3onedata

IES6210 Series

Managed Industrial Ethernet Switch

User Manual

Document Version: 04

Issue Date: 18/07/2023

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

Trademark statement

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

Note

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

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

Preface

This Switch User Manual has introduced:

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

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Hardware engineers

Port Convention

The port number in this manual is only an example, and does not represent the actual port with this number on the device. In actual use, the port number existing on the device shall prevail.

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’.
About this chapter	The section ‘about this chapter’ provide links to various sections of this chapter, as well as links to the Principles

Format	Description
	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.
💡 Tip	Pay attention to the operation or information to ensure success device configuration or normal working.

Revision Record

Version No.	Date	Revision note
01	2019-01-22	Product release
02	2019-02-20	Add Modbus TCP function
03	2022-03-15	Software update
04	2023-07-18	Document maintenance

Contents

1 Login the WEB Interface

1.1 System Requirements for WEB Browsing

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

Hardware and software	System requirements
CPU	Above Pentium 586
Memory	128MB or more
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 default management of the industrial Ethernet switch is as follows:

IP Settings	Default Values
IP address	192.168.1.254
Subnet mask	255.255.255.0

When configuring a switch through the Web:

- Before making remote configuration, make sure that the route between the computer and the switch is reachable.
- Before making a local configuration, make sure that the IP address of the computer and the switch are on the same subnet.

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

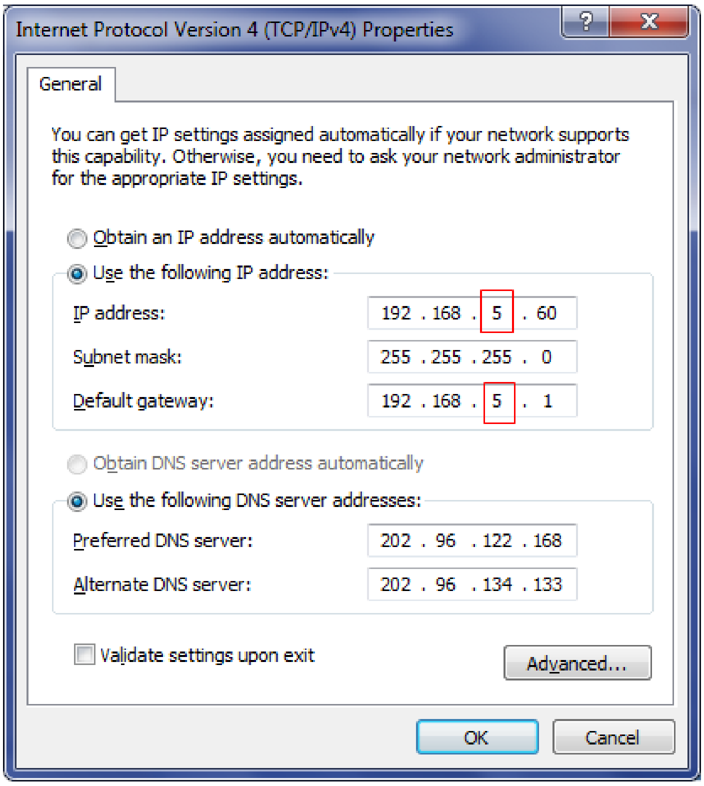
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation steps

Amendment steps as follow:

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

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



Internet Protocol Version 4 (TCP/IPv4) Properties

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

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 5 . 60
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 5 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 202 . 96 . 122 . 168
Alternate DNS server: 202 . 96 . 134 . 133

□ Validate settings upon exit

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

Step 4 End.

1.3 Log in the Web Configuration Interface

Operation steps

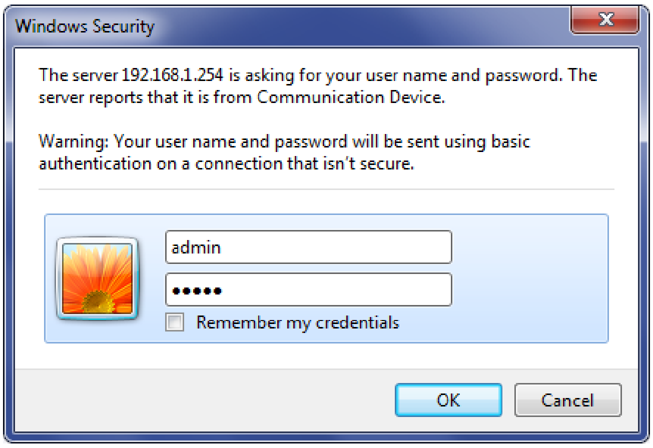
Login in the web configuration interface as follow:

Step 1 Run the computer browser.

Step 2 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.



The server 192.168.1.254 is asking for your user name and password. The server reports that it is from Communication Device.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

admin

•••••

□ Remember my credentials

Note:

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

Step 5 Click “OK”.

Step 6 End.

After successful login, you can configure the relevant parameters and information of the WEB interface as needed.

Note:

After login in the device, modify the switch IP address for usage convenience.

2 System Status

Function Description

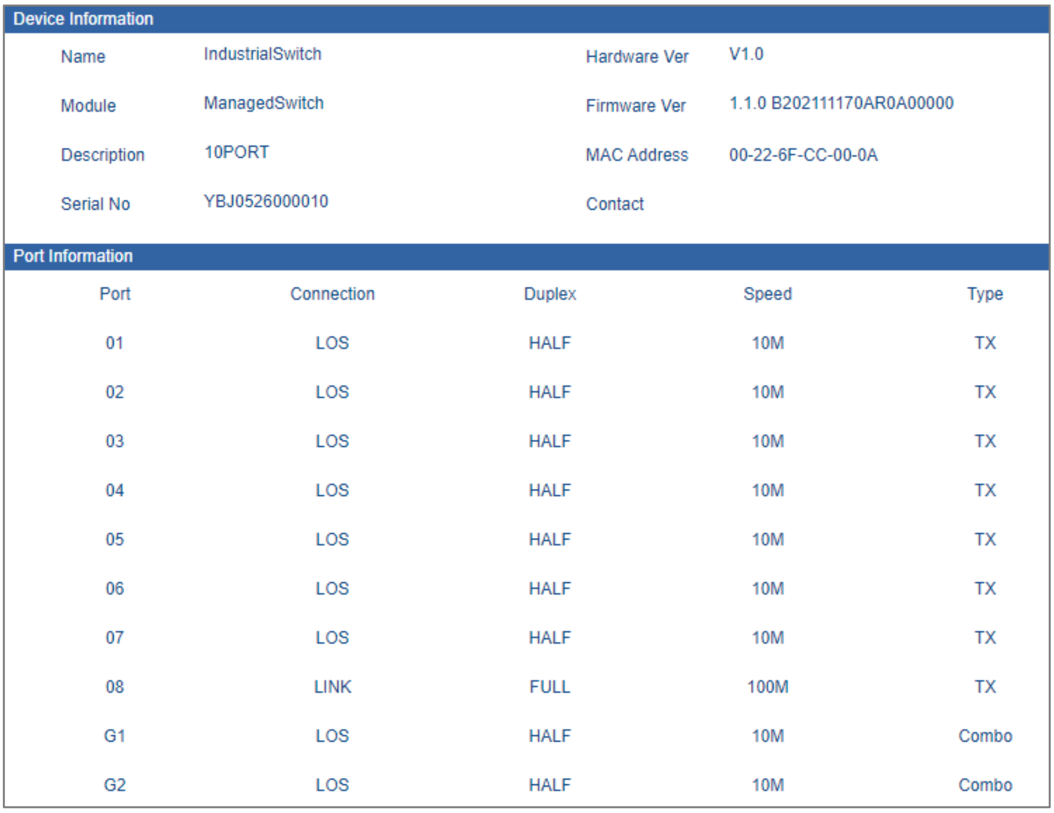
On the page of "System Information", user can check "Device Information" and "Port Information".

Operation Path

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

Interface Description

Device information interface as follows:



Device Information

Name	IndustrialSwitch	Hardware Ver	V1.0
Module	ManagedSwitch	Firmware Ver	1.1.0 B202111170AR0A00000
Description	10PORT	MAC Address	00-22-6F-CC-00-0A
Serial No	YBJ0526000010	Contact	

Port Information

Port	Connection	Duplex	Speed	Type
01	LOS	HALF	10M	TX
02	LOS	HALF	10M	TX
03	LOS	HALF	10M	TX
04	LOS	HALF	10M	TX
05	LOS	HALF	10M	TX
06	LOS	HALF	10M	TX
07	LOS	HALF	10M	TX
08	LINK	FULL	100M	TX
G1	LOS	HALF	10M	Combo
G2	LOS	HALF	10M	Combo

Main elements configuration description of state information interface:

Interface Element	Note
Device information	**Device information status bar.**
Name	Display the device name.
Module	Display the device model.
Description	Display characters description of the device.
Serial 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;

Interface Element	Note
	- "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. - Combo: Combo port.

Note

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

3 Port Configuration

3.1 Port Settings

Function Description

The "Port Config" page mainly includes:

- Check port type;
- Set speed mode and duplex mode;
- Port enable;
- Flow control;

  Network congestion is easy to cause packet loss. Flow control is a technology to prevent packet loss. 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

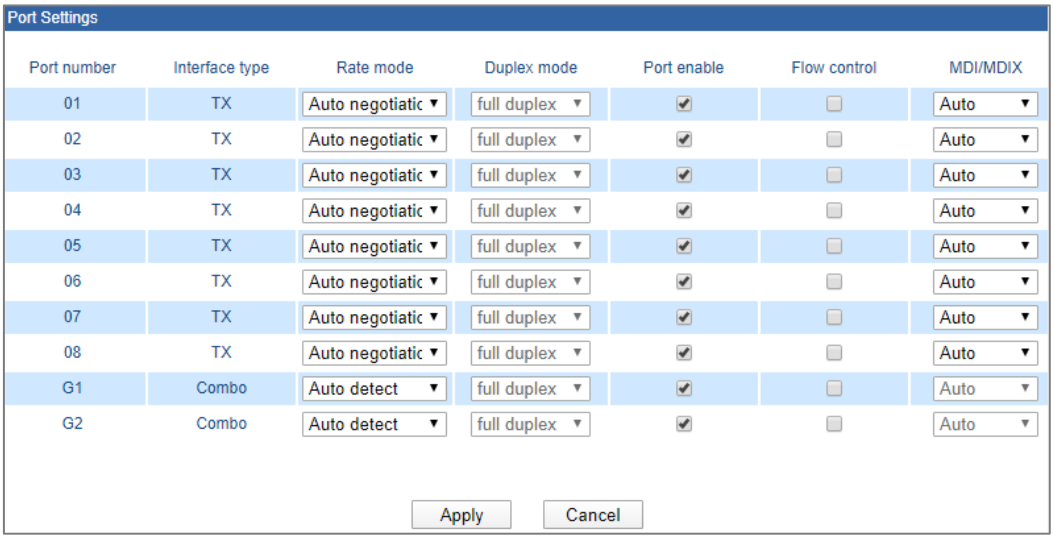
- The speed, duplex, and flow control for a port will only work when the port is enabled.
- After selecting automatic negotiation, speed and duplex will be gained via automatic negotiation.

