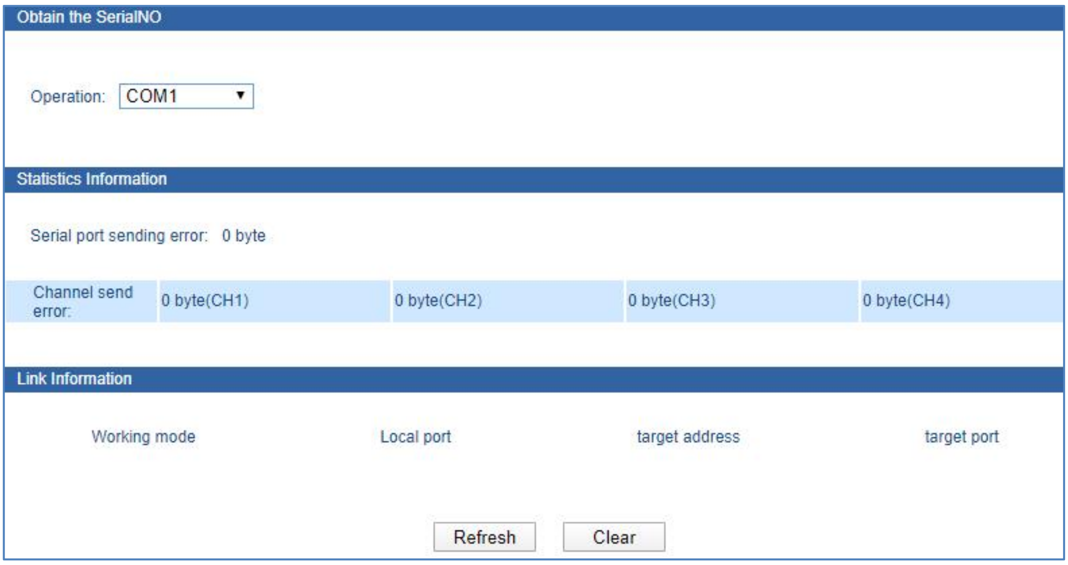
On the page of “COM Information”, user can check the statistics and connection information of serial port.

Operation Path

Open in order: “Main Menu > Serial Server > COM Information”.

Interface Description

Serial port information interface screenshot as follows:



COM information interface, the main elements of the configuration instructions

Interface Element	Description
Serial number configuration	**Serial number configuration column**

Interface Element	Description
Serial port number	Pull-down list of serial port.
Statistics information	**Statistics information column**
COM Send Error	Quantity statistics of error bytes sent out by serial port.
Channel Send Error	Error bytes occur in channel or session 1-4.
Link Information	**Link information column**
Link Information	Display current work type, local port, target address, target port and other information of serial port.

4 Port Configuration

4.1 Port Settings

Function Description

The "Port Config" page mainly includes:

- Check port type;
- Set speed mode and duplex mode;
- STP Enabled;
- Flow control;

  Network congestion can cause packet loss, and flow control is a technology that prevents this from happening. After the flow control function is configured, it will send a message to the opposite end device to notify it to temporarily stop sending the message if the local device becomes congested. After receiving the message, the opposite end device will temporarily stop sending the message to the the local device to avoid congestion, regardless of the working speed of its interface. Flow control can effectively prevent the impact on network caused by the instantaneous mass data in network to ensure the efficient and stable operation of user network.

  Flow control implements half and full duplex mode via different ways:

  - In half duplex mode, flow control is implemented through backpressure, which is usually called backpressure count. This count makes signal source lower its sending speed by sending jamming signal to source.
  - In full duplex mode, flow control usually conforms to IEEE 802.3x standard. The switch sends “pause” frame to signal source to make it stop sending. After signal source receives “pause” frame, it would stop for a while to send messages.

Note

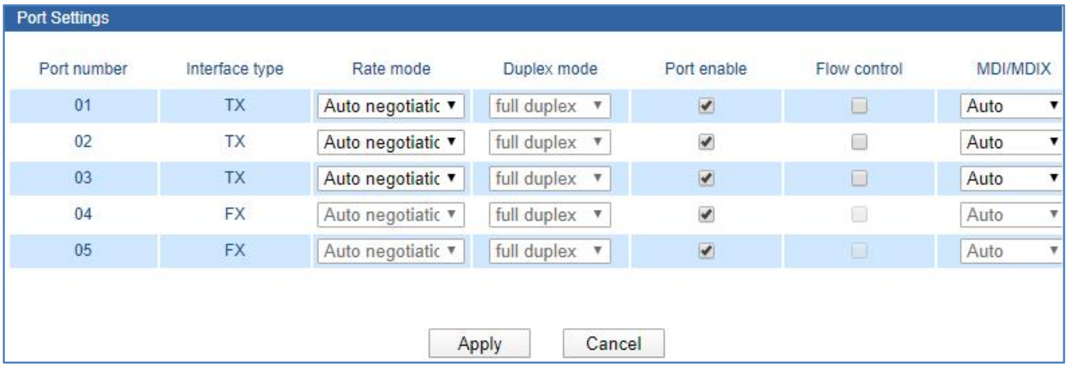
- The speed, duplex and flow control of this port take effects only when the port is enabled.
- After selecting automatic negotiation, speed and duplex will be gained via automatic negotiation.

Operation Path

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

Interface Description

Port settings interface as follows:



The main element configuration description of port setting interface:

Interface Element	Description
Port	Port number of the device.
Interface type	According to the electrical properties of the interface, the Ethernet interface of the device can be divided into: • Copper port: transmit electrical signal via twisted-pair; • Fiber port: transmit optical signal via optical fiber
Rate mode	Click the “Speed” drop-down list to select port speed mode. • Auto-Negotiation: the port can be automatically adjusted to the transmission speed of the opposite port; • 10M speed: the maximum supported speed is 10Mbit/s; • 100M speed: the maximum supported speed is 100Mbit/s;

Interface Element	Description
	Note: The copper ports of the devices are all MDI/MDIX automatic adaptive ports, which support automatic negotiation.
Duplex Mode	Click the "Duplex" drop-down list to select the duplex mode corresponding to the port. The options are as follows: • Half duplex: the interface can only receive or send data at any time. • Full-duplex: interface can receive and send data at the same time. Note: When the speed mode is “Auto negotiation”, the port automatically matches the opposite port duplex mode.
Port Enable	Tick the check box to enable the port. Notice: Uncheck the checkbox means that the port is not enabled and cannot forward data.
Flow Control	Tick the check box to enable the flow control function of the port. • Under full duplex mode, flow control method is IEEE 802.3x flow control. • Under half duplex mode, flow control method is back pressure flow control.
MDI/MDIX	Click "MDI/MDIX" drop-down list box to select MDI type of media-related interface. • Auto: self-adaptive MDI or MDI-X type; • MDI; • MDI-X. Note: The interface type at both ends of the link is recommended to use "Auto" self-adaptation. At this time, both the straight-through line and the cross line can communicate normally. MDI type should be specified only when the device can't get the network cable type parameter. • When using the straight-through network cable, the interfaces at both ends of the link should be configured to different types or at least one end should be "Auto" self-adaption. • When using cross network cables, the interfaces at both ends of the link should be configured to the same type or at least one end should be "Auto" adaptive.

Instance: Port Configuration

For example, port 1, port 2 and port 3 are set as follows:

- Set the "Speed" of port 1 to "Auto".
- Set the "Speed" of port 2 to "100M" and "Duplex" to "Full";
- Set the "Speed" of port 3 to "10M", "Duplex" to "Half" and enable "Flow Control".

Operation Steps

Step 1 Enter "Main Menu > Port Config > Port Settings".

Step 2 Set the parameters of port 1:

1 Check the "Enable" check box;

2 Select "Auto" for "Speed".

Note:

The default configuration for "Speed" is "Auto".

Step 3 Set the parameters of Port 2:

1 Check the "Enable" check box;

2 Select "100M" for "Speed";

3 Select "Full" for "Duplex" .

Step 4 Set the parameters of Port 3:

1 Check the "Enable" check box;

2 Select "10M" for "Speed";

3 Select "Half " for "Duplex" .

4 Check the "Flow Control" check box.

Step 5 Click "Apply".

Step 6 End.

4.2 Bandwidth Management

Function Description

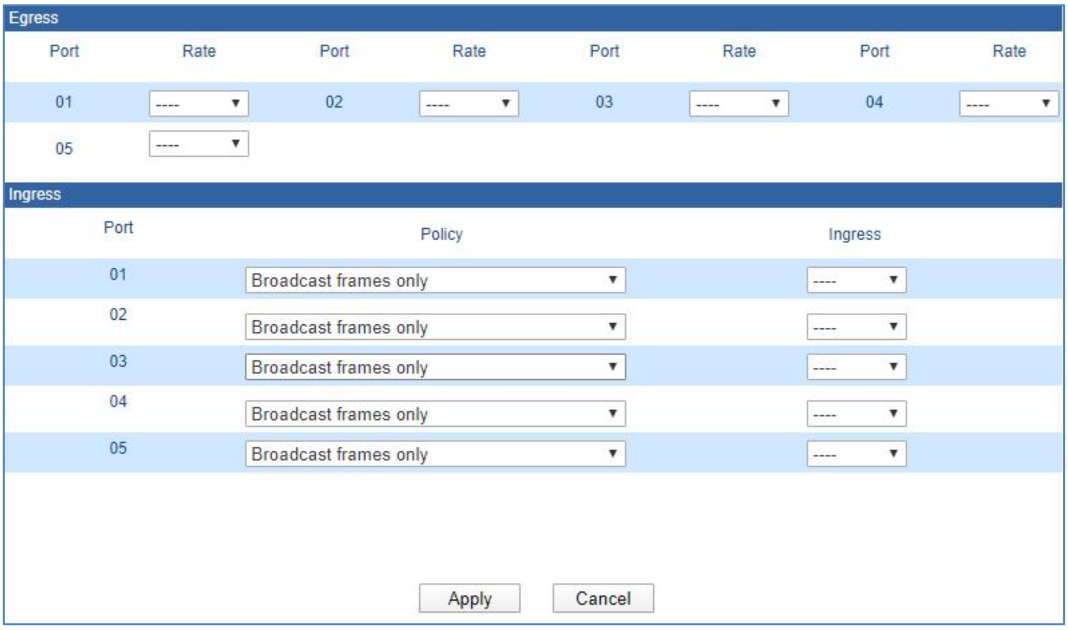
On the page of "Bandwidth Management", user can limit the ingress and egress bandwidth speed of the port.

Operation Path

Open in order: "Main Menu > Port Configuration > Bandwidth Management".

Interface Description

Bandwidth management interface as below:



The main element configuration description of bandwidth management interface:

Interface Element	Description
Port	Port number of the device.
Rate	Egress bandwidth is the bandwidth when the port sends data. Note: “----” represents no speed limit.
Policy	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 frames only.
Ingress	Egress bandwidth is the bandwidth when the port sends data. Note: “----” represents no speed limit.

Note

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

5 Layer 2 Features

5.1 VLAN

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.

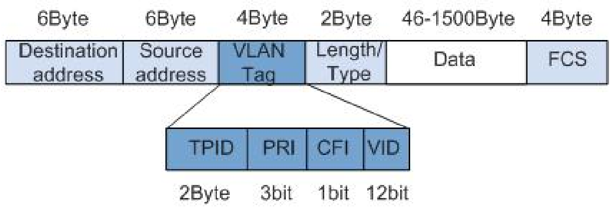
- Limit the broadcast domain;
- Increase the security of LAN;
- Improve the network stability;
- Flexibly construct virtual working team.

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.

Function Description

On the VLAN page, user can configure the following functions:

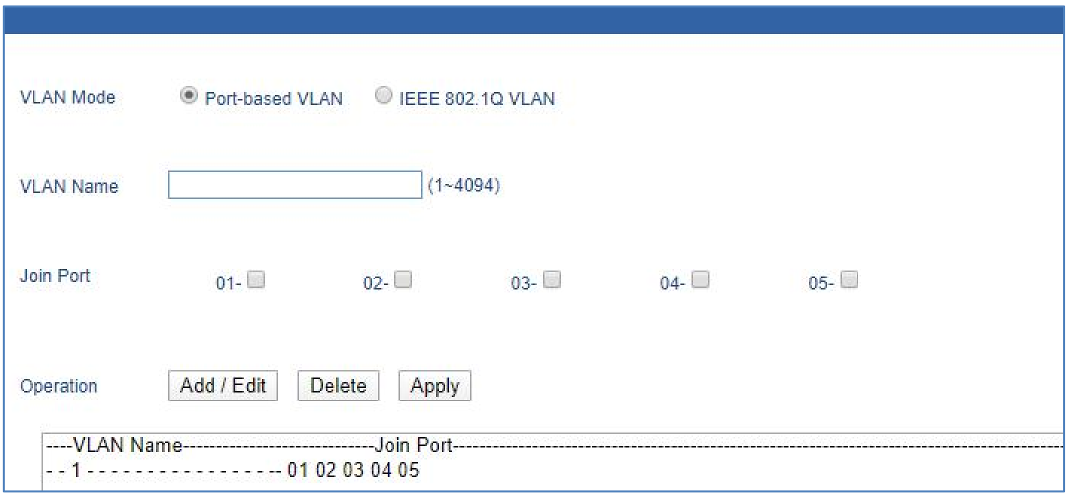
- Configure the port PVID;
- Create VLAN entry;
- Configure the port member type.

Operation Path

Open in order: "Main Menu > L2 Feature > VLAN".

Interface Description 1: Port-based VLAN

Port-based VLAN interface as follows:



The main elements configuration description of port-based VLAN interface:

Interface Element	Description

Interface Element	Description
VLAN Mode	Choose VLAN type, options are: • Port-based VLAN; • IEEE 802.1Q VLAN
VLAN name	Enter VLAN number in digital form.
Join Port	Choose VLAN member.
Operation	Add/edit, delete or save VLAN configuration information.

The steps of configuring port-based VLAN:

Step 1 Open “Main Menu > L2 Feature > VLAN”.

Step 2 On the option box of “VLAN Mode”, select “Port-based VLAN”.

Step 3 Enter VLAN table items in the textbox of “VLAN Name”, such as filling in the figure “3” to represent VLAN3.

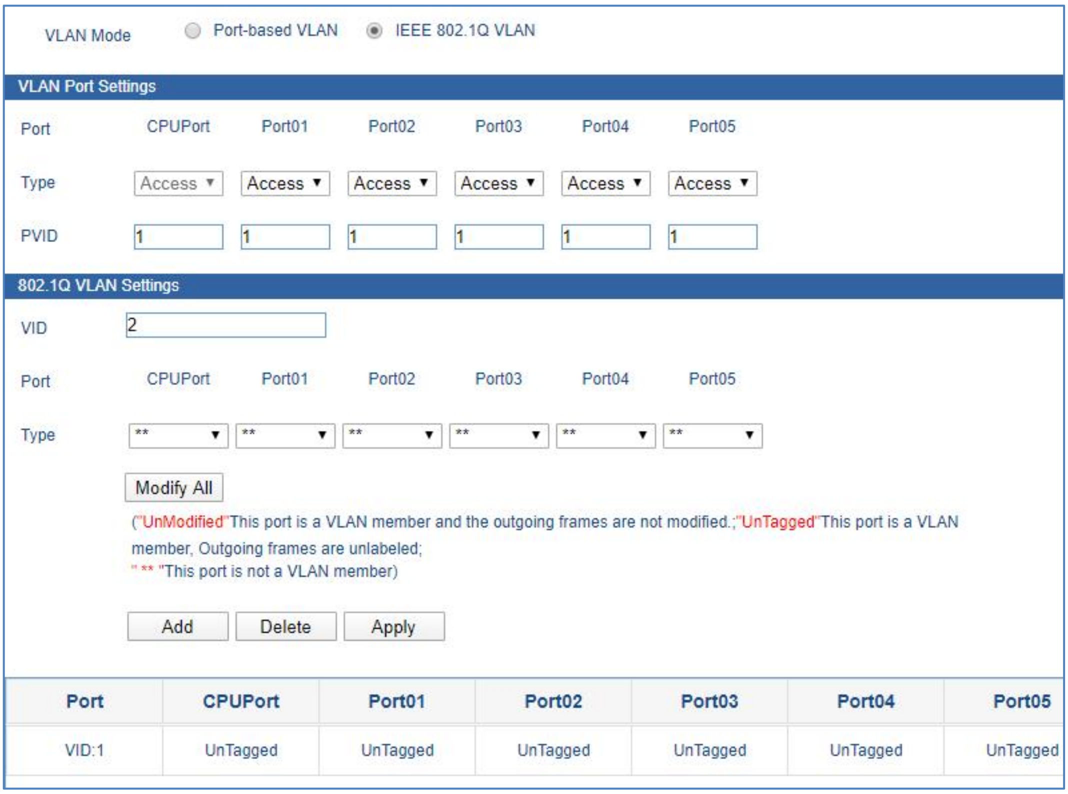
Step 4 Select VLAN member on the check box of “Join Port”, such as select port 2 and port 3.

Step 5 Click “Add/Edit”.

Step 6 Click “Apply”, port 2 and port 3 are divided into VLAN3, port 2 and port 3 that belong to the same VLAN can transmit data to each other.

Interface Description: VLAN based on 802.1Q

Interface screenshot of VLAN based on 802.1Q as follows:



The main element configuration description of 802.1Q Vlan interface:

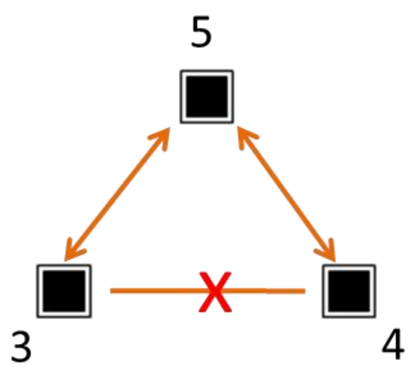
Interface Element	Description
VLAN Port Settings	**Port type and PVID settings column**
Port	Port number of the device.
Type	Configure the link type of port, there are two types as follows: ● Access: the port can only belong to 1 VLAN and is generally used for connecting user equipments. ● Trunk: the port can belong to multiple VLAN; it can receive and send multiple VLAN messages. And it's generally used for connecting network equipments.
PVID	PVID (Port Default VLAN ID) port default VLAN ID, value range is 1-4094. Note: • If the port type is "access", PVID will replace the "VLAN ID" fields in the message. • If the port type is "trunk" and message is untagged, PVID will replace the "VLAN ID" fields in the message. • If the port type is "trunk" and message is tagged, the

Interface Element	Description
	"VLAN ID" fields in the message will be reserved.
802.1Q VLAN Settings	**802.1Q VLAN Entry Settings Column**
VID	Port forwarding rule number, value range is 1-4094. Note: As for two ports that belong to the same VID; two ports with the same "VLAN ID" can communicate with each other.
Type	There are three types of "VLAN ID" for data frames sent out by the port: ● Unmodify: 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,
Modify All	Quickly and simultaneously modify all member types.
Add	Add configured VLAN to VLAN member list.
Delete	Delete a VLAN item in the selected member list.
Apply	Save VLAN configuration information.

5.1.1 Instance: typical VLAN configuration

Instance

Suppose that the switch port 3, 4 and 5 have the following requirements: Port 3 and Port 5 communicate with each other. Port 4 and Port 5 communicate with each other. Port 3 and Port 4 cannot communicate with each other, as the picture below. Do not consider other ports, how to set the VLAN?



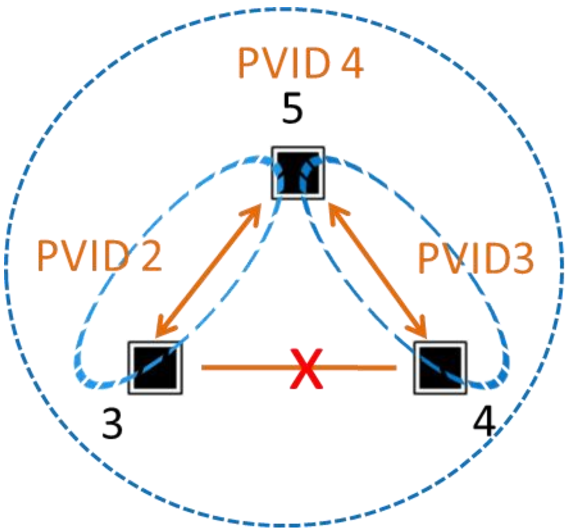
Instance analysis

Configure the “Type” of Port3, Port4 and Port5 as Access. Port3, Port 4 and Port 5 are set with different forwarding entries; forwarding entries can enable the communication between two ports.

Analyze the port forwarding entries design as below:

- Port3
  Port3 and Port5 can communicate with each other. Port3 forwarding entries include Port3 and Port5. Therefore, a forwarding entry PVID3 is designed, including Port 3 and Port 5. Configure the "Type" of Port 3 and Port 5 to Untagged.
- Port 4
  Port 4 and Port 5 can communicate with each other. Port 4 forwarding entries include Port 4 and Port 5. Therefore, a forwarding entry PVID4 is designed, including Port 4 and Port 5. Configure the "Type" of Port 4 and Port 5 to U.
- Port5
  Port 5 and Port 3, Port 4 can communicate with each other, Port 5 forwarding entries include Port 3, Port 4 and Port5. Therefore, design a forwarding entry PVID5, including Port 3, Port 4. Configure the "Type" of Port 3 and Port 4 to U.

According to the forwarding entry analysis of Port 3, Port 4 and Port 5, forwarding entry design picture as follows:



Operation Steps

Step 1 Open “Main Menu > L2 Feature > VLAN”.

Step 2 On the displayed VLAN setting interface, configure the "Type" of Port3, Port4 and Port5 as Access on the column of "VLAN Port Settings".

Step 3 On the column of "VLAN Port Settings", enter the default VLAN "PVID" of Port3, Port4 and Port5 as follows: 2, 3, 4.

Step 4 On the column of "802.1Q VLAN Settings", enter 2 in the "VID" text box of creating VLAN entry.

Step 5 On the drop-down list of "Member Type":

1. Configure the "Type" of Port3 as Untagged.
2. Configure the "Type" of Port5 as Untagged.

Step 6 Click "Add" button to add VLAN entry to the "Port".

Step 7 On the column of "802.1Q VLAN Settings", enter 3 in the "VID" text box of creating VLAN entry.

Step 8 Conduct following operations on the "Type" setting row of "802.1Q VLAN Settings":

1. Configure the "Type" of Port4 as Untagged.
2. Configure the "Type" of Port5 as Untagged.

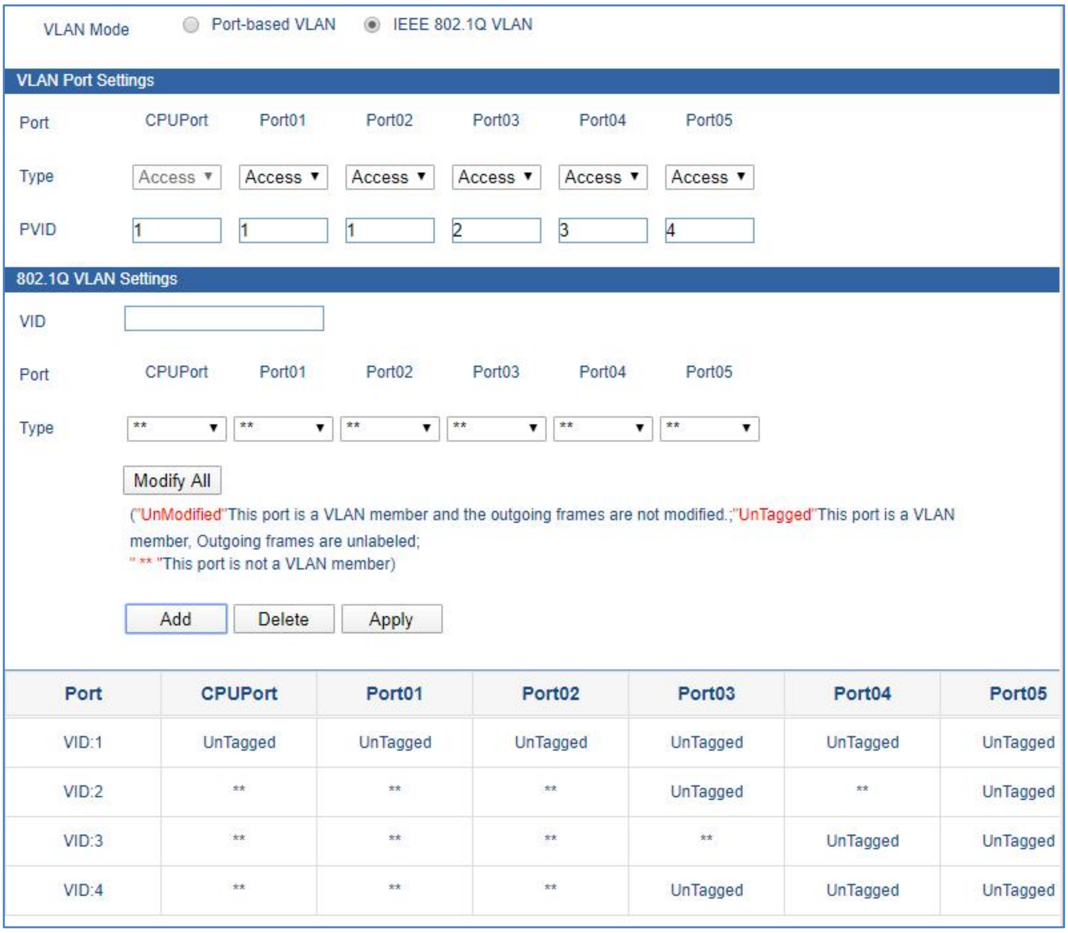
Step 9 Click "Add" button to add VLAN entry to the "Port".

Step 10 On the column of "802.1Q VLAN Settings", enter 4 in the "VID" text box of creating VLAN entry.

Step 11 On the drop-down list of "Member Type":

1. Select the "Type" of Port3 as Untagged.
2. Select the "Type" of Port4 as Untagged.
3. Select the "Type" of Port5 as Untagged.

Step 12 Click "Add" button to add VLAN entry to the "Port".



Step 13 Click “Apply”.

Step 14 Enter “Main Menu > System Management > Device Address”.

Step 15 On the column of “Device Reboot”, click the button of “Reboot”.

Step 16 End.

5.2 Multicast Filtering

5.2.1 IGMP Snooping

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.

Function Description

On the “IGMP Snooping” page, user can:

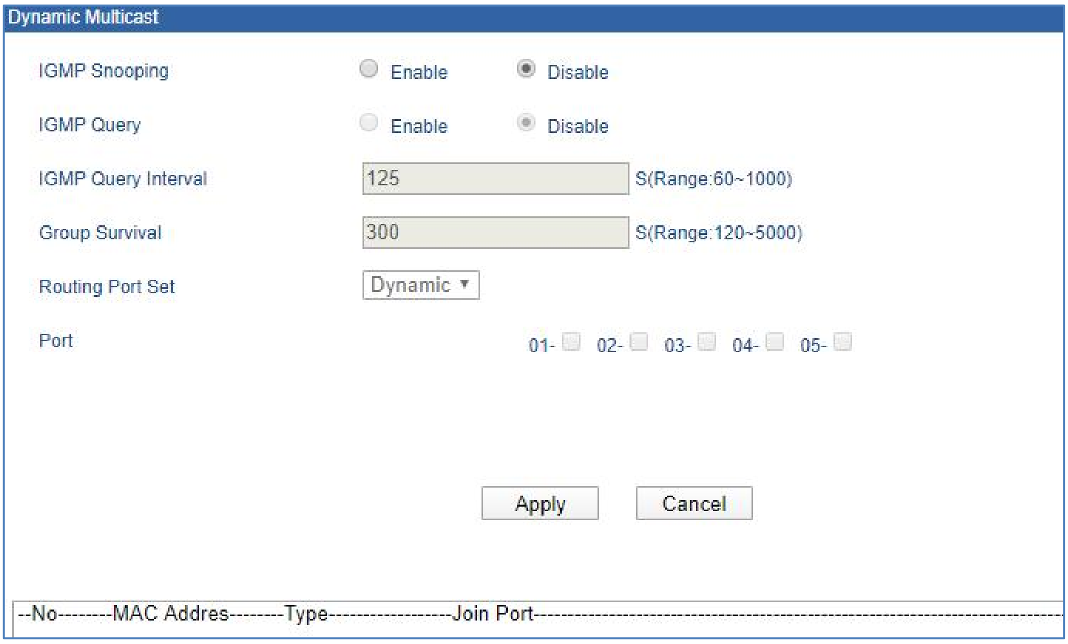
- Enable/disable IGMP Snooping;
- Enable/disable IGMP Snooping inquire;
- Set IGMP Snooping polling interval.

Operation Path

Open in order: “Main Menu > L2 Feature > Multicast Configuration > Dynamic Multicast”.

Interface Description

IGMP Snooping interface as below:



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 60~1000s.
Group survival	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 120-5000s.
Routing port set	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	Device Ethernet port list check box.

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.

5.2.2 Static Filtering

Static multicast filtering is used to set up static MAC address forwarding ports. One or more forwarding ports can be specified. Static MAC Address requests a valid input from user. If the input is a invalid MAC address, a message warning would pop up.

Function Description

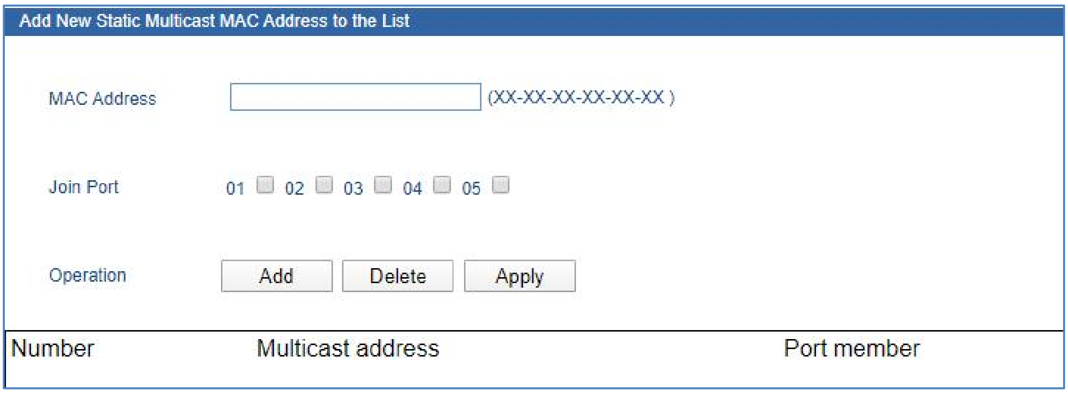
On the page of “Static Multicast”, user can configure the forwarding port list of static multicast.

Operation Path

Open in order: “Main Menu > L2 Feature > Multicast Configuration > Dynamic Multicast”.

Interface Description

Static filtering interface as follows:



Main elements configuration description of static filtering interface:

Interface Element	Description
MAC Address	Input "MAC Address", and the format should be "XX-XX-XX-XX-XX-XX". Note: • Low-order of the highest byte of multicast MAC address is 1, please don't input non-multicast address. • Space and other illegal characters are not allowed for address format, otherwise alarm message will pop up.
Join Port	Tick the check box of corresponding port, it represents that corresponding port joins in the static multicast MAC address.
Operation	Add, delete or apply the configuration information of static multicast filtering.

Warning

- Static multicast filtering has a great impact on multicast data packets forwarding via network, please don't use it unless the added address is exactly right.
- Multicast addresses of 0180C20000xx and 01005E0000xx are reserved for the device or protocol, please don't use them.
- IGMP dynamic learning won't update statically typed multicast address, static multicast forwarding table is more of a security mechanism.