Operation Path

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

Interface Description

Port settings interface as follows:



Port Settings

Port number	Interface type	Rate mode	Duplex mode	Port enable	Flow control	MDI/MDIX
01	TX	Auto negotiatic	full duplex	☑	☐	Auto
02	TX	Auto negotiatic	full duplex	☑	☐	Auto
03	TX	Auto negotiatic	full duplex	☑	☐	Auto
04	TX	Auto negotiatic	full duplex	☑	☐	Auto
05	TX	Auto negotiatic	full duplex	☑	☐	Auto
06	TX	Auto negotiatic	full duplex	☑	☐	Auto
07	TX	Auto negotiatic	full duplex	☑	☐	Auto
08	TX	Auto negotiatic	full duplex	☑	☐	Auto
G1	Combo	Auto detect	full duplex	☑	☐	Auto
G2	Combo	Auto detect	full duplex	☑	☐	Auto

The main element configuration description of port setting interface:

Interface Element	Note
Port number	Port number of the device.
Interface type	According to the electrical properties of the interface, the Ethernet interface of the switch can be divided into: • Copper port: transmission of electrical signals through twisted pair; • Fiber port: transmission of optical signals through optical fiber; • Combo: fiber and copper multiplexing port. When the physical port is connected, the fiber port or copper port will be shown according to the port connection

Interface Element	Note
	property.
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 supported speed is 10Mbit/s; ● 100M speed: the supported speed is 100Mbit/s; ● 1000M speed: the supported speed is 1000Mbit/s; ● Auto-Detect: when the interface type is Combo/Fiber port, it can automatically detect the connected interface type. ● 1000Base-X: when the interface type is Combo/Fiber port, it can be forced to Gigabit fiber port. ● 100Base-X: when the interface type is Combo/Fiber port, it can be forced to 100M fiber port. Note: ● The copper ports of the switch are all MDI/MDIX self-adaptive ports, which support auto-negotiation; ● 1000M speed applies only to the Gigabit ports of the switch.
Duplex Mode	After the specific rate is specified for the copper port, 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: the interface can receive and send data simultaneously. Note: When the speed mode is “Auto negotiation”, the port automatically matches the opposite port duplex mode.
Port Enable	Check the checkbox 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;

Interface Element	Note
	● 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.

3.2 SFP DDM

Function Description

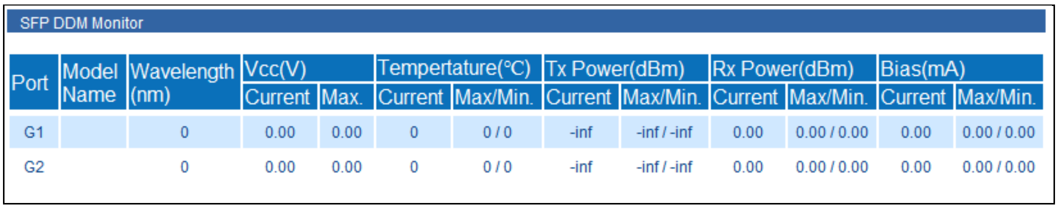
On the “SFP DDM” page, DDM (Digital Diagnostic Monitor) function is supported. User can monitor SFP parameter in real time. This function has greatly facilitated the troubleshooting process of optical fiber link and the cost of on-site debugging.

Operation Path

Open in order: " Main Menu > Port Configuration > DDM".

Interface Description

DDM interface as follows:



SFP DDM Monitor

Port	Model Name	Wavelength (nm)	Vcc(V)		Tempertature(℃)		Tx Power(dBm)		Rx Power(dBm)		Bias(mA)	
			Current	Max.	Current	Max/Min.	Current	Max/Min.	Current	Max/Min.	Current	Max/Min.
G1		0	0.00	0.00	0	0 / 0	-inf	-inf / -inf	0.00	0.00 / 0.00	0.00	0.00 / 0.00
G2		0	0.00	0.00	0	0 / 0	-inf	-inf / -inf	0.00	0.00 / 0.00	0.00	0.00 / 0.00

The main element configuration description of DDM interface:

Interface Element	Note
Port	The corresponding name of this device’s Ethernet port
Model Name	This device’s SFP type
Wavelength	Transmission wavelength of SFP module of the device port, unit is: nm.
Vcc (V)	The voltage that this device offers SFP. Its unit is V. Overvoltage could lead to the breakdown of CMOS device; under voltage would disable the normal operation of lasers.
Temperature (℃)	This device’s SFP temperature. Its unit is ℃. The operating temperature of this SFP module should be within the temperature range of normal operation.
Tx Power (dBm)	Optical output power, referring to the output power of optical source in the sending end of optical module. The unit is dBm

Interface Element	Note
RX Power (dBm)	Optical input power, referring to the lowest optical power of receiving in certain rate and bit error rate. The unit is dBm
Bias (mA)	The bias current of laser. Its unit is mA.

3.3 PoE Configuration

PoE (Power over Ethernet) means supplying power through Ethernet. It’s a wired Ethernet power supply technology that enables electric power to transmit to terminal device through data line or free line.

PoE power supply system includes:

- PSE (Power-sourcing Equipment): PoE device that supplies powered device with power through Ethernet.
- PD (Powered Device): powered device like wireless AP (Access Point), POS machine, camera and so on.
- PoE power supply: PoE power supply powers the whole PoE system. The quantity of PD that connects to PSE is limited by the power of PoE power supply.

Function Description

The "PoE Config" page mainly includes:

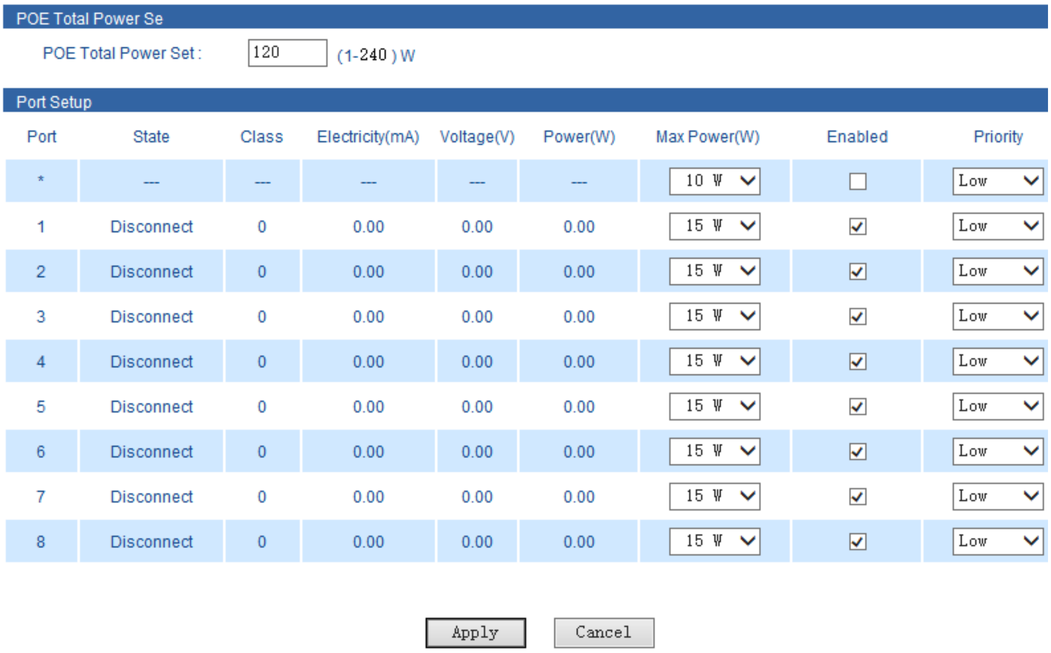
- PoE total power settings;
- PoE port power settings;
- Priority settings;
- PoE port enablement.

Operation Path

Open in order: "Main Menu > Port Config > PoE Config”.

Interface Description

PoE configuration interface as follows:



POE Total Power Se

POE Total Power Set : 120 (1-240) W

Port Setup

Port	State	Class	Electricity(mA)	Voltage(V)	Power(W)	Max Power(W)	Enabled	Priority
*	---	---	---	---	---	10 W	□	Low
1	Disconnect	0	0.00	0.00	0.00	15 W	☑	Low
2	Disconnect	0	0.00	0.00	0.00	15 W	☑	Low
3	Disconnect	0	0.00	0.00	0.00	15 W	☑	Low
4	Disconnect	0	0.00	0.00	0.00	15 W	☑	Low
5	Disconnect	0	0.00	0.00	0.00	15 W	☑	Low
6	Disconnect	0	0.00	0.00	0.00	15 W	☑	Low
7	Disconnect	0	0.00	0.00	0.00	15 W	☑	Low
8	Disconnect	0	0.00	0.00	0.00	15 W	☑	Low

The main element configuration description of PoE configuration interface:

Interface Element	Description
POE total power	The total power of all PoE ports that supply power.
Port	The PoE port number of the device.
State	The power state of PoE port.
Class	The PoE power class.
Electricity (mA)	The current size of PoE port power.
Voltage (V)	The voltage size of PoE port power.
Power (W)	The power size of PoE port power.
Max power (W)	The maximum output power limitation of configuring PoE port.
Enabled	Check the box to enable port PoE power function.
Priority	The priority configuration of PoE port power supply. Port power distribution priority with the constraint of gross power. ● High: high priority; ● Medium: medium priority; ● Low: low priority. Note: When the switch supplies power at nearly full capacity, it would first supply power to the PD device that connects to the port with High priority; then the PD device that connects to port with Medium priority.

3.4 Bandwidth Management

Function Description

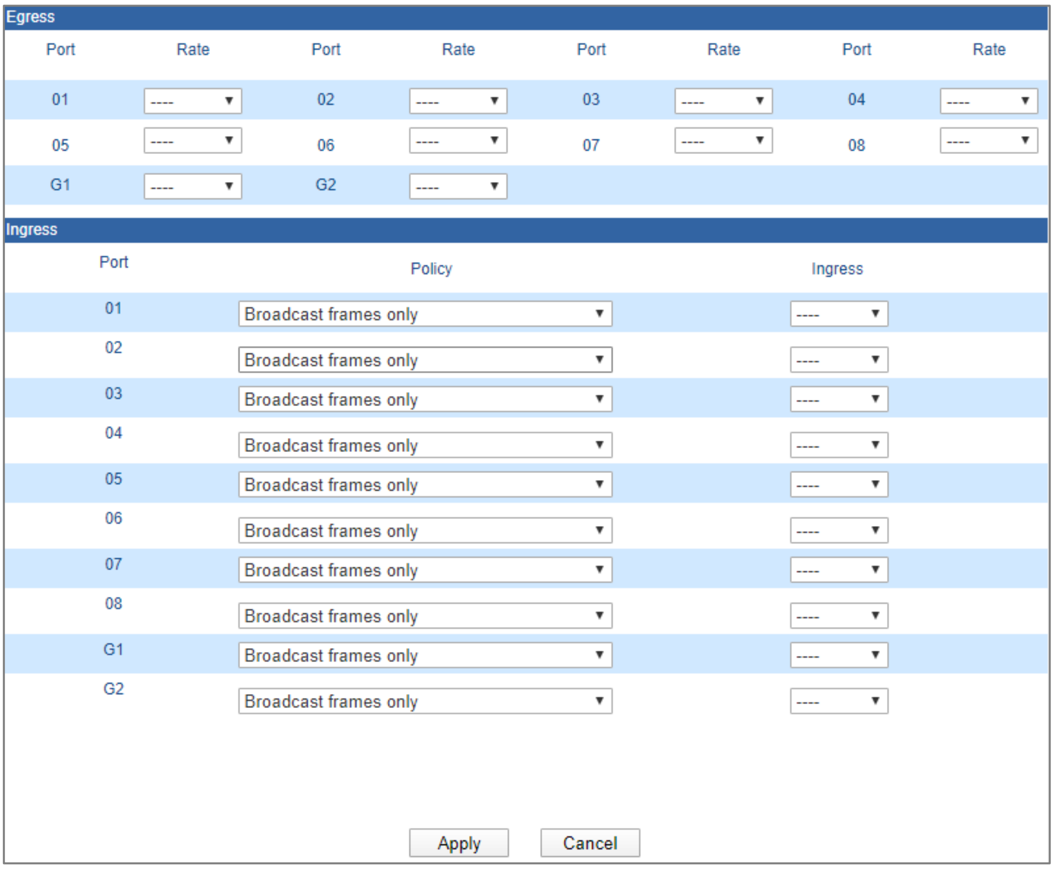
On the page of “Bandwidth Management”, the device can realize the port’s egress bandwidth settings and priority scheduling of ingress data packet.

Operation Path

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

Interface Description

Bandwidth management interface as below:



Egress

Port	Rate	Port	Rate	Port	Rate	Port	Rate
01	----	02	----	03	----	04	----
05	----	06	----	07	----	08	----
G1	----	G2	----				

Ingress

Port	Policy	Ingress
01	Broadcast frames only	----
02	Broadcast frames only	----
03	Broadcast frames only	----
04	Broadcast frames only	----
05	Broadcast frames only	----
06	Broadcast frames only	----
07	Broadcast frames only	----
08	Broadcast frames only	----
G1	Broadcast frames only	----
G2	Broadcast frames only	----

The main element configuration description of bandwidth management interface:

Interface Element	Note
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.

4 Layer 2 Features

4.1 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.

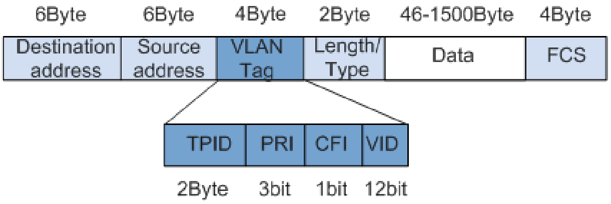
- Limit the broadcast domain;
- Increase the security of LAN;
- Improve the network stability;
- Flexibly construct virtual working team.

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:

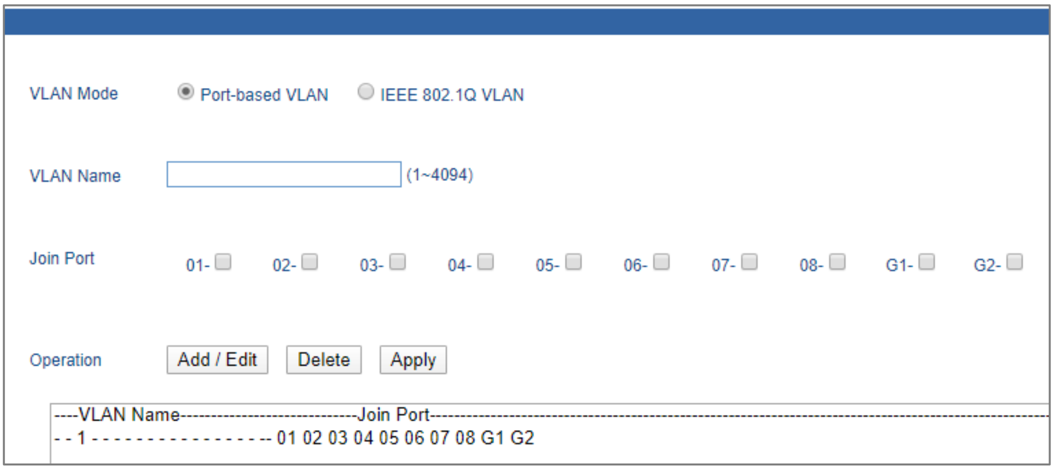
- Configure port type:
- Configure the port PVID;
- Create VLAN entry;
- Configure the port member type.

Operation Path

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

Interface Description 1: Port-based VLAN

Port-based VLAN interface as follows:



VLAN Mode ● Port-based VLAN ○ IEEE 802.1Q VLAN

VLAN Name (1~4094)

Join Port 01- □ 02- □ 03- □ 04- □ 05- □ 06- □ 07- □ 08- □ G1- □ G2- □

```
----VLAN Name--------------------------Join Port----------------------------
- - 1 - - - - - - - - - - - - - - - - -- 01 02 03 04 05 06 07 08 G1 G2
```

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

Interface Element	Note
VLAN Mode	Choose VLAN type, options are: • Port-based VLAN • IEEE 802.1Q VLAN.

Interface Element	Note
VLAN Name	Enter VLAN number in digital form. Note: Input range is 1~4094.
Join Port	Choose VLAN member.
Operation	Add/edit, delete or save VLAN configuration information.

Instance: create port-based VLAN.

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.

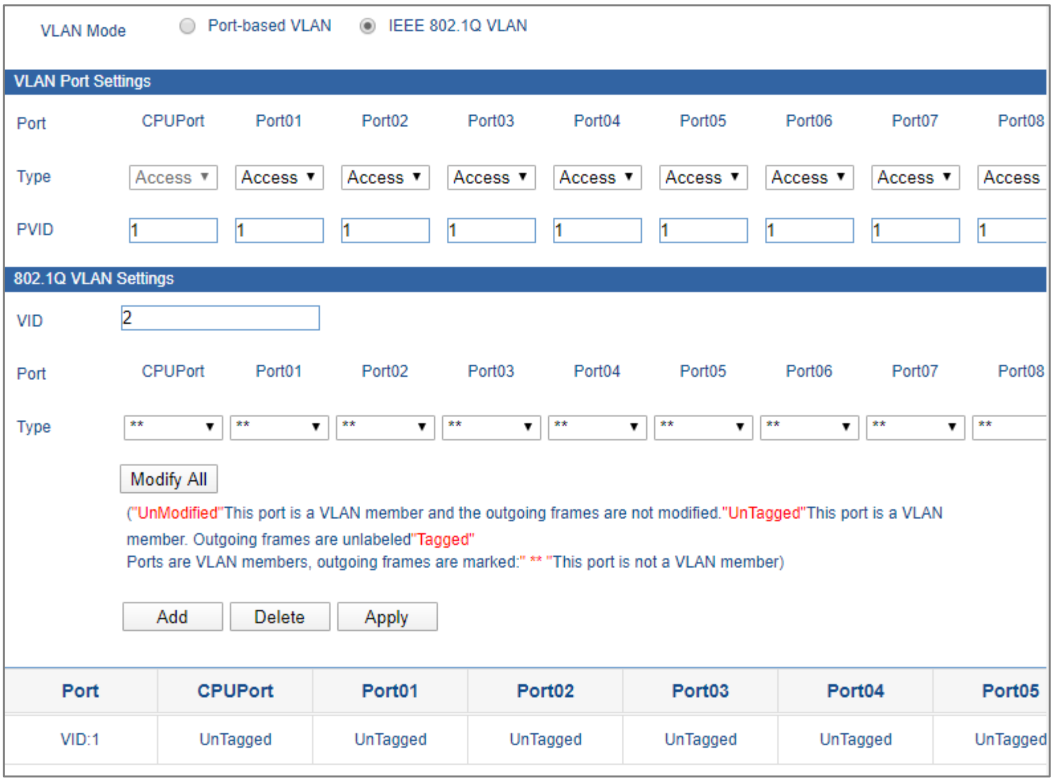
Step 4 Select VLAN member on the check box of “Join Port”, such as select port 2 and port 3.

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:



VLAN Mode ○ Port-based VLAN ● IEEE 802.1Q VLAN

VLAN Port Settings

Port	CPUPort	Port01	Port02	Port03	Port04	Port05	Port06	Port07	Port08
Type	Access	Access	Access	Access	Access	Access	Access	Access	Access
PVID	1	1	1	1	1	1	1	1	1

802.1Q VLAN Settings

VID 2

Port	CPUPort	Port01	Port02	Port03	Port04	Port05	Port06	Port07	Port08
Type	**	**	**	**	**	**	**	**	**

("UnModified"This port is a VLAN member and the outgoing frames are not modified."UnTagged"This port is a VLAN member. Outgoing frames are unlabeled"Tagged" Ports are VLAN members, outgoing frames are marked:" ** "This port is not a VLAN member)

Port	CPUPort	Port01	Port02	Port03	Port04	Port05
VID:1	UnTagged	UnTagged	UnTagged	UnTagged	UnTagged	UnTagged

Main elements configuration descriptions of VLAN interface:

Interface Element	Note
VLAN Port Settings	**Port type and PVID settings column**
Port	Port number of the device.
CPU port	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	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 "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:

Interface Element	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, ● Tagged: reserve "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.

VLAN configuration operations are introduced from the following five aspects:

- Create VLAN
- Modify VLAN
- Delete VLAN
- VLAN configuration for all-purpose single ring
- Examples for typical VLAN configuration

Example: Create IEEE 802.1Q VLAN

Create a new IEEE 802.1Q VLAN.