Example: Static Multicast Filtering Configuration

For example: configure the filtering port of multicast address 01-00-00-00-00-01 as 01, 02 and 03.

The operation steps are as follows:

Step 1 Open “Main Menu > L2 Feature > Multicast Configuration > Static Multicast”.

Step 2 On the text box after “MAC Address”, input “01-00-00-00-00-01”.

Step 3 On the row of “Join Port”:

1 Tick the check box after “1-”;

2 Tick the check box after “2-”;

3 Tick the check box after “3-”.

Step 4 Click “Add”.

Step 5 Configured static filtering is displayed in the display frame on the bottom of the page, click “Apply”.

Step 6 End.

6 QoS

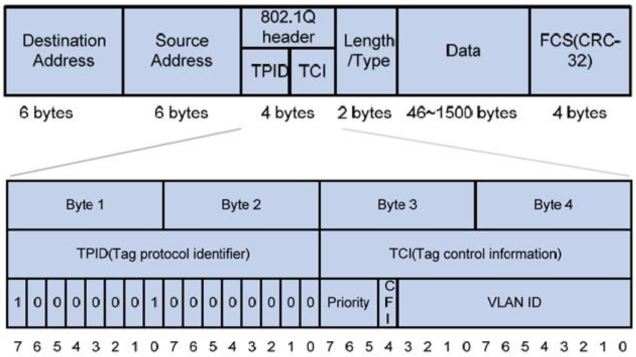
6.1 QoS Classification

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.

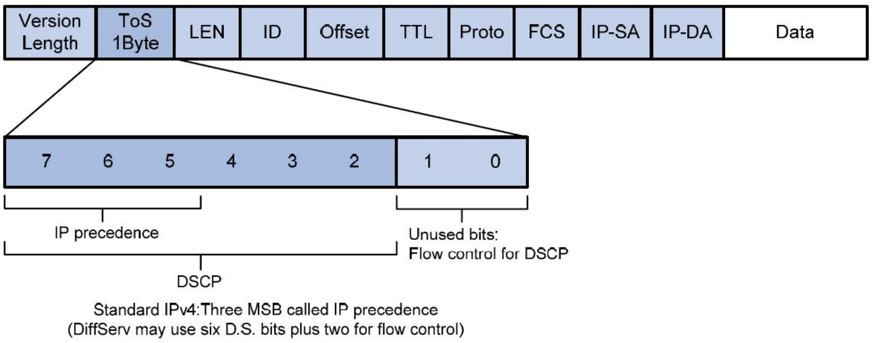
Priority is used to tag the priority of message transmission.

- 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

On the page of QoS Classification, user can set:

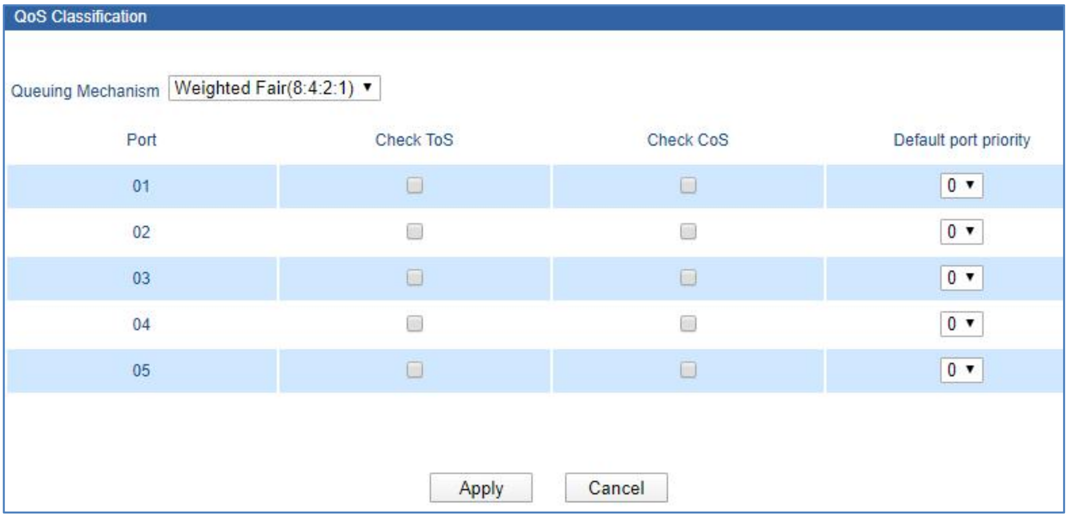
- Queuing mechanism
- Enable ToS
- Enable CoS
- Priority.

Operation Path

Open in order: “Main Menu > QoS > QoS Classification”.

Interface Description

Screenshot of QoS Classification interface:



The main element configuration description of QoS classification interface:

Interface Element	Description
Queuing 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 ToS	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.
Default 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.

Instance: QoS configuration

For example:

- Set port 1's queuing mechanism as "Weight Fair (8:4:2:1)", adopts ToS priority.

Operation Steps

Step 1 Open "Main Menu > QoS > QoS Classification".

Step 2 On the page of classification, choose "Weight Fair (8:4:2:1)" in queuing mechanism.

Step 3 On the line of port 1, check the checkbox of "inspect ToS".

Step 4 Click "Apply".

Step 5 End.

6.2 CoS Mapping

Function Description

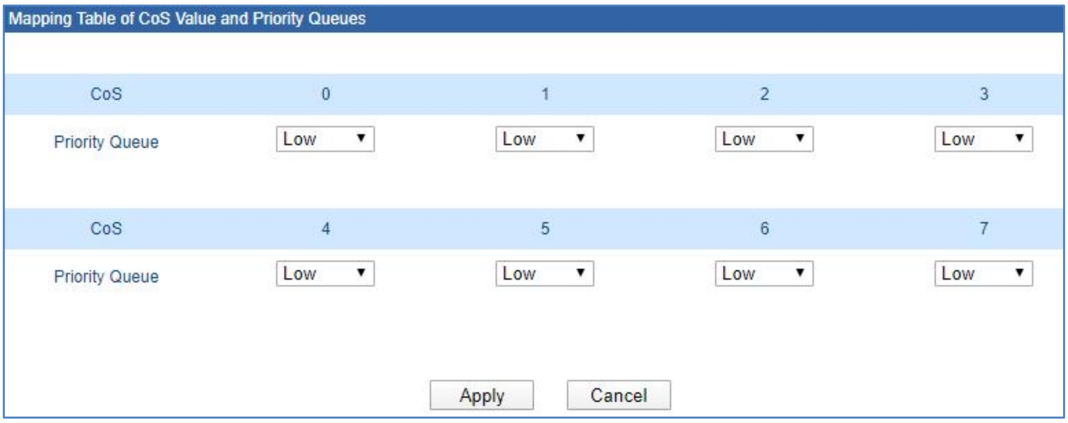
On the page of "CoS Mapping", user can configure mapping between CoS value and priority queues.

Operation Path

Open in order: "Main Menu > QoS > QoS Mapping".

Interface Description

Screenshot of QoS Mapping interface:



The main element configuration description of QoS mapping interface:

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

Instance: CoS mapping configuration

For example:

- When the CoS value is set to 0 and 1, the corresponding priority queue is Low
- When the CoS value is set to 2 and 3, the corresponding priority queue is Normal
- When the CoS value is set to 4 and 5, the corresponding priority queue is Medium
- When the CoS value is set to 6 and 7, the corresponding priority queue is High

Operation Steps

Step 1 Open “Main Menu > QoS > CoS Mapping”.

Step 2 In the table of CoS value and priority queue mapping of CoS mapping page:

1. When the CoS value is “0”，choose Low as the corresponding priority.
2. When the CoS value is “1”，choose Low as the corresponding priority;
3. When the CoS value is “2”，choose Normal as the corresponding priority.
4. When the CoS value is “3”，choose Normal as the corresponding priority;

5 When the CoS value is “4”，choose Medium as the corresponding priority.

6 When the CoS value is “5”，choose Medium as the corresponding priority;

7 When the CoS value is “6”，choose High as the corresponding priority.

8 When the CoS value is “7”，choose High as the corresponding priority.

Step 3 Click “Apply”.

Step 4 End.

6.3 ToS Mapping

Function Description

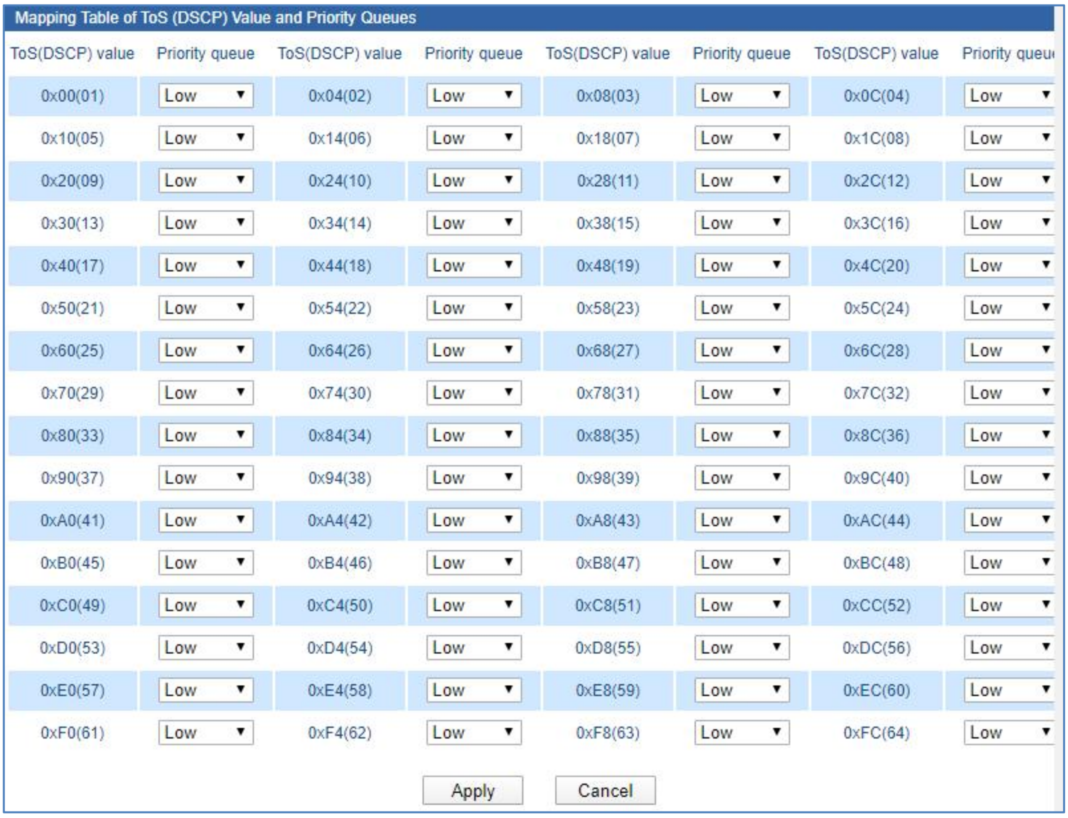
On the page of “ToS Mapping”, user can configure mapping between CoS value and priority queue.

Operation Path

Open in order: “Main Menu > QoS > ToS Mapping”.

Interface Description

Screenshot of ToS Mapping interface:



Mapping Table of ToS (DSCP) Value and Priority Queues

ToS(DSCP) value	Priority queue	ToS(DSCP) value	Priority queue	ToS(DSCP) value	Priority queue	ToS(DSCP) value	Priority queu
0x00(01)	Low	0x04(02)	Low	0x08(03)	Low	0x0C(04)	Low
0x10(05)	Low	0x14(06)	Low	0x18(07)	Low	0x1C(08)	Low
0x20(09)	Low	0x24(10)	Low	0x28(11)	Low	0x2C(12)	Low
0x30(13)	Low	0x34(14)	Low	0x38(15)	Low	0x3C(16)	Low
0x40(17)	Low	0x44(18)	Low	0x48(19)	Low	0x4C(20)	Low
0x50(21)	Low	0x54(22)	Low	0x58(23)	Low	0x5C(24)	Low
0x60(25)	Low	0x64(26)	Low	0x68(27)	Low	0x6C(28)	Low
0x70(29)	Low	0x74(30)	Low	0x78(31)	Low	0x7C(32)	Low
0x80(33)	Low	0x84(34)	Low	0x88(35)	Low	0x8C(36)	Low
0x90(37)	Low	0x94(38)	Low	0x98(39)	Low	0x9C(40)	Low
0xA0(41)	Low	0xA4(42)	Low	0xA8(43)	Low	0xAC(44)	Low
0xB0(45)	Low	0xB4(46)	Low	0xB8(47)	Low	0xBC(48)	Low
0xC0(49)	Low	0xC4(50)	Low	0xC8(51)	Low	0xCC(52)	Low
0xD0(53)	Low	0xD4(54)	Low	0xD8(55)	Low	0xDC(56)	Low
0xE0(57)	Low	0xE4(58)	Low	0xE8(59)	Low	0xEC(60)	Low
0xF0(61)	Low	0xF4(62)	Low	0xF8(63)	Low	0xFC(64)	Low

Apply Cancel

The main element configuration description of ToS mapping interface:

Interface Element	Description
ToS (DSCP)	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

Instance: ToS mapping configuration

For example:

- When the ToS value is set to 0x00~0x3C, the corresponding priority is Low.
- When the ToS value is set to 0x40~0x7C, the corresponding priority is Normal.
- When the ToS value is set to 0x80~0xBC, the corresponding priority is Medium.
- When the ToS value is set to 0xC0~0xFC, the corresponding priority is High.

Operation Steps

Step 1 Open “Main Menu > QoS > ToS Mapping”.

Step 2 In the table of ToS value and priority queue mapping of ToS mapping page:

1. When the “ToS value” is “0x00”~“0x3C”, choose Low as the corresponding priority.
2. When the “ToS value” is “0x40”~“0x7C”, choose Normal as the corresponding priority.
3. When the “ToS value” is “0x80”~“0xBC”, choose Medium as the corresponding priority.
4. When the “ToS value” is “0xC0”~“0xFC”, choose High as the corresponding priority.

Step 3 Click “Apply”.

Step 4 End.

7 Link Backup

7.1 Rapid Ring

The ring network protocols supported by the switch are Ring and RSTP.

- Ring

  SW-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.
- RSTP

  To solve the loop problem in switching network, Spanning Tree Protocol (STP) is proposed. Because of the slow speed of STP topological convergence, IEEE released 802.1W standard in 2001 which has defined RSTP (Rapid Spanning Tree Protocol). RSTP is improved on the basis of STP to realize the fast convergence of network topology (the fastest rate can be less than 1 second). Devices running STP/RSTP exchange information to discover loops on the network and block some ports. The ring network structure is pruned into tree network structure without loop to prevent messages from looping in ring network and that the packet processing capabilities of switches is not impacted by receiving the same messages.

  Working process of STP:

- First is to select the root bridge The selection is based on the bridge ID, which is a combination of bridge priority and bridge MAC address. The smallest bridge ID will become the root bridge in the network, and all its ports will be connected to the downstream bridge, so the port role will become the specified port.
- Next, the downstream bridges connecting to the root bridge will each select a "strongest" branch as the path to the root bridge, and the role of the corresponding port will become the root port. Loop this process to the edge of the network, the specified port and the root port are determined and a tree is formed.
- when the spanning tree is stabled (default value is 30 seconds) after a while, the specified port and root port will enter forwarding state, and other ports will enter block state.
- The STP BPDU is sent periodically from the specified ports of each bridge to maintain the state of the link. If the network topology changes, the spanning tree will recalculate and the port state will change together.