Operation steps

Step 1 Open "Main Menu > L2 Feature > VLAN".

Step 2 On the displayed VLAN settings interface, configure "Type" of each port in the column of "VLAN Port Settings".

Step 3 In the column of "VLAN Port Settings", enter the default VLAN "PVID" value of each port.

Step 4 In the column of "802.1Q VLAN Settings", enter "VID" value of VLAN entry to be created.

Step 5 In the drop-down list of "Type", choose the member type of each port.

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

Step 7 Click “save configuration” button and reboot the device, and then VLAN creation is finished.

Step 8 End.

Note

VLAN configuration will take effect after rebooting.

Example: Modify IEEE 802.1Q VLAN

The operation can reconfigure the existing VLAN and change the “Type”, “Quantity”,etc.

Operation steps

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

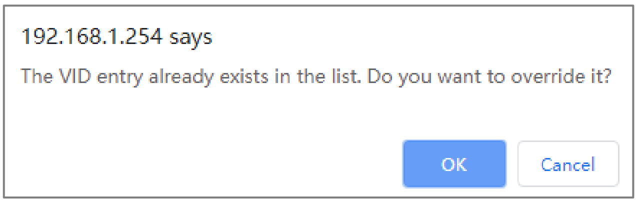
Step 2 In the column of “802.1Q VLAN Settings”, click a VLAN entry to be modified in the “Port”, such as VLAN1. And then the type of VLAN1 will display in the option of current VLAN entry settings.

Step 3 Modify the “VID” as required.

Step 4 Modify the “Type” as required.

Step 5 Click “Add” button.

Step 6 A prompt box pops up.



192.168.1.254 says

The VID entry already exists in the list. Do you want to override it?

Step 7 Click “Yes” to add the modified VLAN entry to the list.

Step 8 Click "Save” button.

Step 9 Enter “Main Menu > System Management > Device Management”.

Step 10 On the column of “Device Reboot”, click the button of “Reboot”.

Step 11 End.

Note

VLAN configuration will take effect after rebooting.

Example: Delete IEEE 802.1Q VLAN

The operation can delete existing VLAN

Operation steps

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

Step 2 On the column of “VLAN Port Settings”, click a VLAN entry to be modified in the “Port”.

Step 3 Click “Delete” button.

Step 4 Click “Apply”.

Step 5 Enter “Main Menu > Basic Settings > Network & Reboot”.

Step 6 On the column of “Device Reboot”, click the button of “Reboot”.

Step 7 End.

Note

VLAN configuration will take effect after rebooting.

Example: IEEE 802.1Q VLAN Configuration for the Single Ring

Note

VLAN of single ring means creating VLAN in the single ring to prevent too many data frames from entering the single ring, causing single ring blocking.

For example, create VLAN on the single ring composed of port 2~8, port G1 and G2, among which port G1 and port G2 are the ring network ports.

The operation steps are as follows:

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

Step 2 On the column of “VLAN Port Settings”, configure the port 1 as management port.

Note:
Management port refers to the port that can manage and configure switch, which also has to in the same VLAN with CPU port.
The default management port of system is port 1.

Step 3 On the “Type” setting row of “VLAN Port Settings” column:

1. Configure the “Type” of port 2-8 as “Access”.
2. Configure the “Type” of port G1 and G2 as “Trunk”.

Step 4 On the “PVID” setting row of “VLAN Port Settings” column:

1. Configure the “PVID” of port 2-8 as “2”.
2. Configure the “PVID” of port G1 and G2 as “2”.

Step 5 On the “VID” setting row of “802.1Q VLAN Settings” column, configure the value of “VID” as 2.

Step 6 On the “Type” setting row of “802.1Q VLAN Settings” column:

1. Configure the “Type” of port 2-8 as “Untagged”.
2. Configure the “Type” of port G1 and G2 as “Tagged”.

Step 7 Click “Add”.

Step 8 Click “Apply”.

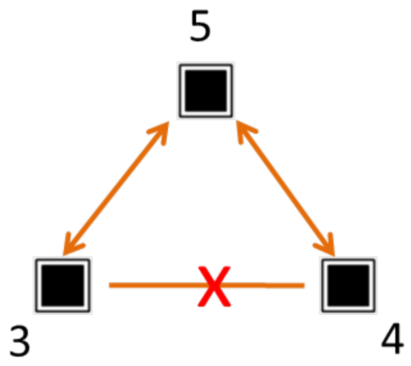
Step 9 Enter “Main Menu > System Management > Device Management”.

Step 10 On the column of “Device Reboot”, click the button of “Reboot”.

Step 11 End.

Example: Typical IEEE 802.1Q VLAN Configuration

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



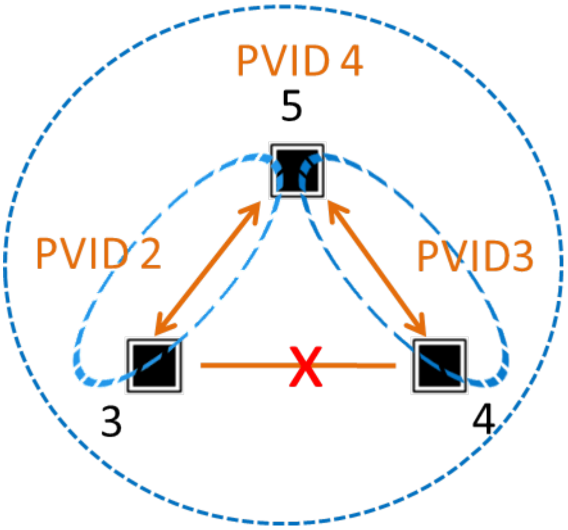
Instance analysis

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.
- Port4
  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:



Note:

The port here is for example only, please refer to the actual port number of the device.

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 In the drop-down list of “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.

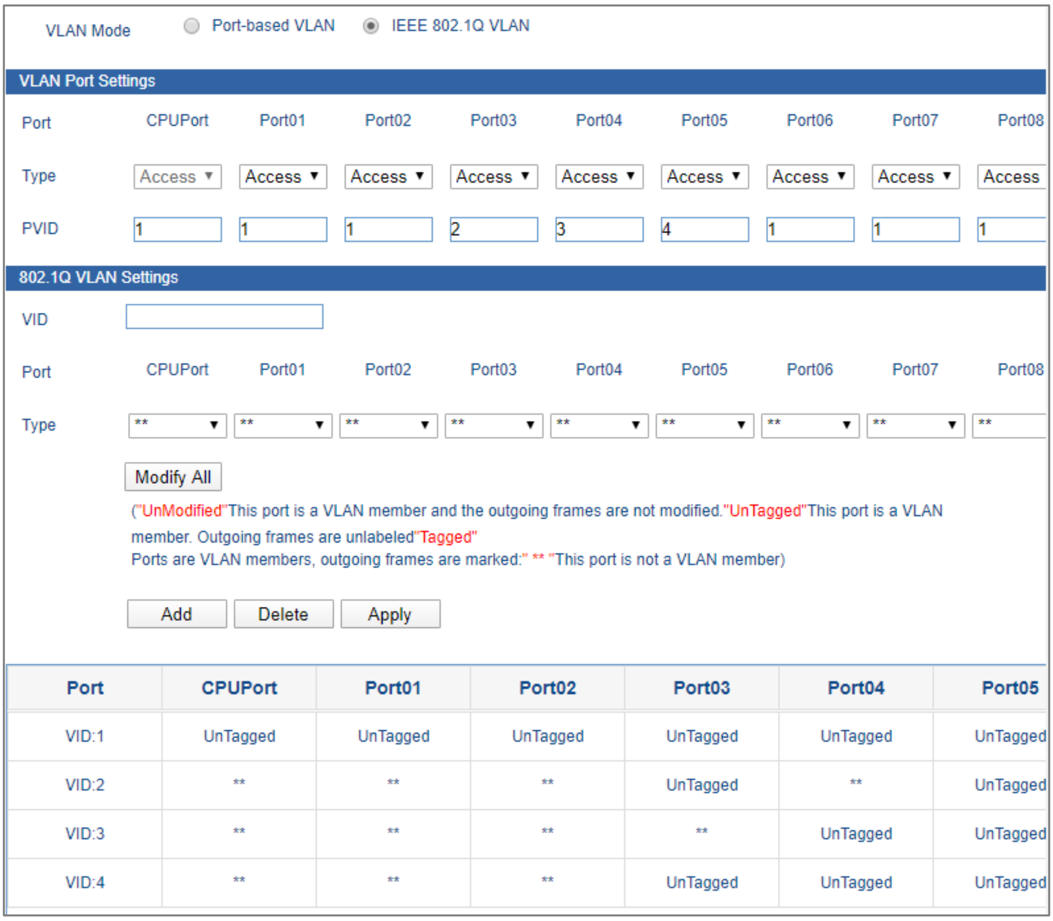
Step 9 Click “Add” button to add VLAN entry to the “Port”.

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

Step 11 In the drop-down list of “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”.



VLAN Mode ○ Port-based VLAN ● IEEE 802.1Q VLAN

VLAN Port Settings

Port	CPUPort	Port01	Port02	Port03	Port04	Port05	Port06	Port07	Port08
Type	Access	Access	Access	Access	Access	Access	Access	Access	Access
PVID	1	1	1	2	3	4	1	1	1

802.1Q VLAN Settings

VID

Port	CPUPort	Port01	Port02	Port03	Port04	Port05	Port06	Port07	Port08
Type	**	**	**	**	**	**	**	**	**

Modify All

("UnModified"This port is a VLAN member and the outgoing frames are not modified."UnTagged"This port is a VLAN member. Outgoing frames are unlabeled"Tagged" Ports are VLAN members, outgoing frames are marked:" ** "This port is not a VLAN member)

Add Delete Apply

Port	CPUPort	Port01	Port02	Port03	Port04	Port05
VID:1	UnTagged	UnTagged	UnTagged	UnTagged	UnTagged	UnTagged
VID:2	**	**	**	UnTagged	**	UnTagged
VID:3	**	**	**	**	UnTagged	UnTagged
VID:4	**	**	**	UnTagged	UnTagged	UnTagged

Step 13 Click “Apply”.

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

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

Step 16 End.

4.2 Multicast Filtering

4.2.1 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: members respond with IGMP report message when they receive IGMP IGMP General Query message. Members send IGMP Report messages to IGMP querier proactively to declare joining this multicast group.
- IGMP Leave message: members that run IGMPv2 or IGMPv3 send IGMP leave report to notify IGMP querier that they have left some multicast groups.