Function Description

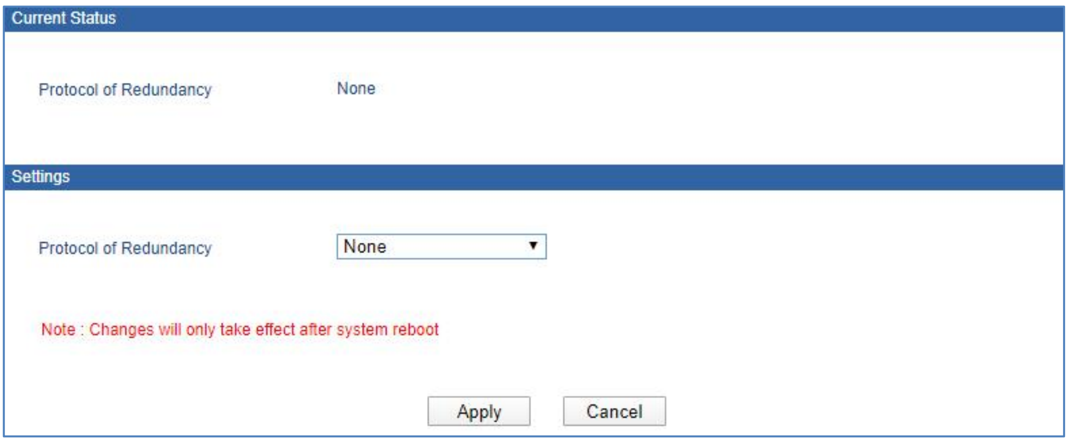
On the "Rapid ring" page, user can choose redundancy protocol and configure the ring network under this protocol quickly.

Operation Path

Open in order: "Main Menu > Redundancy > Rapid Ring".

Interface Description

Initial rapid ring interface as follows:



The main element configuration description of initial rapid ring interface:

Interface Element	Description
Current status	**Current status bar**
Protocol of Redundancy	The current status of ring network protocol of the device.
Settings	**Settings bar**
Protocol of Redundancy	Choose the corresponding redundancy protocol. Options: ● None: it means that the ring network function is disabled. ● Ring V3: supports single ring, coupling ring, chain and Dual_homing; ● RSTP (IEEE 802.1W/1D): rapid spanning tree.

Function Description of Ring V3

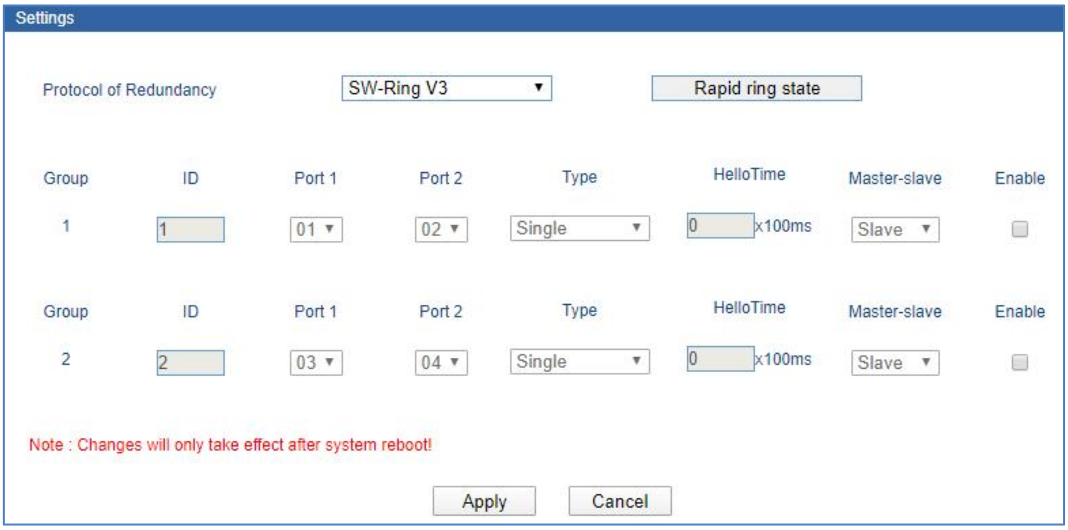
On the “rapid ring” page, user can choose Ring redundancy protocol and configure the ring network under this protocol quickly.

Operation Path

Open in order: “Main Menu > Redundancy > Rapid Ring”. Choose “Ring V3” in the drop-down list of “protocol of redundancy”.

Interface Description

Ring network interface as follows:



The main element configuration description of Ring network interface:

Interface Element	Description
Rapid ring state	Click “rapid ring state” to check the ring state of current ring network group configuration.
Group	Support Group 1-2, it means that the device supports up to 2 groups.
ID	When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID.
Port1	The network port 1 on the switch device used to form a ring.
Coupling port	When the ring type is “Couple”, the coupling port would be the one connects different network ID.
Port2	Port 2 can be used for the formation of ring network in switch.
Coupling control port	When the ring type is “Couple”, the control port would be the one in the link of the intersection of two rings.
Ring Type	According to the requirement in the scene, user can choose different ring type. ● Single: single ring, using a continuous ring to connect all device together. ● Couple: couple ring is a redundant structure used for connecting two independent networks. ● Chain: chain can enhance user’s flexibility in constructing all types of redundant network topology via an advanced software technology. ● Dual-homing: two adjacent rings share one switch. User could put one switch in two different networks or two different switching equipments in one network.
HelloTime	Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends information packet to adjacent device for confirming the connection is normal or not.
Master-slave	Single ring has master/slave device option. One-Master Multi-Slave mode is recommended in one single ring. When the device is set as master device and one end of it is backup link, it can enable backup link to ensure the normal operation of the network when failure occurs in ring network.
Enable	Enable or disable the corresponding ring group.

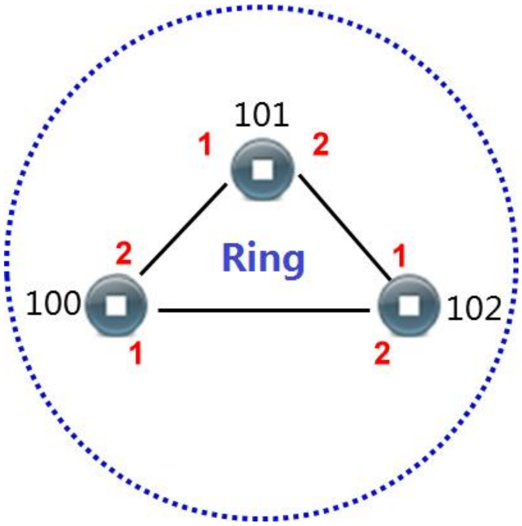
Now introduce the creation process respectively according to different ring network:

- Create single ring
- Create coupling ring
- Create chain
- Create rapid spanning tree

7.1.1 Instance: create single ring

Instance

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

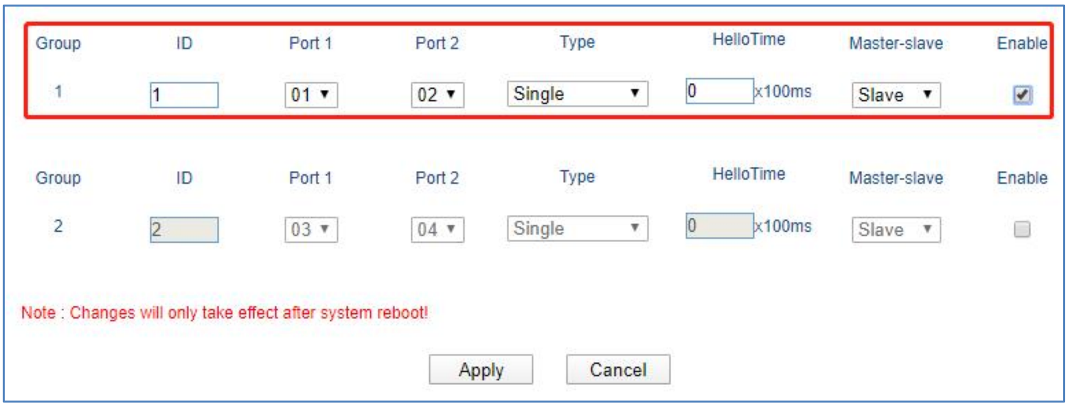
Configuring Device 100, 101 and 102 in the following steps:

Step 1 Choose “Main Menu > Redundancy > Rapid Ring”.

Step 2 In the setting area of the “Rapid Ring” page, choose “Ring V3” as the “protocol of redundancy”.

Step 3 Check the box of “Enable” in “Group 1”.

Step 4 Choose “Single” in the drop-down list of “Type” of “Group 1”.



Step 5 Enter “1” into the “ID” textbox of “Group 1”.

Step 6 Set “Port 1” to “01” and “Port 2” to “02” separately.

Note:

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

Step 7 Click “Apply”. Enter “Main Menu > System Management > Device Address”.

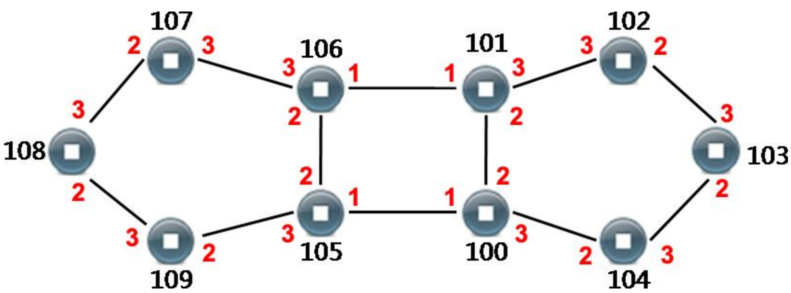
Step 8 On the column of “Device Reboot”, click the button of “Reboot”.

Step 9 End.

7.1.2 Instance: create coupling ring

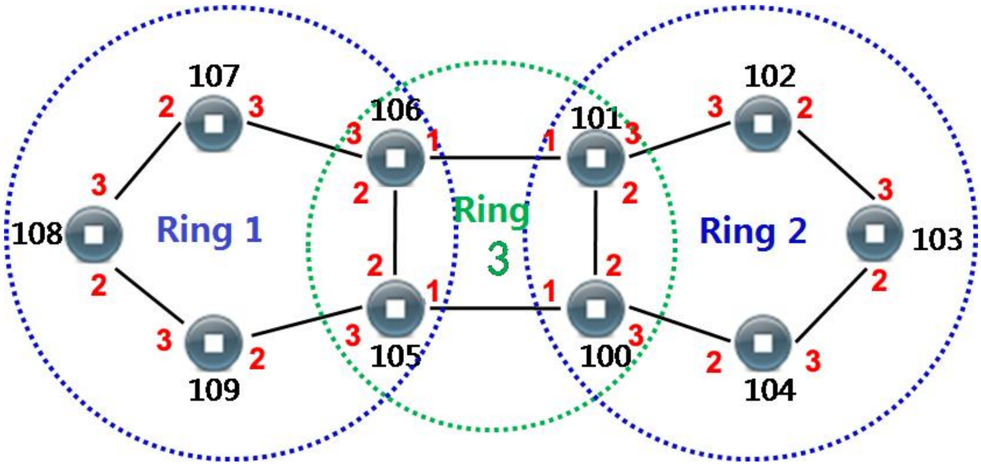
Instance

For example: creating coupling ring. Its basic architecture is shown as below:



Instance Analysis

We can get the following picture by analyzing the coupling ring above.



There are three rings in coupling ring. Ring 1 and Ring 2 intersect Ring 3 respectively. When setting ring in WEB interface, we can set Ring 1 and Ring 2 as single ring, Ring 3 as coupling ring. In coupling ring, we set the port in the link where the two rings intersect as control port. The Port 2 of Device 105 in the picture above is the control port. The analyses of each switch are displayed as follows:

- 105, 106, 107, 108 and 109 are in Ring 1; ring network ports are Port 1 and Port 2; single ring;
- 100, 101, 102, 103 and 104 are in Ring 2; ring network ports are Port 1 and Port 2; single ring;
- 100, 101, 105 and 106 are in Ring 3. It is a coupling ring. Port 1 is coupling port. Port 2 is control port.

Operation Step 1: configuring Ring 1 in WEB interface

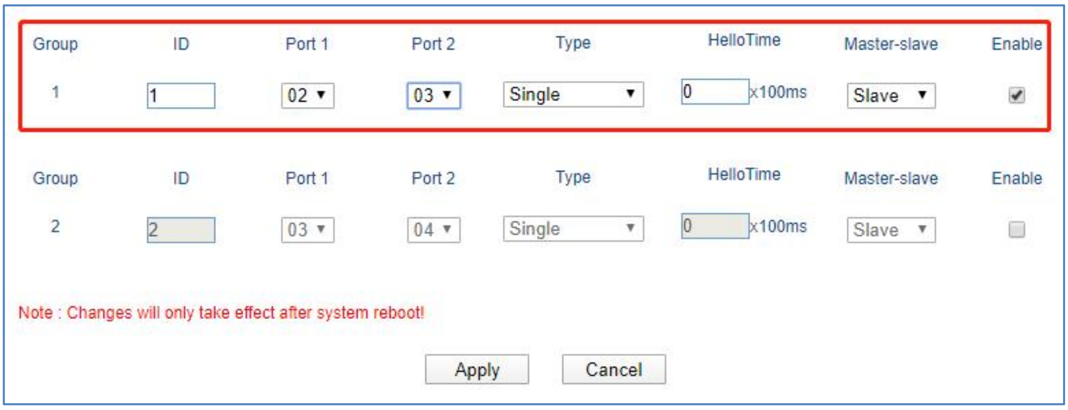
Configuring Device 105, 106, 107, 108 and 109 in the following steps respectively.

Step 1 Choose “Main Menu > Redundancy > Rapid Ring”.

Step 2 In the setting area of the “Rapid Ring” page, choose “Ring V3” as the “protocol of redundancy”.

Step 3 Check the box of “Enable” in “Group 1”.

Step 4 Choose “Single” in the drop-down list of “Type” of “Group 1”.



Step 5 Enter “1” into the “ID” textbox of “Group 1”.

Step 6 Set “Port 1” and “Port 2” to “2” and “3” respectively.

Note:

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

Step 7 Click “Apply”. Enter “Main Menu > System Management > Device Address”.

Step 8 On the column of “Device Reboot”, click the button of “Reboot”.

Step 9 End.

Operation Step 2: configuring Ring 2 in WEB interface

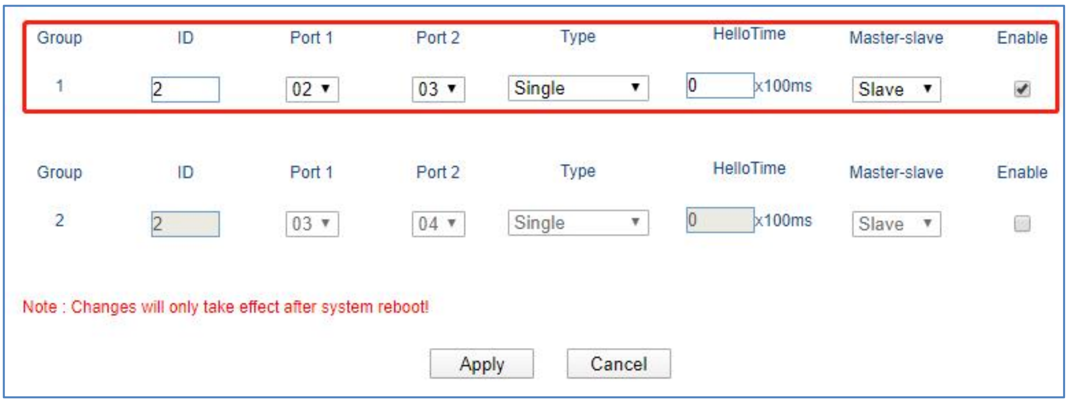
Configuring Device 100, 101, 102, 103 and 104 in the following steps respectively.

Step 1 Choose “Main Menu > Redundancy > Rapid Ring”.

Step 2 In the setting area of the “Rapid Ring” page, choose “Ring V3” as the “protocol of redundancy”.

Step 3 Check the box of “Enable” in “Group 1”.

Step 4 Choose “Single” in the drop-down list of “Type” of “Group 1”.



Step 5 Enter “2” into the “ID” textbox of “Group 1”.