Function Description

On the “Multicast Filtering (IGMP Snooping)” page, user can:

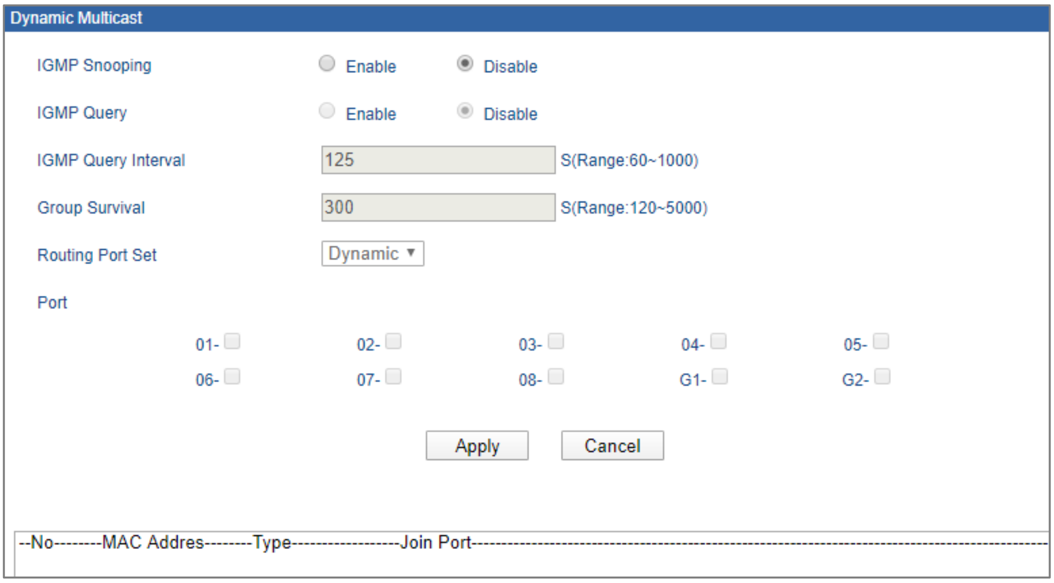
- Enable/disable IGMP snooping
- Enable/disable IGMP query
- Routing port settings

Operation Path

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

Interface Description

Multicast Filtering (IGMP Snooping) interface as below:



Dynamic Multicast

IGMP Snooping ○ Enable ● Disable

IGMP Query ○ Enable ● Disable

IGMP Query Interval 125 S(Range:60~1000)

Group Survival 300 S(Range:120~5000)

Routing Port Set Dynamic ▾

Port

01- □ 02- □ 03- □ 04- □ 05- □

06- □ 07- □ 08- □ G1- □ G2- □

Apply Cancel

--No--------MAC Addres--------Type-----------------Join Port---

The main element configuration description of Multicast Filtering (IGMP Snooping) interface:

Interface Element	Note
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.

4.2.2 Static Filtering

Static multicast filtering is used to set the forwarding port of static MAC address, one or multiple forwarding ports can be specified. The Static MAC Address requests a valid input from the user, and a warning message will pop up if the input is an invalid MAC Address.

Function Description

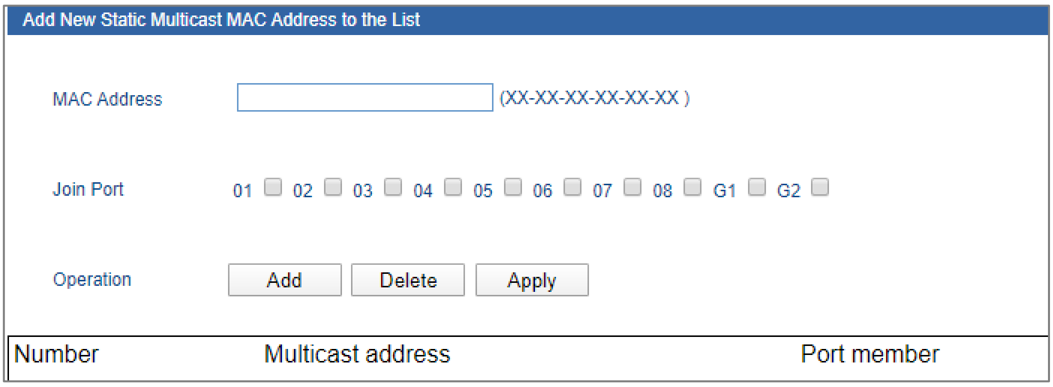
On the page of “Static Filtering”, user can configure the forwarding port list of static multicast.

Operation Path

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

Interface Description

Static filtering interface as follows:



Add New Static Multicast MAC Address to the List

MAC Address (XX-XX-XX-XX-XX-XX)

Join Port 01 □ 02 □ 03 □ 04 □ 05 □ 06 □ 07 □ 08 □ G1 □ G2 □

Number	Multicast address	Port member

Main elements configuration description of static filtering interface:

Interface Element	Note
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 “01”;
2. Tick the check box after “02”;
3. Tick the check box after “03”;

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.

5 QoS

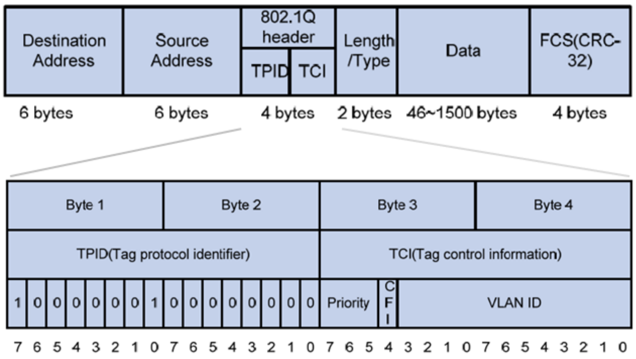
5.1 QoS Classification

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

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

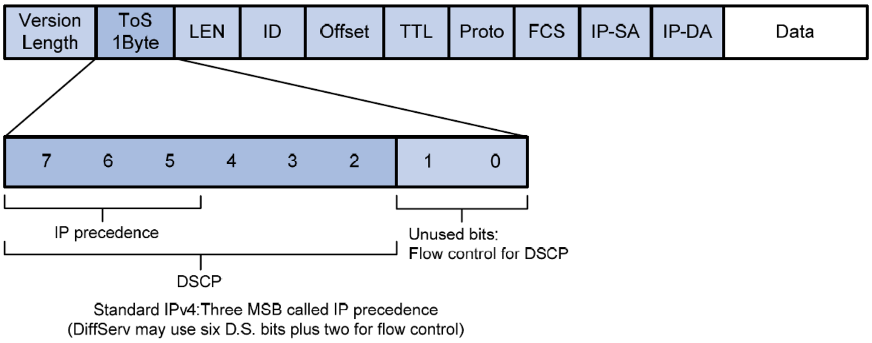
Priority is used to tag the priority of message transmission.

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



- ToS

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



Function Description

On the page of QoS Classification, user can set:

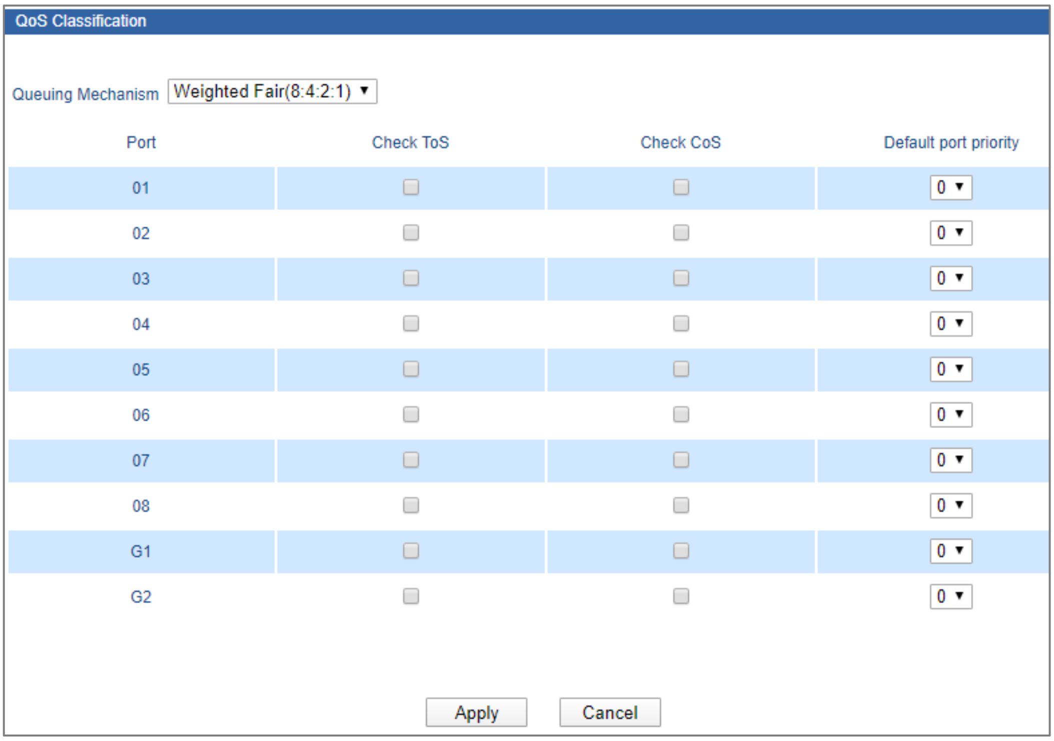
- Queuing mechanism
- Enable ToS
- Enable CoS
- Port priority.

Operation Path

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

Interface Description

Screenshot of QoS Classification interface:



QoS Classification

Queuing Mechanism: Weighted Fair(8:4:2:1) ▾

Port	Check ToS	Check CoS	Default port priority
01	□	□	0 ▾
02	□	□	0 ▾
03	□	□	0 ▾
04	□	□	0 ▾
05	□	□	0 ▾
06	□	□	0 ▾
07	□	□	0 ▾
08	□	□	0 ▾
G1	□	□	0 ▾
G2	□	□	0 ▾

The main element configuration description of QoS classification interface:

Interface Element	Note
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 "Check ToS".

Step 4 Click "Apply".

Step 5 End.

5.2 CoS Mapping

Function Description

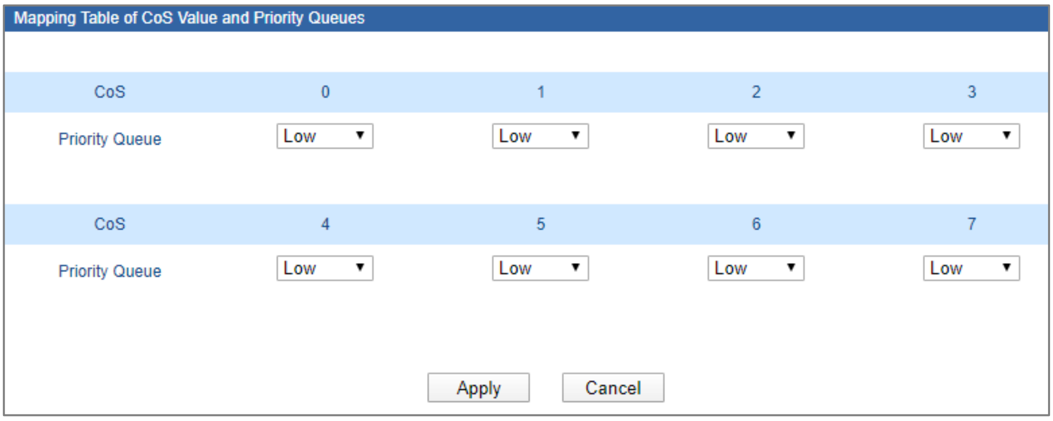
On the page of "CoS Mapping", user can configure mapping between CoS value and priority queues.

Operation Path

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

Interface Description

Screenshot of QoS Mapping interface:



Mapping Table of CoS Value and Priority Queues

CoS	0	1	2	3
Priority Queue	Low	Low	Low	Low
CoS	4	5	6	7
Priority Queue	Low	Low	Low	Low

The main element configuration description of QoS mapping interface:

Interface Element	Note
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.

5.3 ToS Mapping

Function Description

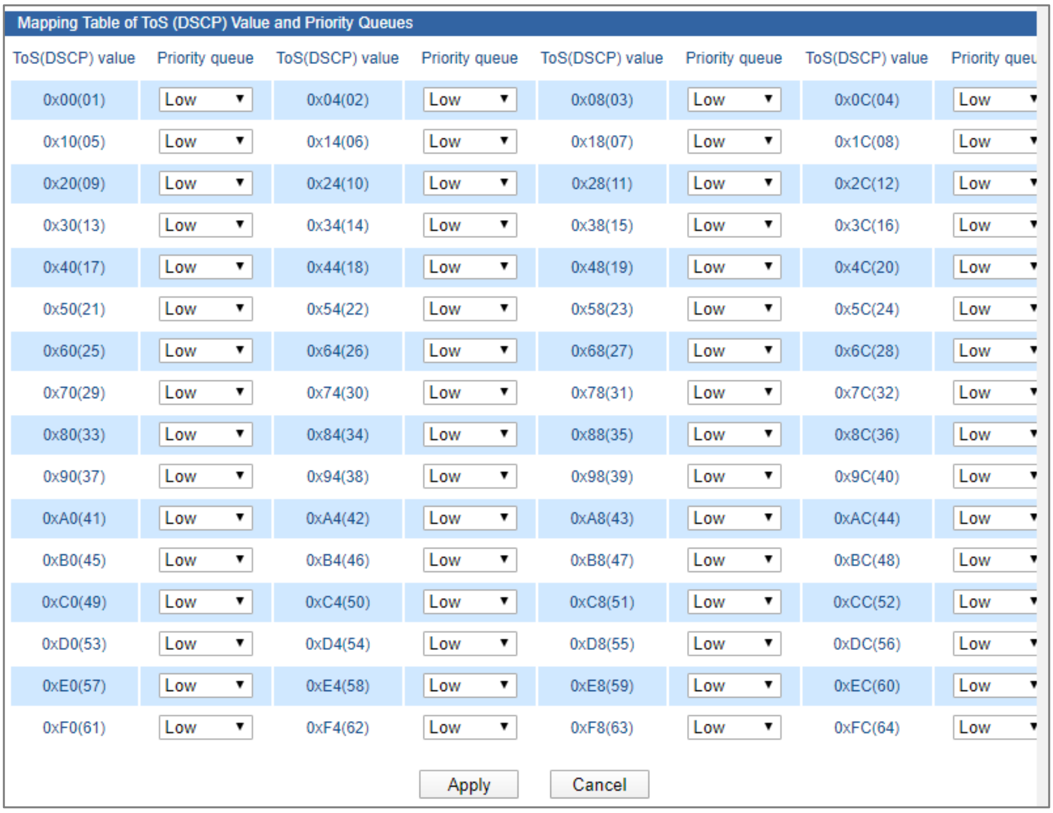
On the page of "ToS Mapping", user can configure mapping between CoS value and priority queue.

Operation Path

Open in order: "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 ▼

The main element configuration description of ToS mapping interface:

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

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.

6 Link Backup

6.1 Rapid Ring

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

- SW-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 has made improvement on the basis of STP, which has achieved quick topological convergence of network. (The fastest speed could be in 1 second) Equipments running STP/RSTP protocol find the loop in the network by interact information, and congest the ports selectively to cut the ring network structure to a non-loop tree network structure, thus preventing message cycle in the ring network and the decline in processing capacity of the device due to the repetitive receiving of the same message.

  Working process of STP:
  - First, elect 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

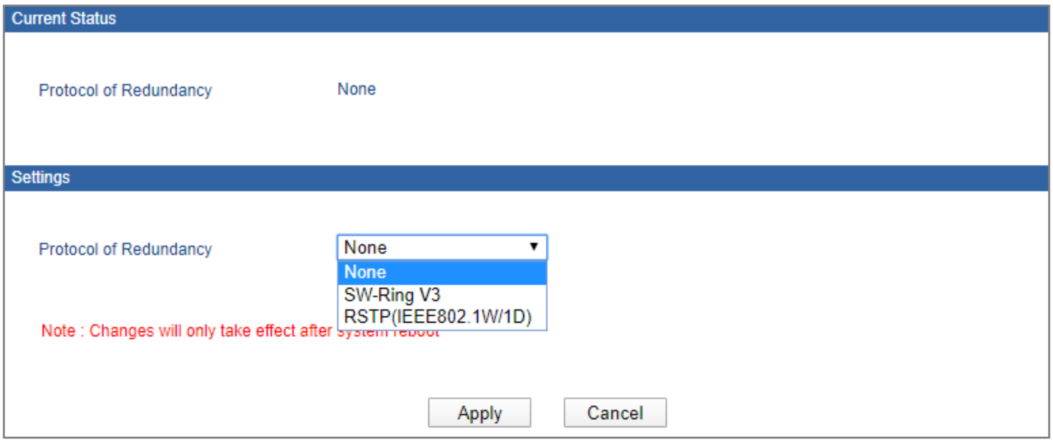
On the “Rapid ring” page, user can choose redundancy protocol and configure the ring network under this protocol quickly.

Operation Path

Open in order: “Main Menu > Redundancy > Rapid Ring”.

Interface Description

Initial rapid ring interface as follows:



Current Status

Protocol of Redundancy None

Settings

Protocol of Redundancy None

Note : Changes will only take effect after system reboot

The main element configuration description of initial rapid ring interface:

Interface Element	Note
Current Status	**Current status bar**

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

Function description of SW-Ring V3

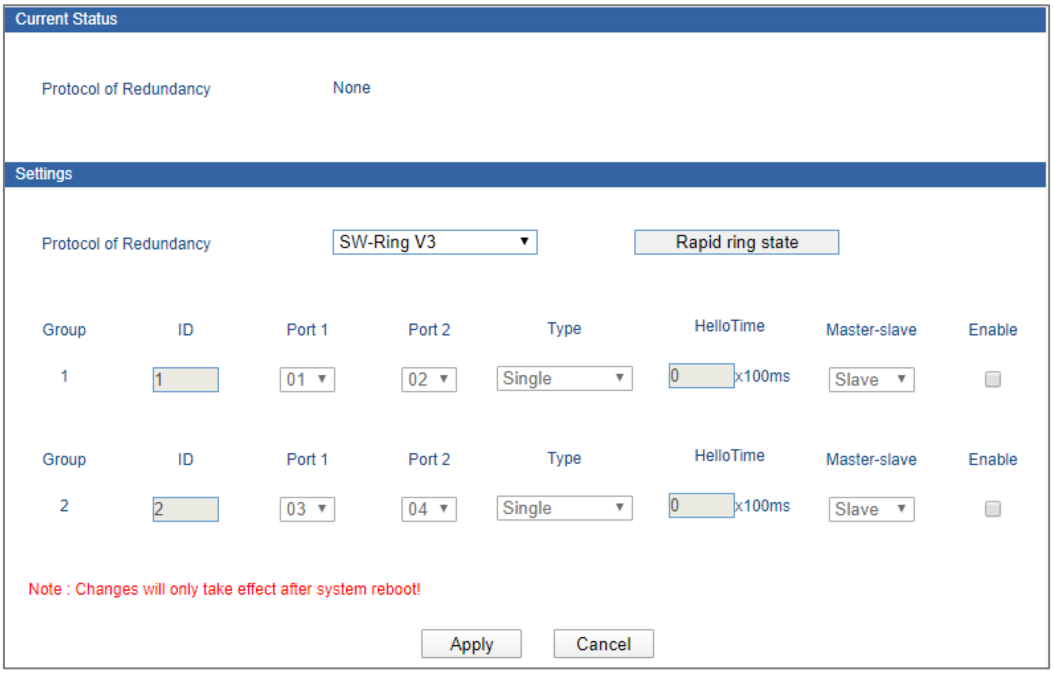
On the “rapid ring” page, user can choose Ring redundancy protocol and configure the ring network under this protocol quickly.

Operation Path

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

Interface Description

SW-Ring network interface as follows:



Current Status

Protocol of Redundancy None

Settings

Protocol of Redundancy SW-Ring V3

Group	ID	Port 1	Port 2	Type	HelloTime	Master-slave	Enable
1	1	01	02	Single	0 x100ms	Slave	□
2	2	03	04	Single	0 x100ms	Slave	□

Note : Changes will only take effect after system reboot!