Step 6 Set “Port 1” and “Port 2” to “2” and “3” respectively.

Note:

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

Step 7 Click “Apply”. Enter “Main Menu > System Management > Device Address”.

Step 8 On the column of “Device Reboot”, click the button of “Reboot”.

Step 9 End.

Operation Step 3: configuring Ring 3 in WEB interface

Configuring Device 100, 101, 105 and 106 in the following steps respectively.

Step 1 Choose “Main Menu > Redundancy > Rapid Ring”.

Step 2 In the setting area of the “Rapid Ring” page, choose “Ring V3” as the “protocol of redundancy”.

Step 3 Check the box of “Enable” in “Group 2”.

Step 4 Choose “Couple” in the drop-down list of “Type” of “Group 2”.

Step 5 Enter “3” into the “ID” textbox of “Group 2”.

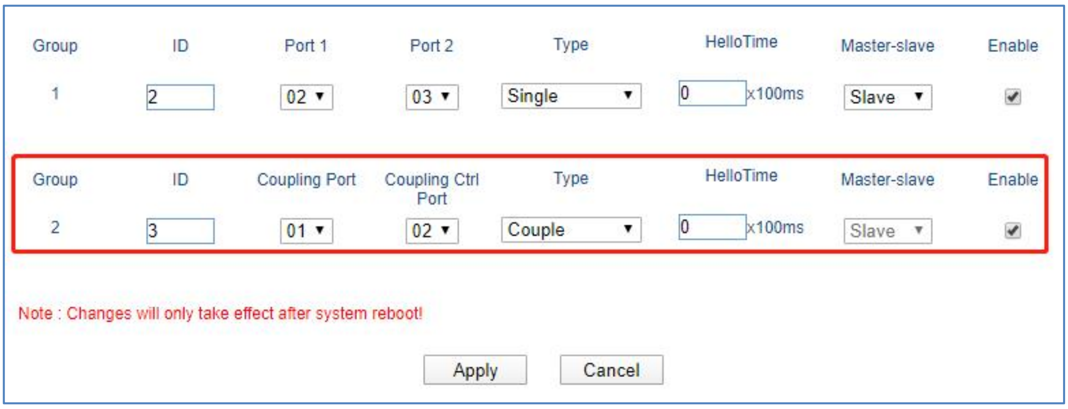
Step 6 Choose “1” in the drop-down list of “Coupling Port” of “Group 2”.

Step 7 Choose “2” in the drop-down list of “Coupling Control Port” of “Group 2”.

Step 8 Click “Apply”. Enter “Main Menu > System Management > Device Address”.

Step 9 On the column of “Device Reboot”, click the button of “Reboot”.

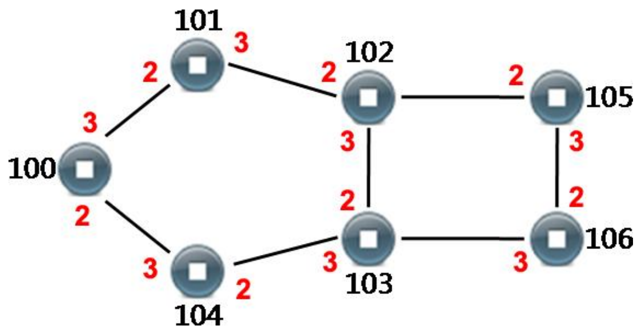
Step 10 End.



7.1.3 Instance: creating chain

Instance

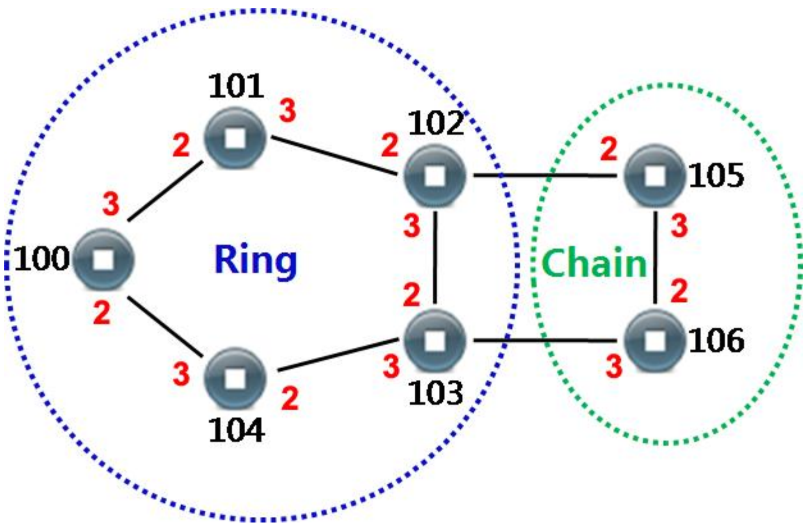
For example: creating chain. Its basic architecture is shown as below:



Instance Analysis

Basic framework, we can make the following analyses:

- 100, 101, 102, 103 and 104 are in the ring. The ring network ports are 2 and 3.
- Device 105 and 106 are in the chain. The ring network ports are 2 and 3.



Operation Step 1: creating ring

Configuring Device 100, 101, 102 and 103 in the following steps respectively.

Step 1 Choose “Main Menu > Redundancy > Rapid Ring”.

Step 2 In the setting area of the “Rapid Ring” page, choose “Ring V3” as the “protocol of redundancy”.

Step 3 Check the “Enable” box in the “Group 1”.

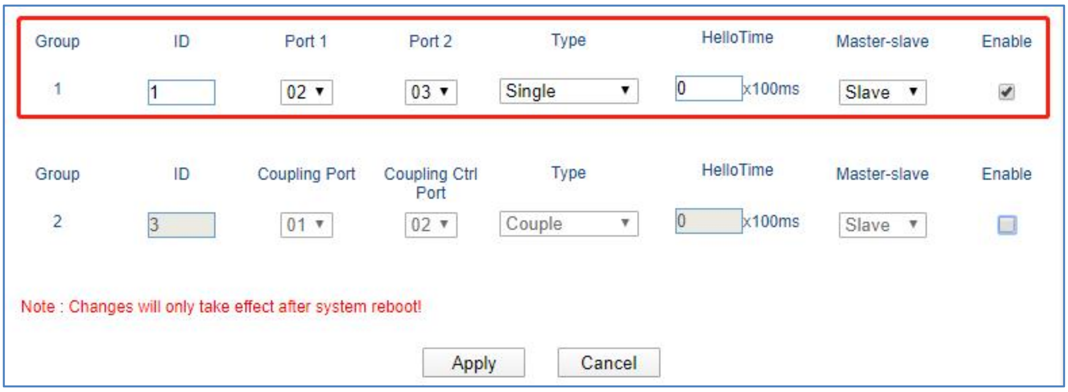
Step 4 In the “settings” area of “Rapid Ring”:

1 Set “Type” to “Single”;

2 Set “ID” to “1”;

3 Set “Port 1” to “2”;

4 Set “Port 2” to “3”;



Step 5 Click “Apply”.

Step 6 Enter “Main Menu > System Management > Device Address”.

Step 7 On the column of “Device Reboot”, click the button of “Reboot”.

Step 8 End.

Operation Step 2: creating chain

Configuring Device 105 and 106 in the following steps respectively.

Step 1 Choose “Main Menu > Redundancy > Rapid Ring”.

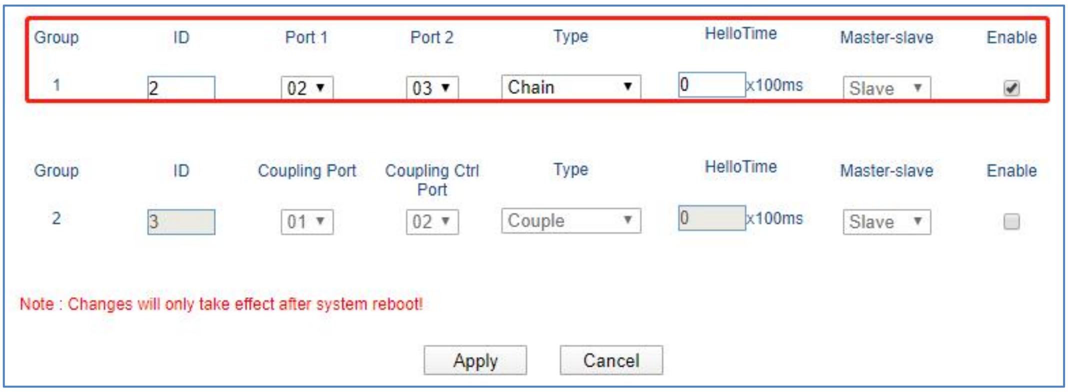
Step 2 In the setting area of the “Rapid Ring” page, choose “Ring V3” as the “protocol of redundancy”.

Step 3 Check the “Enable” box in the “Group 1”.

Step 4 In the “Settings” area of “Rapid Ring” page, set the “Type” to “Chain”.

Step 5 In the “Settings” area of “Rapid Ring” page, set the “ID” to “2”.

Step 6 Set “Port 1” to “2” and set “Port 2” to “3”.



Note

The chain + single ring combination could be formed by using configured ring network port of chain ring device to connect the normal port of single ring device.

Step 7 Click “Apply”.

Step 8 Enter “Main Menu > System Management > Device Address”.

Step 9 On the column of “Device Reboot”, click the button of “Reboot”.

Step 10 End.

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.

7.1.4 Creating Spanning Tree

Function Description

On the “Rapid ring” page, user can choose “RSTP (IEEE 802.1W/1D)” as redundancy protocol to create spanning tree quickly.

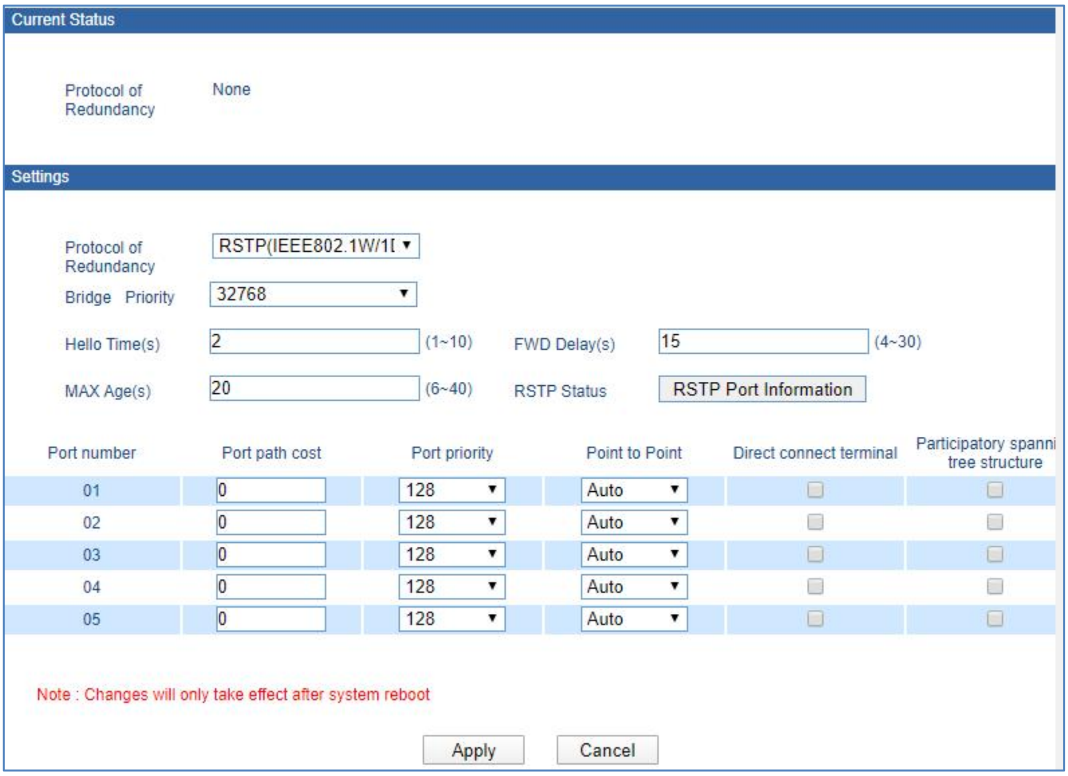
Operation Path

Open in order: “Main Menu > Link backup > Rapid Ring > Protocol of Redundancy > RSTP (IEEE 802.1W/1D)”.

Interface Description

RSTP interface as follows:

The main element configuration description of RSTP interface:



Interface Element	Note
Redundancy protocol	Choose the algorithm of redundancy protocol, options are: ● None: it means that the ring network function is disabled. ● Ring V3: supports single ring, coupling ring, chain and Dual_homing;

Interface Element	Note
	• RSTP (IEEE 802.1W/1D): rapid spanning tree.
Bridge priority	The priority of bridge. Note: In STP/RSTP network, the device with smallest bridge ID would be elected as root bridge. The bridge ID consists of bridge priority and bridge MAC address.
Hello time	The transmission time interval of the BPDU data packet. Note: The protocol message that STP/RSTP adopts is BPDU (Bridge Protocol Data Unit).
FWD delay	The forward delay time that the port of switch maintains in transition state (listening and learning). Note: STP/RSTP adopts a mechanism of state transition. The newly-selected root port and specified port have to go through twice the Forward Delay time to enter the forwarding state.
MAX age	The lifetime of BPDU packets.
RSTP status	Button, used for checking the current status of rapid spanning tree.
Port number	Display the device port number.
Cost	The path cost from network bridge to root bridge. Note: Path cost is a reference value for STP protocol to choose links. The path cost from a port to the root bridge is cumulated by the path cost it go through each port of each bridge.
Port priority	The priority of ports in bridge. The smaller the value, the higher the priority. Note: PID (Port ID) consists of two parts. The high 4 digits are port priorities, the low 12 digits are port numbers. In the case of same root path cost, it would not block the port with the smallest PID value, but the one with greater PID value.
P2P	The directly connected switch port, options are: • Yes; • No; • Auto: adopt negotiation mechanism that could implement quick conversion of port states.
Direct connection terminal	The switch that is on the edge of network and connects to the terminal devices.
Port STP	Checking this checkbox. It represents participating in the operation of spanning tree protocol.

RSTP status interface as follows:

The main element configuration description of RSTP status interface:

Interface Element	Description
Root information	**The display bar of root information table**
Local ID	It displays the priority of this switch and MAC address information ID.
Root ID	It displays the priority of the root switch and MAC address information ID.
Root port	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 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.
Basic information	**The display bar of basic information table**
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 Cost	The path cost from network bridge to root bridge.

Interface Element	Description
P2P	The directly connected switch port.
Edge port	The port that directly connects to terminal instead of other switches.
Connected	It displays the network protocol of devices with connected ports.
Port Role	Root port, specified port, Alternate port and Backup port.
FWD 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.

Note

The settings of rapid spanning tree will take effect after rebooting the device.

8 LLDP

8.1 Parameters Configuration

At present, there are more and more types of network equipment and their configurations are complex. In order to enable devices from different manufacturers to find each other and interact with each other's systems and configuration information in the network, a standard information exchange platform is required.

LLDP (Link Layer Discovery Protocol) is created under such background, it provides a standard way of Link Layer Discovery, which can organize the main power, management address, device id, interface identification into different TLV (Type/Length/Value), and encapsulate them in LLDPDU (Link Layer Discovery Protocol Data Unit) and publish them to the neighbors that connect to itself directly. After receiving the Information, the neighbor saves them in the form of standard MIB (Management Information Base) for the network Management system to query and judge the communication status of link.

LLDP message sending mechanism

When the LLDP function is enabled, the device will periodically send LLDP messages to neighboring devices. If the local configuration of the device changes, the LLDP message is sent immediately to inform the neighbor device of the change of local information as soon as possible. For preventing abounding LLDP sending caused by frequent changes of local information, next message should be delayed to send out after sending a LLDP message.