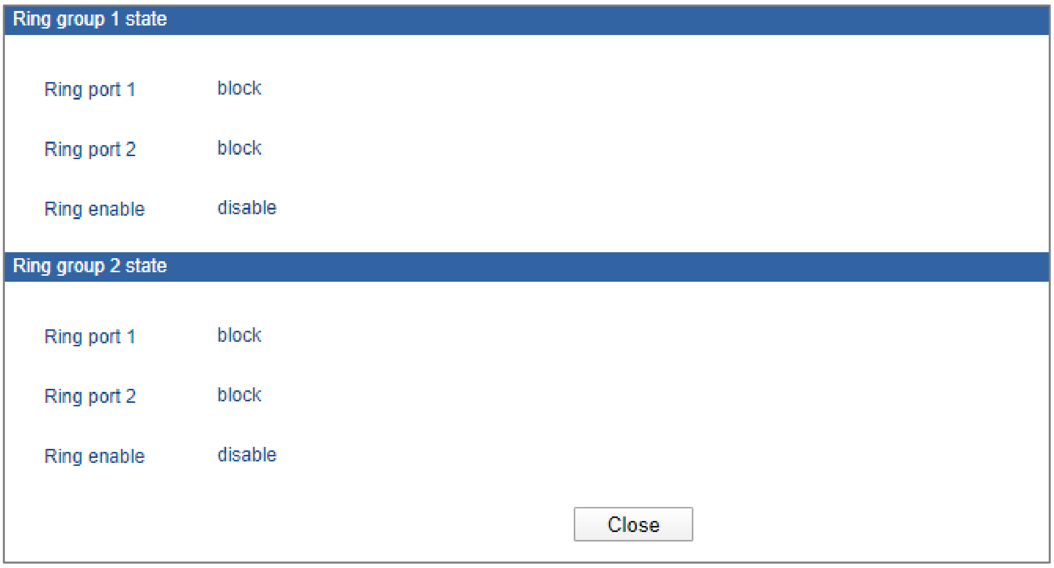
The main element configuration description of Ring network interface:

Interface Element	Note
Protocol of Redundacy	Click “rapid ring state” to check the ring state of current ring network group configuration.
Group	Support Group 1-2 or Group 1-4, it means that the device supports up to 2 or 4 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	The network port 2 on the switch device used to form a ring.
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.
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.

Interface Element	Note
	● 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 time interval of Hello packet transmission. It is a query packet sent to adjacent device via ring network port to confirm whether the connection is normal.
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. Note: Some products don't support Master-slave option, so their ring network is non-master station structure.
Enable	Enable or disable the corresponding ring group.

Click "rapid ring state" to check the ring state of current ring network group configuration.

Rapid ring state interface as follows:



Ring group 1 state

Ring port 1 block

Ring port 2 block

Ring enable disable

Ring group 2 state

Ring port 1 block

Ring port 2 block

Ring enable disable

The main element configuration description of rapid ring interface

Interface Element	Note
Ring group state	Display the current state of ring group, ring port and ring enable.

Interface Element	Note
Ring port	Display the current state of ring port in the ring group.
Ring enable	Display the current state of ring enable.

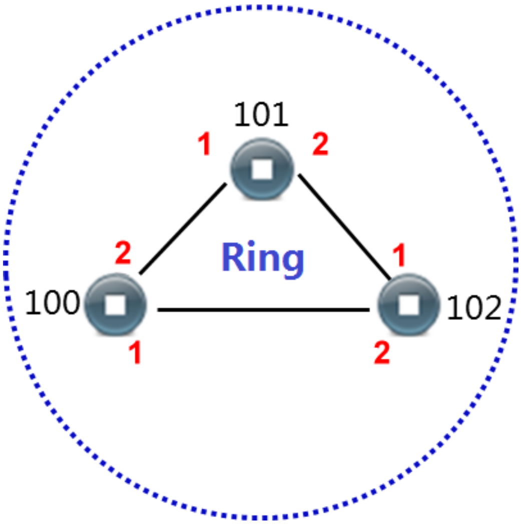
Now introduce the creation process respectively according to different ring network:

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

6.1.1 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

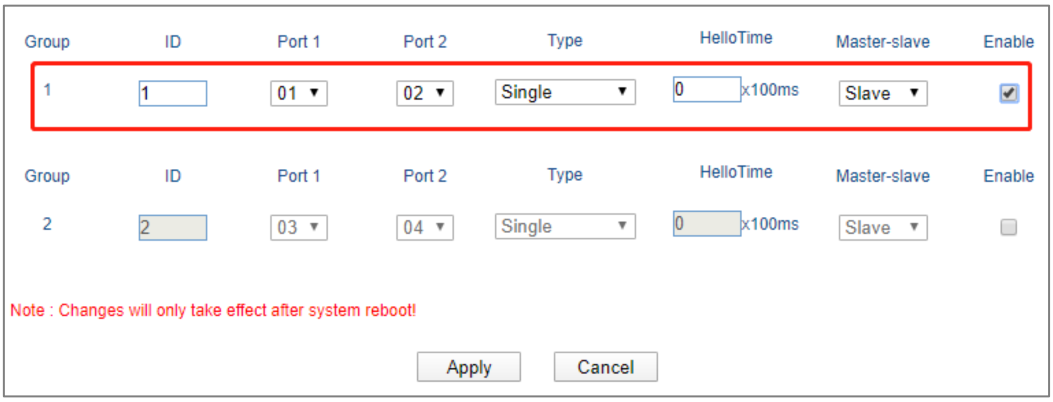
Configuring Device 100, 101 and 102 in the following steps:

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

Step 2 In the “Settings” area of “Rapid Ring” page, choose “SW-Ring V3” as “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”.



Group	ID	Port 1	Port 2	Type	HelloTime	Master-slave	Enable
1	1	01	02	Single	0 x100ms	Slave	☑

Group	ID	Port 1	Port 2	Type	HelloTime	Master-slave	Enable
2	2	03	04	Single	0 x100ms	Slave	☐

Note : Changes will only take effect after system reboot!

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 For Device 100 and 101, choose “Slave” in the drop-down list of “Master-slave” of “Group 1”.

Step 8 For Device 102, choose “Master” in the drop-down list of “Master-slave” of “Group 1”.

Step 9 Click “Apply”. Enter “Main Menu > System Management > Device Address”.

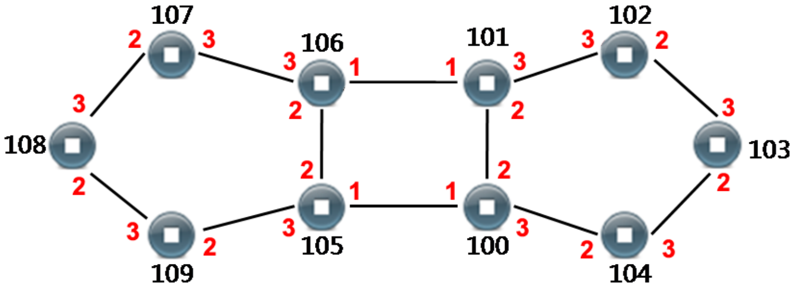
Step 10 In the area of “reboot the device”, click “reboot”.

Step 11 End.

6.1.2 Instance: create coupling ring

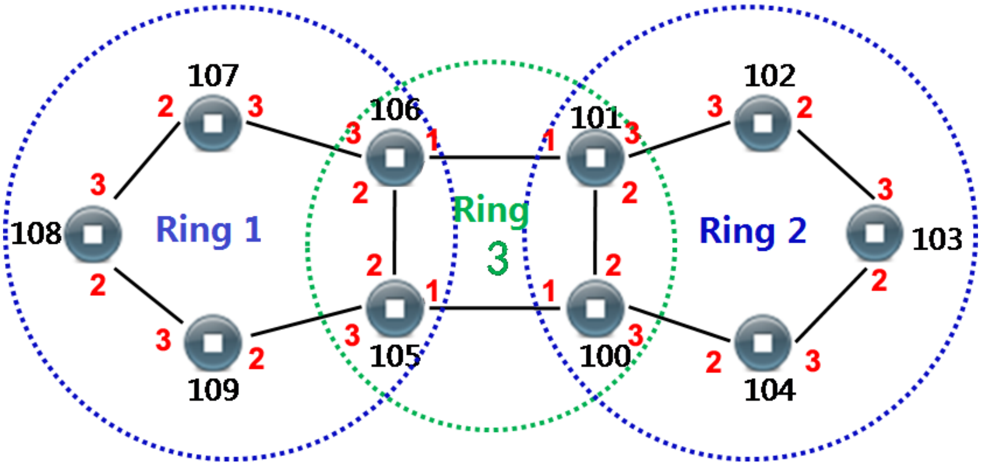
Instance

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; 105 is the master station, others are slave stations.
- 100, 101, 102, 103 and 104 are in Ring 2; ring network ports are Port 2 and Port 3; single ring; 100 is the master station, others are slave stations;
- 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

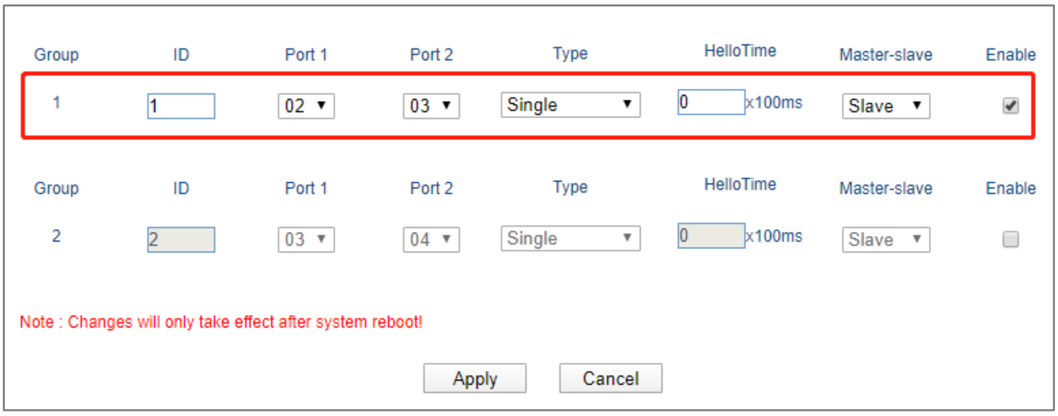
Configuring Device 105, 106, 107, 108 and 109 in the following steps respectively.

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

Step 2 In the “Settings” area of “Rapid Ring” page, choose “SW-Ring V3” as “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”.



Group	ID	Port 1	Port 2	Type	HelloTime	Master-slave	Enable
1	1	02	03	Single	0 x100ms	Slave	☑

Group	ID	Port 1	Port 2	Type	HelloTime	Master-slave	Enable
2	2	03	04	Single	0 x100ms	Slave	□

Note : Changes will only take effect after system reboot!

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

Step 6 Set “Port 1” and “Port 2” to “02” and “03” respectively.

Note:

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

Step 7 For Device 106/107/108/109, choose “Slave” in the drop-down list of “Master-slave” of “Group 1”.

Step 8 For Device 105, choose “Master” in the drop-down list of “Master-slave” of “Group 1”.

Step 9 Click “Apply”. Enter “Main Menu > System Management > Device Management”.

Step 10 In the area of “reboot the device”, click “reboot”.

Step 11 End.