LLDP message receiving mechanism

When enabling LLDP function, the device will check the validity of the received LLDP message and the TLV(Type/Length/Value) carried by it. After checking, the neighbor information will be saved in the local device, and the aging time of neighbor information in the local device will be set according to the TTL(Time To Live) Value carried by TLV in the LLDPDU(LLDP Data Unit) message. If the TTL value in the received LLDPDU is equal to zero, the neighbor information will be aged immediately.

Function Description

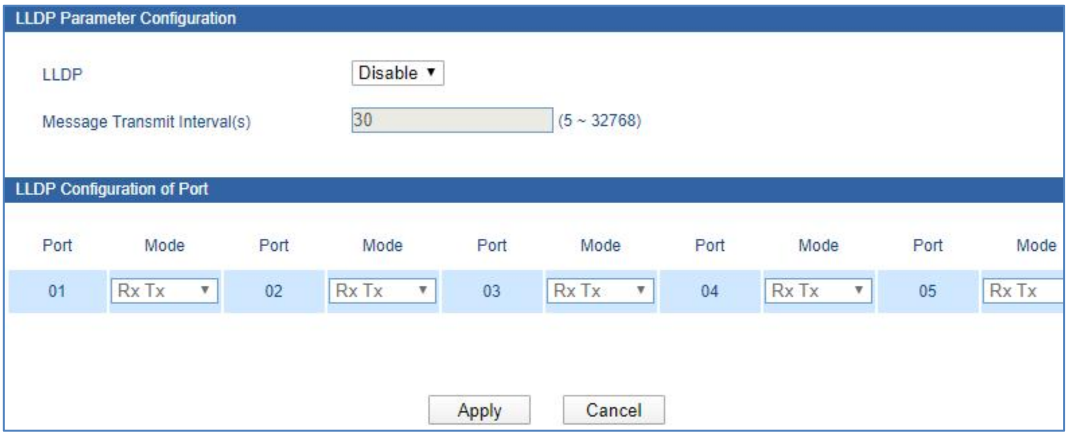
On the page of “Parameters Configuration”, user can configure LLDP function of the port and notify its device identity and performance in the local device.

Operation Path

Open in order: “Main Menu > System Management > LLDP > Parameters Config”.

Interface Description

Parameter configuration interface as follows:



Main elements configuration description of parameter configuration interface:

Interface Element	Description
LLDP	Enable/disable LLDP function.
message transmit interval	Interval time for messages sending is 5-32768s. For preventing abounding LLDP sending caused by frequent changes of local information, next message should be delayed to send out after sending a LLDP message.
Mode	LLDP function settings of each port, options are as follows: ● Disable: disable LLDP function. ● Tx Rx: send and receive LLDP message. ● Tx only: periodically send LLDP message to neighbor device. ● Rx only: check the validity of received LLDP and carried

Interface Element	Description
	TLV, and configure the ageing time of neighbor device in the local device according to TTL (Time To Live) value in TLV.

8.2 Neighbor Information

Function Description

On the page of “Neighbor Information”, user can check the following items discovered by the local port:

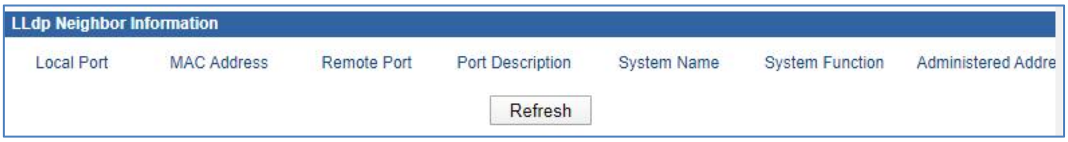
- MAC address;
- Remote port;
- Port description;
- System name;
- System function;
- Management address.

Operation Path

Open in order: " Main Menu > System Manage > LLDP > Neighbor Information".

Interface Description

Neighbor information interface as follows:



Main elements configuration description of neighbor information interface:

Interface Element	Description
Local port	Corresponding local port number of the device.
MAC Address	Discover corresponding MAC address of the neighbor device.
Remote port	Port number of neighbor device.
Port description	Port description information of the neighbor device.
System Name	System name of the neighbor device.
System function	System functions of the neighbor device.

Interface Element	Description
Management address	Management addresses information of the neighbor device. Management address is the address provided for network management system to identify and manage the network devices. Management address can definitely identify a device, which is convenient for the drawing of network topology and network management. Management address is released to public after being packaged in Management Address TLV of LLDP message.

9 Access Control

9.1 Password

Enterprises often require that the administrator of monitoring equipment and the administrator of the system or network should be two different roles, and their permissions should be separated, that is, the former is only responsible for the management of monitoring business, the latter is only responsible for the management of the system or network. The switch provides level management :

- Observer: check permissions.
- System Administrator: modify and check privilege

Function Description

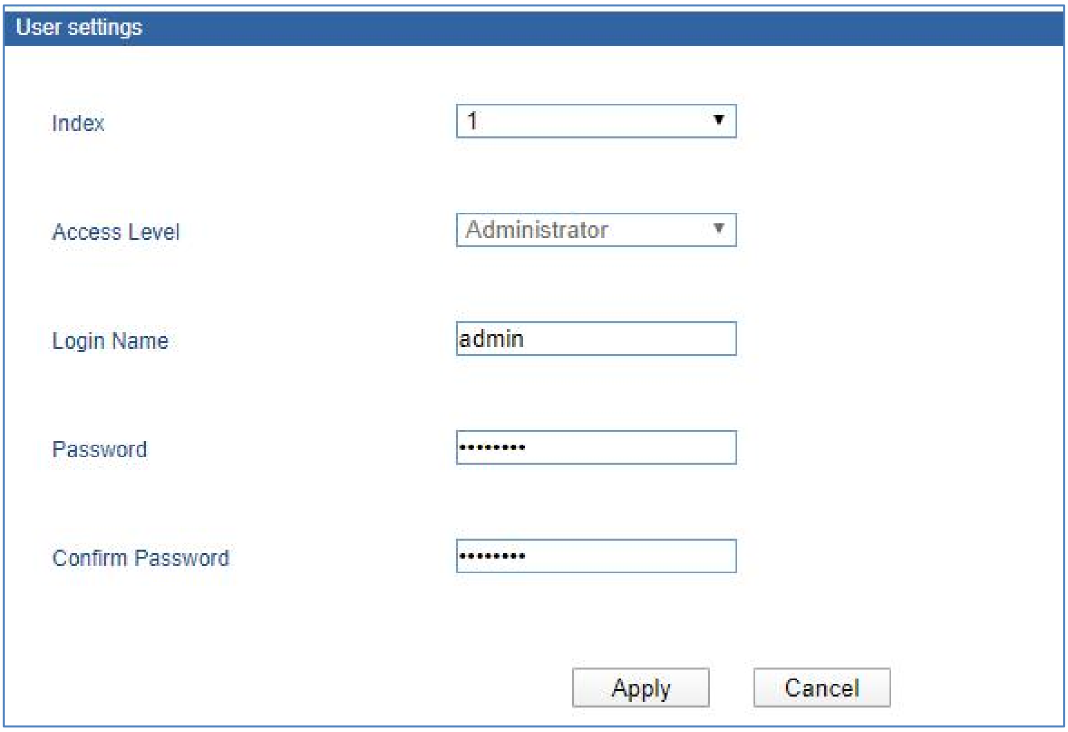
On the page of “Login Settings”, user can configure the login name, password and other parameters information of logging in to WEB configuration page.

Operation Path

Open in order: “Main Menu > Access control > Login settings”.

Interface Description

Login settings interface as follows:



The main element configuration description of login settings interface:

Interface Element	Description
Index	The index number is corresponding to the access level. • 1: administrator • 2: administrator or observer • 3: administrator or observer
Access level	Access level settings, options: • Administrator: check and modify permissions. • Observer: check permissions.
User name	Login name settings for the guest to log in to the WEB configuration interface.
Password	Login password settings for the guest to log in to the WEB configuration interface. Note: The password should be a combination of letters less than 16 bytes.
Confirm password	Confirm visitor password.

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”.

For instance: create administrator

For example: create a new administrator “admin8” and set the management password to “admin8”.

Operation Steps

Step 1 Log into Web configuration interface.

Step 2 Choose “Main Menu > Access Control > Login Settings”.

Step 3 On the “Login settings” page:

1 Choose “1” as “Index” number

2 Choose “administrator” as “access level”

3 Enter “admin8” as “login name”

4 Enter “admin8” as “password”

5 Enter “admin8” as “confirm password”.

Step 4 Click “Apply”.

Step 5 End.

10 Remote Monitoring

10.1 SNMP Configuration

SNMP (Simple Network Management Protocol)is a network management standard protocol widely used in TCP/IP networks. SNMP provides a way to manage devices by running network management software on a central computer (or network management workstation). Network administrators can use SNMP platform to complete information query, information modification and fault troubleshooting on any node on the network, and the work efficiency can be improved.

SNMP System consists of NMS (Network Management System), Agent Process, Management Object and MIB (Management Information Base) four parts.

- NMS plays the role of administrator in the network. It is a system that adopts SNMP protocol to manage/monitor network devices and runs on the NMS server.
- Agent: Agent is an agent process in the managed devices, which is used to maintain the information data of the managed devices and respond to the request from the NMS, and report the management data to the NMS that sends the request.
- **Management object：** Management object refers to the managed object. Each device may contain multiple Management objects, which may be a piece of hardware in the device or a set of parameters configured on hardware or software.
- MIB: MIB is a database that identifies the variables maintained by the managed device. MIB defines a series of properties of the managed device in the database: object name, object state, object access rights and object data type.

As the network management center of the entire network, NMS manages the equipments. Each managed device includes Agent process, MIB and multiple managed objects that reside in the device. The NMS interacts with the Agent running on the managed device, and the Agent completes the instructions of the NMS through the operation of the MIB on the device end.

SNMPv1/SNMPv2c specifies 7 types of operations to complete information exchange between NMS and Agent. SNMPv1 version doesn’t support GetBulk and Inform operation.

Operation	Description
Get	The Get operation can extract one or more parameter values from the Agent.
GetNext	The GetNext operation extracts the next parameter value in lexicographical order from the Agent.
Set	The Set operation can set one or more parameter values of the Agent.
Response	The Response operation can back to one or more parameter values. This operation is issued by the Agent, which is the response operation of GetRequest, GetNextRequest, SetRequest and GetBulkRequest. After receiving the Get/Set instruction from NMS, the Agent completes the corresponding query/modification operation through MIB, and then uses Response operation to respond the information to NMS.
Trap	Trap information is the information sent by the Agent to NMS to inform the management process of the situation on the device end.
GetBulk	The GetBulk operation implements the NMS to query the information group of managed devices.
Inform	InformRequest is also a managed device that sends an active alert to the NMS. Different from Trap alarm, NMS needs to reply InformResponse for confirmation after the managed device sends Inform warning.

Function Description

On the page of "SNMP Configuration", user can conduct the following operations:

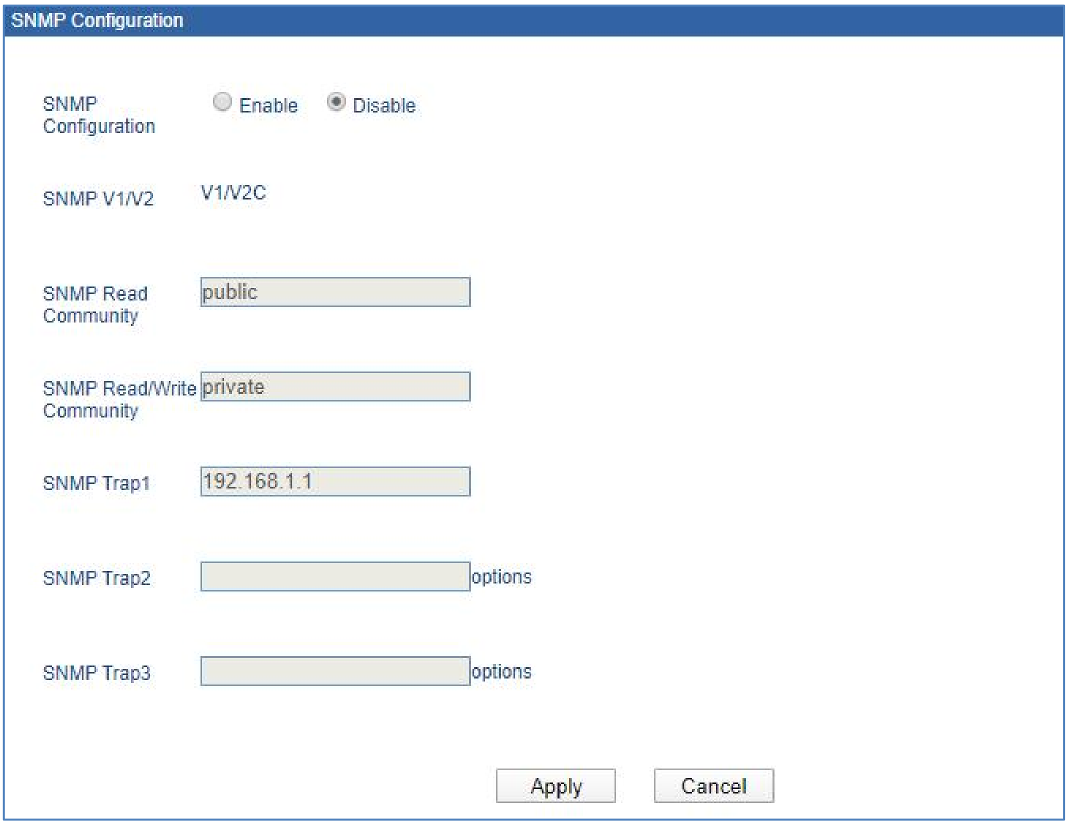
- Enable or disable SNMP configuration functions;
- Configure SNMP V1/V2 read-only community name;
- Configure SNMP V1/V2 read-only community name;
- Configure SNMP gateway.

Operation Path

Open in order: "Main Menu > Remote Monitoring > SNMP Configuration".

Interface Description

Interface screenshot of SNMP configuration:



Main elements configuration description of SNMP configuration interface:

Interface Element	Description
SNMP Configuration	SNMP configuration function, options as follows: • Enable; • Disable.
SNMP version	SNMP supports the following version: • SNMP V1: It adopts UDP protocol which can be used widely but will be insecure. • SNMP V2c: Semantics has been enhanced, and it supports TCP protocol.
SNMP Read community	Configure the read-only SNMP community name with the only operation permission of Get.
SNMP Read/Write Community	Configure the Read/Write SNMP community name with the operation permission of Get and Set.
SNMP Trap1	Configure Trap information destination IP address 1. Note: It will send out alarm during cold or warm start, port offline/online, power on/off.

SNMP Trap2	Configure Trap information destination IP address 2.
SNMP Trap3	Configure Trap information destination IP address 3.

Note

Please pay attention to the permission problem of read and write in the SNMP browser, user can check the permission of used "community name" if the permission of "write" is invalid.

Instance SNMP Configuration

For example: Enable SNMP configuration and configure the "Read-only community name" to "public", "Read-write community name" to "private", "SNMP Trap1" to "192.168.1.1".

Operation Steps

Step 1 Log into Web configuration interface.

Step 2 Select "Main Menu > Remote Monitoring > SNMP Configuration".

Step 3 On the displayed page of "SNMP Configuration":

1 Select "enable" on the column of "SNMP Configuration";

2 Select "Read-only community name" as "public";

3 Select "Read/Write community name" as "private";

4 Enter "SNMP Trap1" as "192.168.1.1".

Step 4 Click “Apply”.

Step 5 End.

10.2 Alarm Settings

Function Description

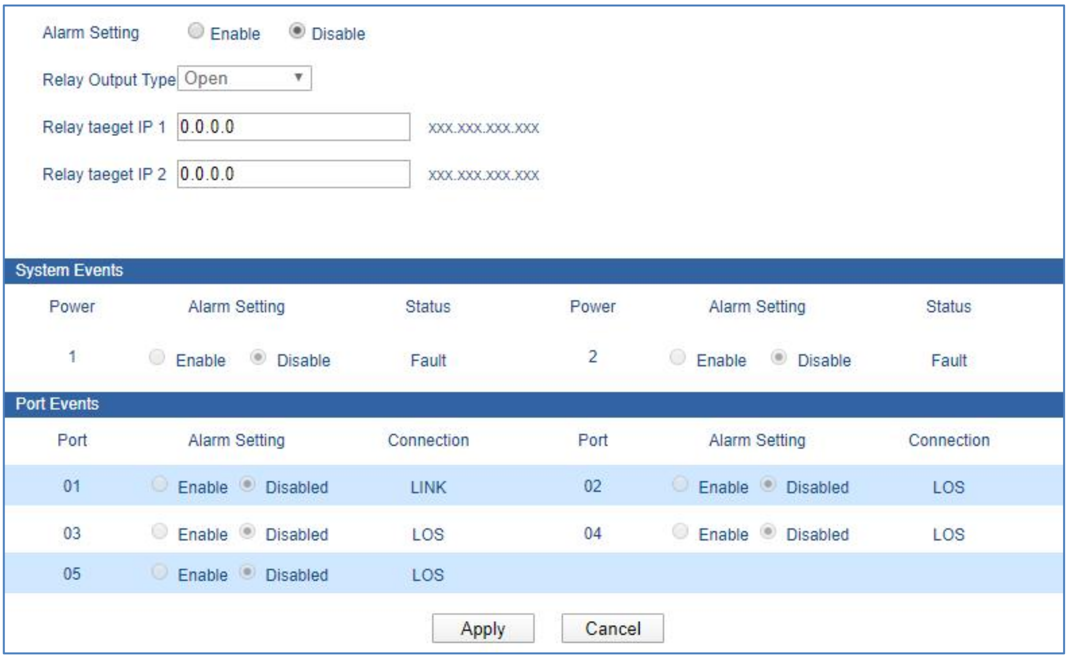
On the page of "Alarm Warning", user can configure power supply alarm and port alarm; when the equipment runs abnormally, it can promptly notify the administrator, and quickly repair the equipment to avoid excessive loss.

Operation Path

Open in order: "Main Menu > Remote Monitoring > Relay Warning".

Interface Description

Alarm warning interface as follows:



Main elements configuration description of alarm warning interface:

Interface Element	Description
Alarm Settings	Configure alarm settings. Options: • Enable; • Disable.
Relay Output Type	Click the drop-down list of "Relay Output Type", options as follows: • Normally open: when the relay is normal without alarm, it is in closed status; when alarm occurs, relay is in open status; • Normally closed: when the relay is normal without alarm, it is in open status; when alarm occurs, relay is in closed status.
Alarm target IP1	Alarm destination IP address 1. When an alarm occurs, the device sends alarm information to the destination host, which can be viewed by management software such as BlueEyes.
Alarm target IP2	Alarm destination IP address 2. When an alarm occurs, the

Interface Element	Description
	device sends alarm information to the destination host, which can be viewed by management software such as BlueEyes.
Power Supply Alarm Settings	**The power supply alarm setting bar**
Power	Display the power supply number of the device.
Alarm Settings	Configure the alarm functions of the power supply. Options: • Enable; • Disable. Note: • DC provides 2 power supplies (Single power without power supply alarm), when one power supply goes wrong, another power supply can supply electricity soon, dual power supply hot standby is supported. • After enabling power supply alarm, the device will output alarm signal to hint abnormal operation of power supply when power supply runs abnormally.
Power status	Display current state of power supply: • Fault; • Normal.
Port Alarm Settings	**Port events column**
Port number	Display the device port number.
Alarm Settings	Configure the port alarm function. Options: • Enable; • Disable. Note After enabling port alarm, when the port is in abnormal status, such as connection or disconnection, the device will output a signal to hint the abnormal operation of the device.
Connection status	Display port connection status of the device: • Not connected; • Connected.

Instance Alarm Settings

For example: Enable alarm configuration, and enable power supply alarm for power 1, port alarm for port 1.

Operation Steps

Step 1 Log into Web configuration interface.

Step 2 Click "Main Menu > Remote Monitoring > Relay Warning".

Step 3 On the displayed page of "Relay Warning":

1. Select "enable" on the column of "Alarm Setting";
2. Select "Relay Output Type" as "open".

Step 4 On the region of "System Events", select "Enable" the "Alarm Setting" of power 1.

Step 5 On the region of "Port Events", select "Enable" the "Alarm Setting" of power 1.

Step 6 Click “Apply”.

Step 7 End.

11 Port Statistics

11.1 Frame Statistics

Function Description

On the page of “Frame Statistics”, user can check frame statistics of sending/receiving data packets transmitted by the port within a period of time.

Operation Path

Open in order: “Main Menu > Port Statistics > Frame Statistics”.

Interface Description

Frames statistics interface as follows:

Rx Frame Statistics					
Item/ Port	Port 01	Port 02	Port 03	Port 04	Port 05
InGoodOctets	191321	0	0	0	0
InBadOctets	0	0	0	0	0
InUnicast	1759	0	0	0	0
InBroadCasts	24	0	0	0	0
InMulticasts	105	0	0	0	0
InPause	0	0	0	0	0
InUndersize	0	0	0	0	0
InFragments	0	0	0	0	0
InOversize	0	0	0	0	0
InJabber	0	0	0	0	0
IN RxErr	0	0	0	0	0
INFCSErr	0	0	0	0	0

Tx Frame Statistics					
Item/ Port	Port 01	Port 02	Port 03	Port 04	Port 05
OutOctets	1818829	0	0	0	0
OutUnicast	2695	0	0	0	0
OutBroadCasts	10	0	0	0	0
OutMulticasts	0	0	0	0	0
OutPause	0	0	0	0	0
Excessive	0	0	0	0	0
Collisions	0	0	0	0	0
Deferred	0	0	0	0	0
Single	0	0	0	0	0
Multiple	0	0	0	0	0
OutFCSErr	0	0	0	0	0
Late	0	0	0	0	0

Refresh Clear

Main elements configuration description of received frames statistics interface:

Interface Element	Description
InGoodOctets	Received valid data bytes (including FCS).
InbadOctets	Received invalid data bytes (including FCS).
InUnicasts	Number of valid unicast data frames.
InBroadcasts	Number of valid broadcast data frames.
InMulticasts	Number of valid multicast data frames. Note: Broadcast data frames are not included.
InPause	Valid flow control pause frames number.
InUndersize	Valid data frames number whose length is less than 64 bytes.
InFragments	Fragmented frames number. Note FCS verification is invalid when the data frame length is less than 64 bytes.
InOversize	Number of received valid oversize data frames. Note: Oversize frames refer to those data frames whose length is more than 1518 or 1522 bytes.
InJabber	Number of received invalid oversize data frames. Note: Oversize frames refer to those data frames whose length is more than 1518 or 1522 bytes.

Interface Element	Description
InFCSErr	Number (complete data) of error frames counted by FCS verification.

Main elements configuration description of transmitted frames statistics interface:

Interface Element	Description
OutOctets	Output bytes number. Note: This data packet includes FCS parity bit.
OutUnicasts	Number of output unicast data frames.
OutBroadcasts	Number of output multicast data frames.
OutMulticasts	Number of output multicast data frames.
OutPause	Number of output flow control pause frames.
Excessive	Number of output unsuccessful data frames. Note: Frames with over 16 times of half duplex flow control attempts are unsuccessful.
Collisions	Collision number during outputting.
Deferred	Number of frames with successfully delayed sending.
Single	Number of successfully output data frames after one time collision.
Multiple	Number of successfully output data frames after multiple times collision.
OutFCSErr	Number of output invalid FCS data frames.
Late	Number of output frames with the occurrence of collisions after 64 bytes.

12 Network Diagnosis

12.1 Port Mirroring

Mirroring refers to copying a message that passes through a specified port (source port or mirror port) to another specified port (destination port or acquisition port). In the process of network operation and maintenance, in order to facilitate business monitoring and fault location, the network administrator can analyze the message copied from the observation port through the network monitoring equipment and judge whether the business running in the network is normal or not.

Function Description

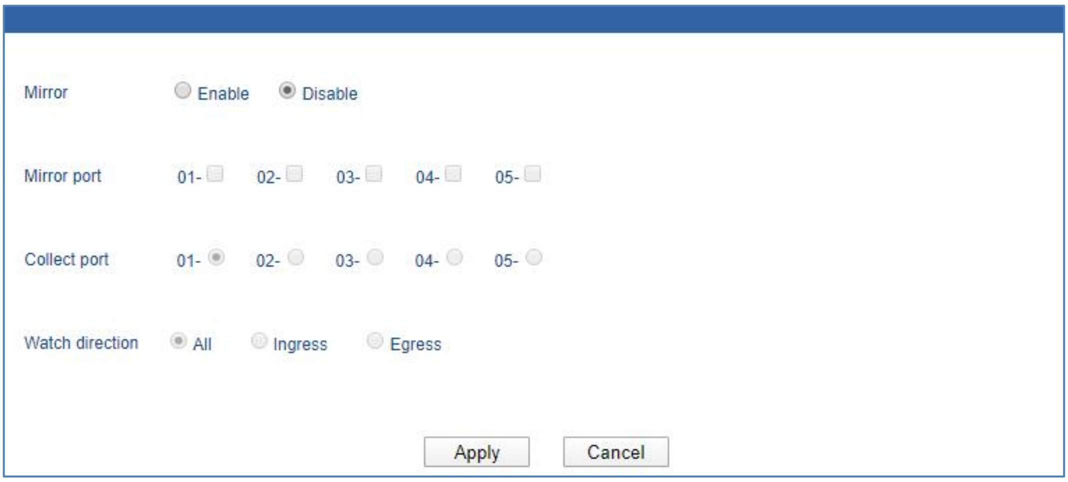
On the “Port Mirror” page, user can enable or configure the correspondence between ingress data mirror and egress data mirror.

Operation Path

Open in order: “Main Menu > Diagnosis > Mirror”.

Interface Description

Port mirror interface as follows:



The main element configuration description of port mirror interface:

Interface Element	Description
Port Mirroring	Setting port mirror function, options are: • Enable; • Disable.
Mirror port	Choose the ingress and egress data port that needs mirroring.
Collect port	Configure the collect ports with ingress/egress data mirroring.
Collect data	Backup data during mirroring, options are: • All; • Ingress; • Egress.

For instance: port mirror configuration

For example: use port 4 to collect ingress data and egress data of port 1, port 2 and port 3.

Operation Steps

Step 1 Log into Web configuration interface.

Step 2 Choose “Main Menu > Diagnosis > Mirror”.

Step 3 On the “Mirror” page, choose “enable” in the “mirror”.

Step 4 In the option of “mirror port”, choose port “1”, “2” and “3”.

Step 5 In the option of “collect port”, choose port “4”.

Step 6 In the option of “watch direction”, choose “all”.

Step 7 Click “Apply”.

Step 8 End.

13 System Management

13.1 Log Information

Function Description

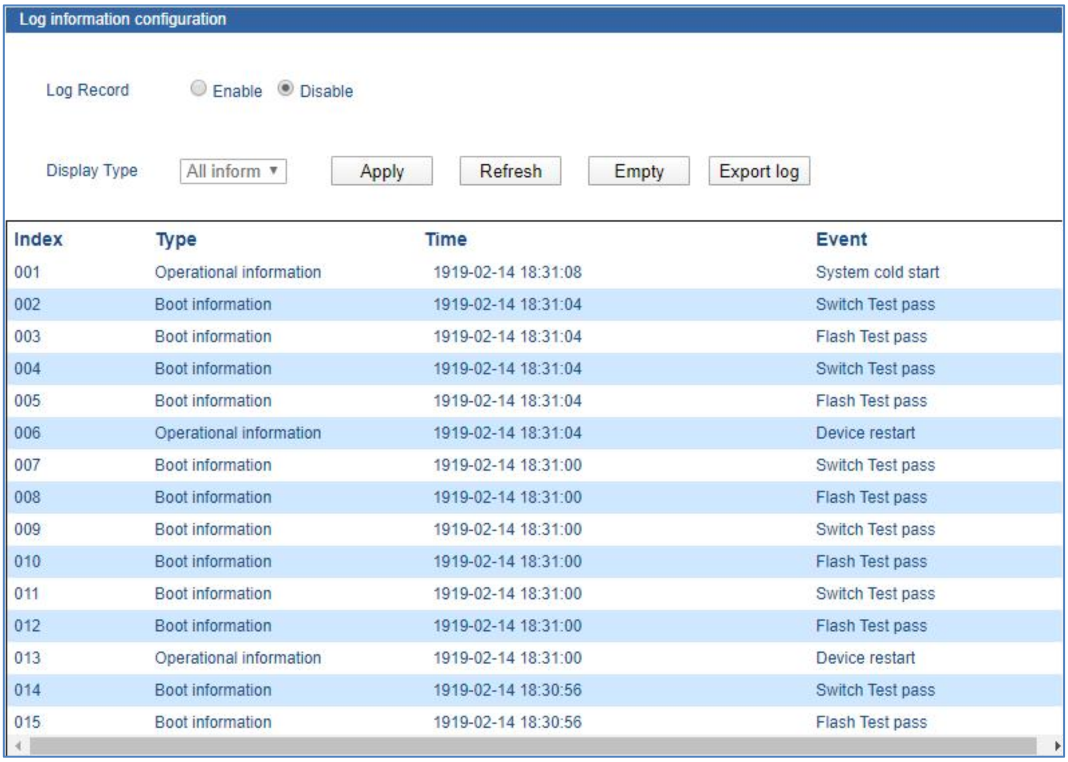
On the page of “Log information”, user can enable “log record” to check the status information of the device.

Operation Path

Open in order: “Main Menu > Basic Settings > Log information”.

Interface Description

Log information interface as follows:



Index	Type	Time	Event
001	Operational information	1919-02-14 18:31:08	System cold start
002	Boot information	1919-02-14 18:31:04	Switch Test pass
003	Boot information	1919-02-14 18:31:04	Flash Test pass
004	Boot information	1919-02-14 18:31:04	Switch Test pass
005	Boot information	1919-02-14 18:31:04	Flash Test pass
006	Operational information	1919-02-14 18:31:04	Device restart
007	Boot information	1919-02-14 18:31:00	Switch Test pass
008	Boot information	1919-02-14 18:31:00	Flash Test pass
009	Boot information	1919-02-14 18:31:00	Switch Test pass
010	Boot information	1919-02-14 18:31:00	Flash Test pass
011	Boot information	1919-02-14 18:31:00	Switch Test pass
012	Boot information	1919-02-14 18:31:00	Flash Test pass
013	Operational information	1919-02-14 18:31:00	Device restart
014	Boot information	1919-02-14 18:30:56	Switch Test pass
015	Boot information	1919-02-14 18:30:56	Flash Test pass

Main elements configuration description of log information interface:

Interface Element	Description
Log record	Enable or disable log record.
Display Type	Click the drop-down list of “Display Type”, user can check the information of device booting, connection and operation. ● Full detail; ● Boot information; ● Operation information; ● Connection information;
Export log	Click the “Export Log” button to export the current log information "syslog_txt.cfg".

13.2 Time Configuration

Function Description

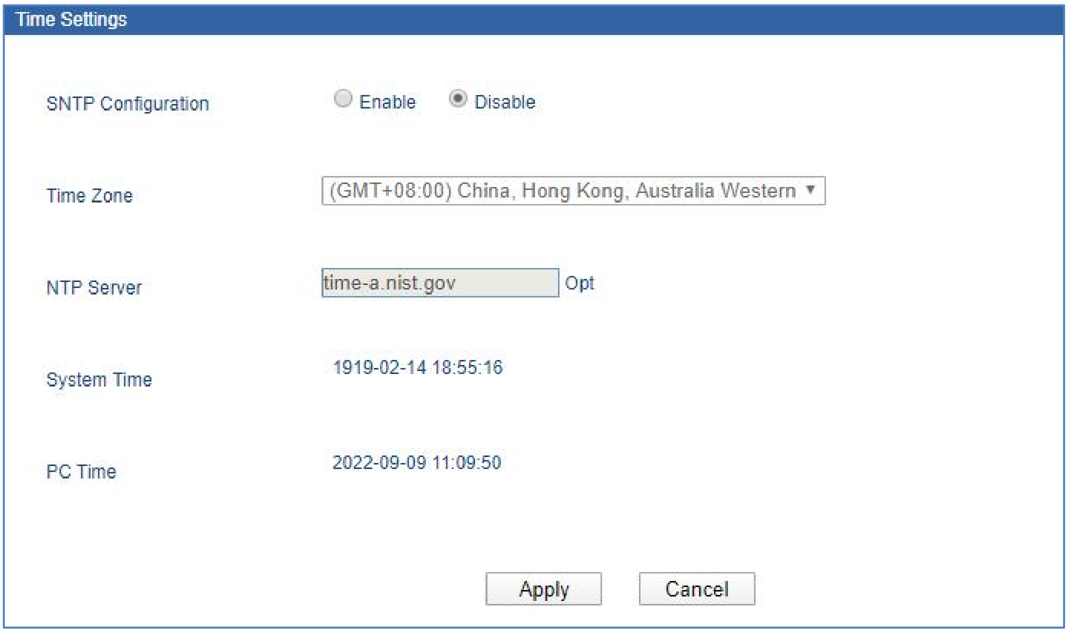
On the page of “Time Configuration”, user can check current PC time or system operation time, and select relative time zone.

Operation Path

Open in order: “Main Menu > Basic Settings > SNTP”.

Interface Description

Time settings interface as follows:



Main elements configuration description of time settings interface:

Interface Element	Description
SNTP Configuration	Enable or disable time configuration.
Time Zone	Selection of standard time zone for countries in the world.
NTP Server	Host name or IP address that provides NTP timing and time service for user.
System Time	The device time can be manually or automatically updated using NTP.
PC Time	PC time of the guest, the time display isn’t relative to the switch.

Notes

1. NTP server can be empty, the device adopts self-contained server updating and must ensure the correct configuration of DNS and gateway;
2. NTP server can’t be empty, it must be valid host name or legal IP address;
3. Only the “administrator” has the privilege to manually configure the device time.

13.3 Device Management

IP Address

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

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

Notes

- Category A, B, C address are unicast address; category D address is multicast address; category E address is reserved address for the future special purpose. Now, most of the using IP addresses belong to category A, B, C address.
- IP address adopts dotted decimal notation recording mode. Each IP address is expressed as four decimal integers separated by radix point, each integer is corresponding to a byte, such as 10.110.50.101.

Subnet Mask

A mask is a 32-bit number that corresponds to an IP address, some of which is 1 and some of which is 0. These 1 and 0 can be any combination in principle, but generally when designing masks, set the first consecutive digits to 1. A mask divides an IP address into two parts: the subnet address and the host address. The portion of the IP address that corresponds to the 1 bit in the mask is the subnet address, and the rest is the host address. The corresponding mask of Class A address is 255.0.0.0; The corresponding mask of Class B address is 255.255.0.0; The corresponding mask of Class C address is 255.255.255.0.

Gateway

The gateway address is often referred to as the default gateway. The Default gateway, or Default Route, is the Route selected by the router when no other Route exists for the destination address in the IP packet. All packets whose destination is not in the router's routing table will use the default route.

DNS Server

DNS, the full Name is the Domain Name Server, is used to resolve the Domain Name that easy for us to remember to the IP address that the Internet can recognize. If the device needs to access a host name, this server will be used to resolve it into an IP address.

Function Description

On the page of "Device Management", user can:

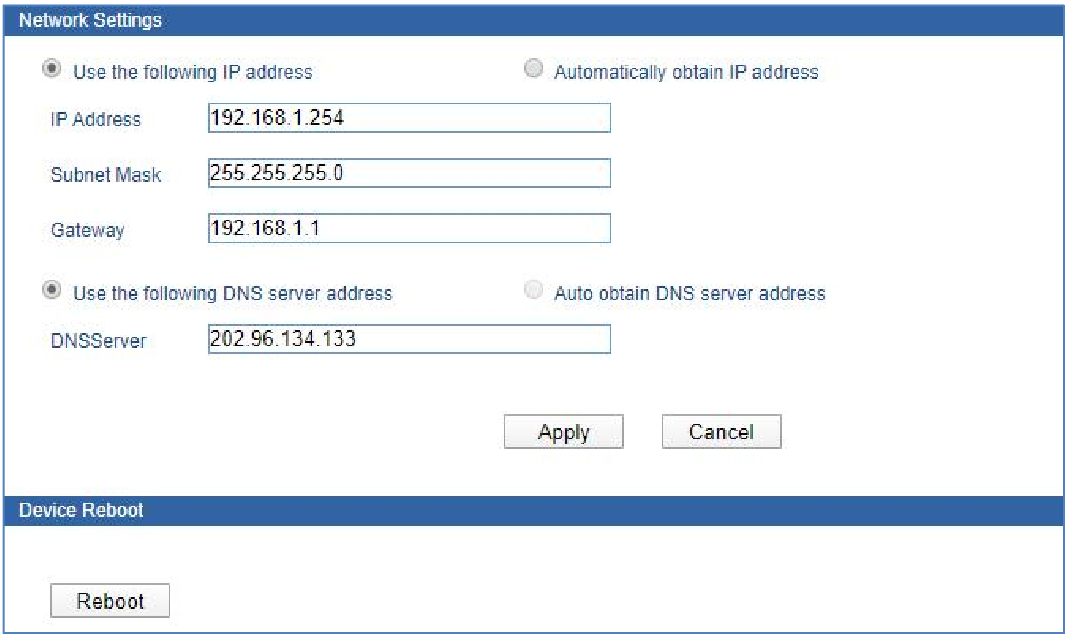
- Configure default IP address of the device;
- Configure netmask;
- Configure gateway address;
- Configure DNS server;
- Reboot the device.

Operation Path

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

Interface Description

The Device management interface is as follows:



Main elements configuration description of device address interface:

Interface Element	Description
Device Address	**Configuration column of the device address**
Use the following IP address	It represents that manually enabling configured IP address, netmask and gateway address.
Automatically obtain IP address	It represents that enabling the system automatical acquisition of the IP address of the device.
IP Address	Configure IP address of the device. Note Default configured IP address is 192.168.1.254.
Subnet Mask	Configure subnet mask of the device. Note Default configured subnet mask is 255.255.255.0.
Gateway	Configure gateway address of the device. Note Default configured gateway address is 192.168.1.1.
Use the following DNS server address	Configure the acquisition form of DNS server address as manual configuration. Note Default configured DNS server address is 202.96.134.133.
Automatically obtain DNS server address	Configure the acquisition form of DNS server address as automatic acquisition. Note: When IP address is manual configuration, this option becomes gray and is not optional.
DNS server	Configure DNS server address.

Interface Element	Description
Apply	Save the device address information. Note: Some devices may automatically reboot after configuration, and the configuration will take effect after rebooting.
Cancel	Cancel the modification of device address information.
Reboot the device	**Configuration column of device reboot**
Reboot	Reboot the device

For Example: Manual Configuration

For example: Configure the device address information, IP address is 192.168.5.88, gateway address is 192.168.5.1.

Operation Steps

Step 1 Log into Web configuration interface.

Step 2 Select “Main Menu > Basic Settings > Network & Reboot”.

Step 3 On the “Network Settings” region of displayed page of “Device Management”, select “Use the following IP address”.

1. Enter “192.168.5.88” in the textbox of “IP Address”.
2. Enter “192.168.5.1” in the textbox of “Gateway”.

Step 4 Click “Apply”, system will automatically save the configuration.

Step 5 End.

For Example: Automatic Acquisition of IP

For example: configure the device IP address as automatic acquisition.

Operation Steps

Step 1 Log into Web configuration interface.

Step 2 Select “Main Menu > Basic Settings > Network & Reboot”.

Step 3 On the “Network Settings” region of displayed page of “Device Management”, select “Automatically obtain IP address”.

Step 4 Click “Apply”, system will automatically save the configuration.

Step 5 End.

13.4 System Information

Function Description

On the page of “System Identification”, user can configure the following options:

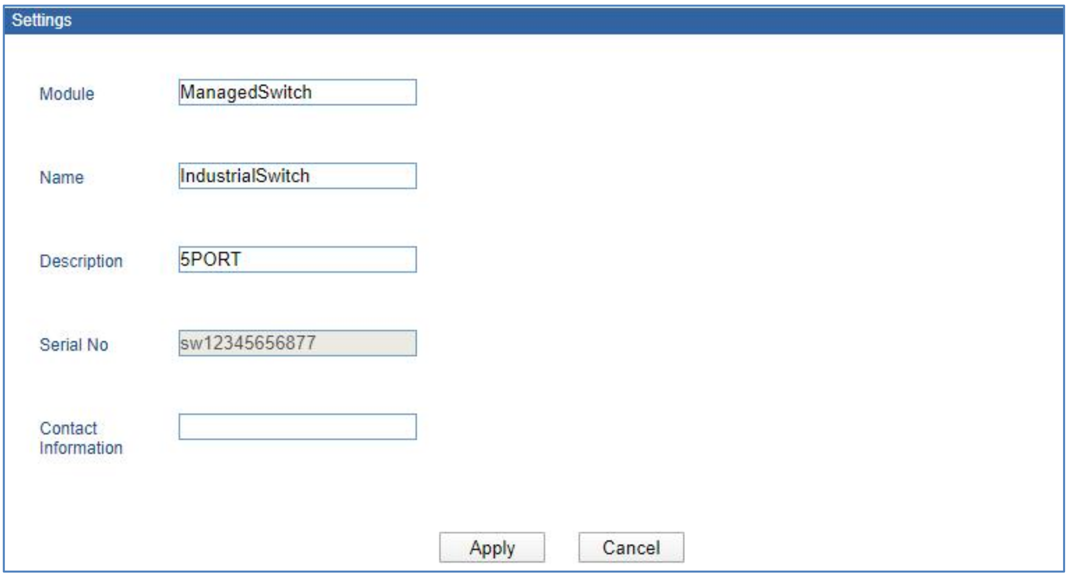
- Device model;
- Device name;
- Device description;
- Contact information.

Operation Path

Open in order: “Main Menu > Basic Settings > System Identification”.

Interface Description

System information interface as follows:



The main element configuration description of system information interface:

Interface Element	Description
Module	Configure the device model.
Name	Configure the device name to identify each device in the network.
Description	Configure the summary description of the device.

Serial No.	Configure the device number.
Contact information	Configure the contact Information of the maintenance personnel of the device. Note: ● Support the entering of Chinese characters, English letters, number, characters like "-", "_", "@", ",", "."; ● The entering of blank space is not supported.

For Example: Device Information Configuration

For example: Configure the device according to following information:

- "Module" is "ManagedSwitch1";
- "Name" is "IndustrialSwitch";
- "Description" is "8ports".

Operation Steps

Step 1 Log into Web configuration interface.

Step 2 Select "Main Menu > Basic Settings > System Identification".

Step 3 On the "Settings" region of displayed page of "System Identification":

1 Enter "Module" as "ManagedSwitch1";

2 Enter "Name" as "IndustrialSwitch";

3 Enter "Description" as "8ports".

Step 4 Click "Apply" to save the configuration.

Step 5 End.

13.5 File Management

Function Description

On the page of "File Management", user can conduct following operations:

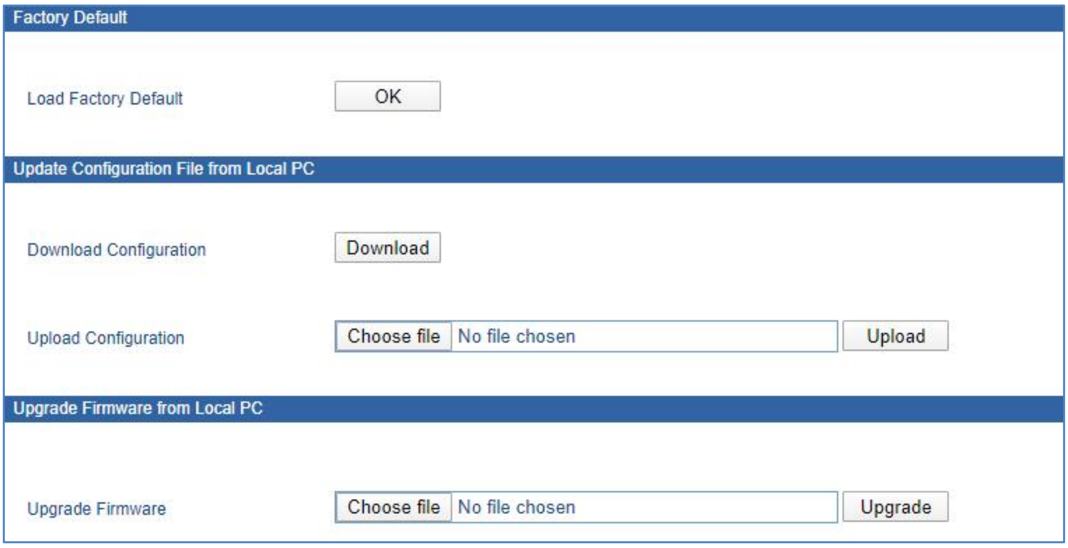
- Restore factory defaults;
- Upload and download configuration files;
- System upgrading.

Operation Path

Open in order: "Main Menu > System Manage > System File".

Interface Description

File management interface as follows:



Main element configuration instructions in System File interface.

Interface Element	Description
Factory Default	**Configuration column of restore factory defaults**
Load Factory Default	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".
Update Configuration File from Local PC	**Configuration column of configuration files**
Download Configuration	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	Configure the switch via uploading configuration files information.
Upgrade Firmware from Local PC	**Configuration column of system upgrade**
Upgrade Firmware	Upgrade operating system of the switch.

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.

Example: Download Configuration Files

For example: Download configuration files.

Operation Steps

Step 1 Log into Web configuration interface.

Step 2 Select "Main Menu > System Management > File Management".

Step 3 On the region of "Configuration File" of displayed page of "File Management", click "Download".

Step 4 Select save path on the pop-up dialog box of "Save as".

Step 5 Click "Apply".

Step 6 End.

Example: Upload Configuration

For example: Upload configuration files to the switch for updating the switch configuration.

Operation Steps

Notes

Please prepare the configuration files and then conduct uploading operation.

Step 1 Log into Web configuration interface.

Step 2 Select "Main Menu > System Management > File Management".

Step 3 On the region of "Configuration File" of displayed page of "File Management", click "Browse" after the label of "Upload Configuration".

Step 4 Select prepared cfg configuration files on the pop-up "select files to load".

Step 5 Click "Open".

Step 6 Click "Upload".

Step 7 Alarm information is displayed in the pop-up dialog box of "messages from the webpage", click "OK".

Step 8 The device is rebooted automatically and its configuration is updated.

Step 9 End.

13.6 System Logout

Function Description

On the page of “System log off”, user can log off the login information of current user.

Operation Path

Open in order: “Main Menu > Basic Settings > System log off”.

Interface Description

System logout interface as follows:

Main elements configuration description of system logout interface:

Interface Element	Description
System Log Off	Log off the login information of current user.

For example: Log off and change administrator to login

For example: Log off current user, and then login again via entering “admin8” in the column of administrator and “admin8” in the column of password.

Operation Steps

Step 1 Log into Web configuration interface.

Step 2 Select “Main Menu > Basic Settings > System log off”.

Step 3 Click “OK” on the displayed page of “System log off”.

1 Conduct following operations on the pop-up login dialog box:
2 Enter “admin8” on the option box of “User name”.
3 Enter “admin8” on the option box of “Password”.

Step 4 Click “OK”

Step 5 Alarm information is displayed in the pop-up dialog box of "messages from the webpage", click "OK".

Step 6 Login successfully to the WEB interface.

Step 7 End.