Operation Step 2: configuring Ring 2 in WEB interface

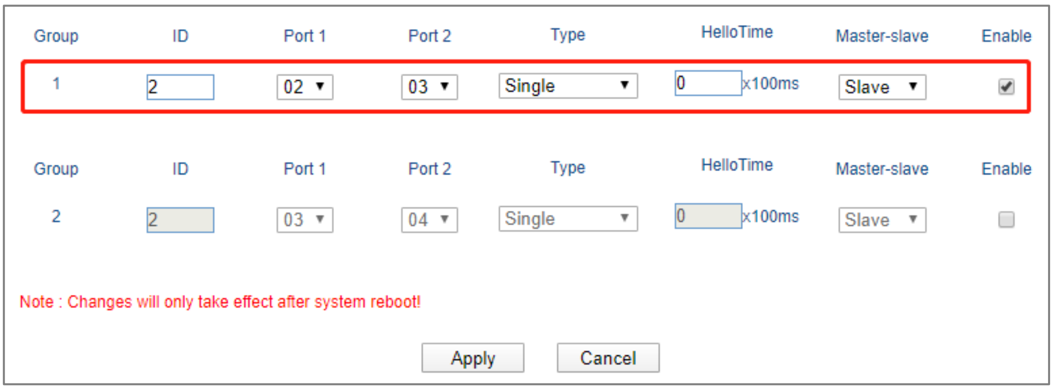
Configuring Device 100, 101, 102, 103 and 104 in the following steps respectively.

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

Step 2 In the “Settings” area of “Rapid Ring” page, choose “SW-Ring V3” as “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”.



Group	ID	Port 1	Port 2	Type	HelloTime	Master-slave	Enable
1	2	02	03	Single	0 x100ms	Slave	☑

Group	ID	Port 1	Port 2	Type	HelloTime	Master-slave	Enable
2	2	03	04	Single	0 x100ms	Slave	☐

Note : Changes will only take effect after system reboot!

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 For Device 101/102/103/104, choose “Slave” in the drop-down list of “Master-slave” of “Group 1”.

Step 8 For Device 100, choose “Master” in the drop-down list of “Master-slave” of “Group 1”.

Step 9 Click “Apply”. Enter “Main Menu > System Management > Device Management”.

Step 10 In the area of “reboot the device”, click “reboot”.

Step 11 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 “Settings” area of “Rapid Ring” page, choose “SW-Ring V3” as “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”.

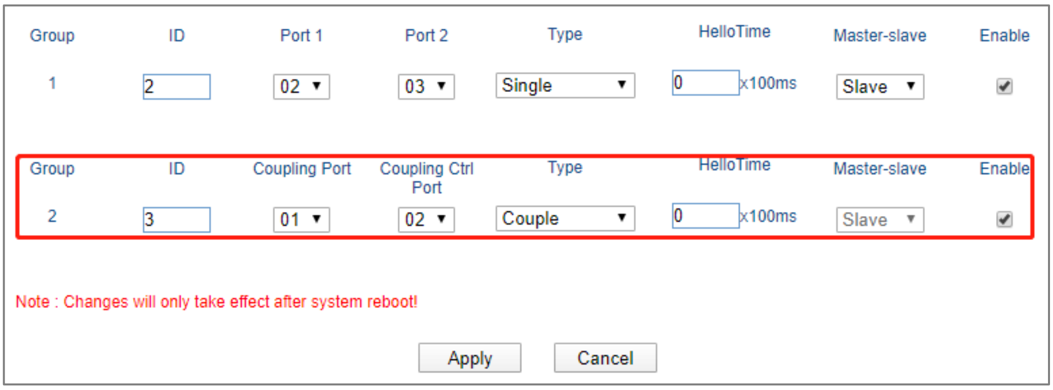
Step 6 Choose “1” in the drop-down list of “Coupling Port” of “Group 2”.

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 Management”.

Step 9 In the area of “reboot the device”, click “reboot”.

Step 10 End.



Group	ID	Port 1	Port 2	Type	HelloTime	Master-slave	Enable
1	2	02 ▼	03 ▼	Single ▼	0 x100ms	Slave ▼	☑

Group	ID	Coupling Port	Coupling Ctrl Port	Type	HelloTime	Master-slave	Enable
2	3	01 ▼	02 ▼	Couple ▼	0 x100ms	Slave ▼	☑

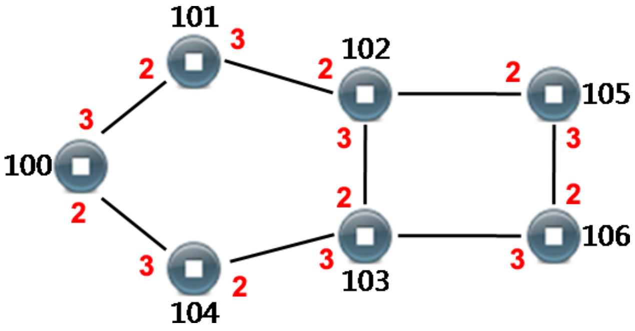
Note : Changes will only take effect after system reboot!

6.1.3 Instance: creating chain

The chain could be created when the “Protocol of Redundancy” is “SW-Ring V3”.

Instance

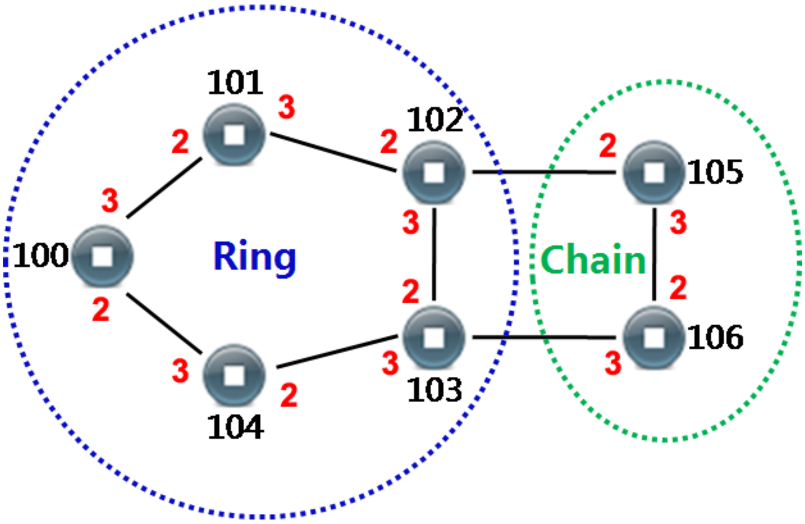
For example: creating chain. Its basic architecture is shown as below:



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 100 is the master station, others are slave stations.
- 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 “Settings” area of “Rapid Ring” page, choose “SW-Ring V3” as “Protocol of Redundancy”.

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

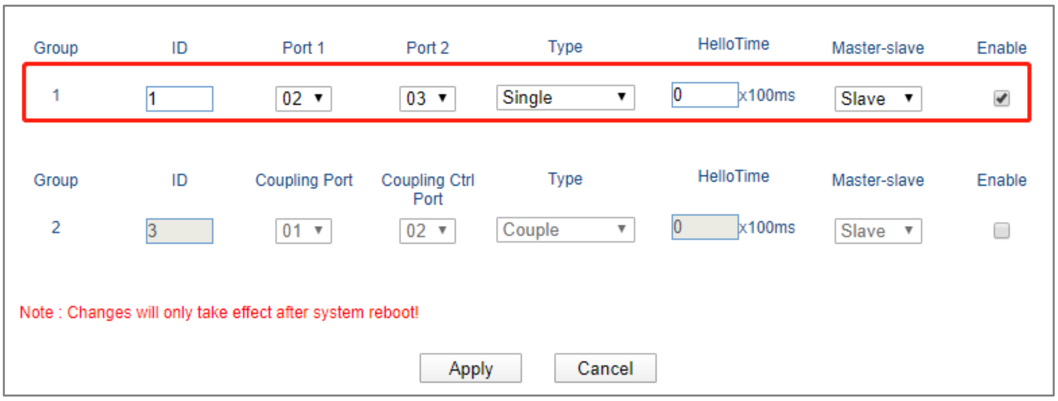
Step 4 In the “settings” area of “Rapid Ring”:

1 Set “Type” to “Single”;

2 Set “ID” to “1”;

3 Set “Port 1” to “2”;

4 Set “Port 2” to “3”;



Group	ID	Port 1	Port 2	Type	HelloTime	Master-slave	Enable
1	1	02 ▼	03 ▼	Single ▼	0 x100ms	Slave ▼	☑

Group	ID	Coupling Port	Coupling Ctrl Port	Type	HelloTime	Master-slave	Enable
2	3	01 ▼	02 ▼	Couple ▼	0 x100ms	Slave ▼	□

Note : Changes will only take effect after system reboot!

Step 5 For Device 101/102/103/104, choose “Slave” in the drop-down list of “Master-slave” of “Group 1”.

Step 6 For Device 100, choose “Master” in the drop-down list of “Master-slave” of “Group 1”.

Step 7 Click “Apply”.

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

Step 9 In the area of “reboot the device”, click “reboot”.

Step 10 End.

Operation Step 2: creating chain

Configuring Device 105 and 106 in the following steps respectively.

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

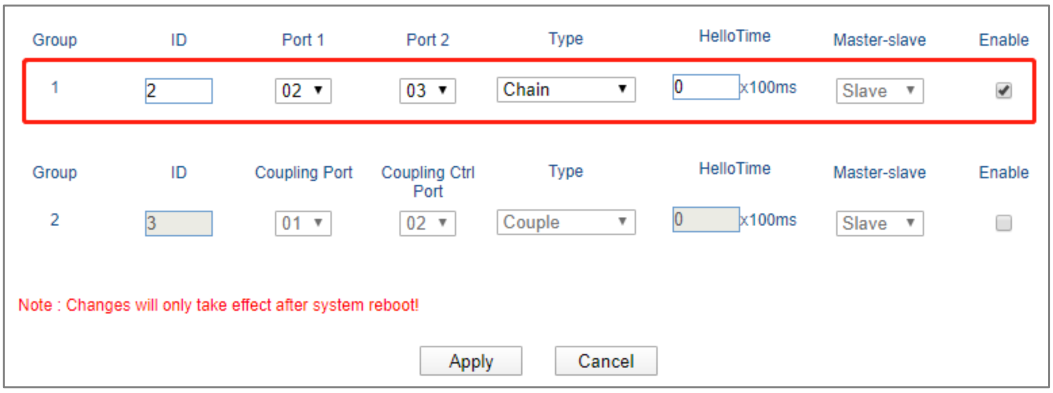
Step 2 In the “Settings” area of “Rapid Ring” page, choose “SW-Ring V3” as “Protocol of Redundancy”.

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”.



Group	ID	Port 1	Port 2	Type	HelloTime	Master-slave	Enable
1	2	02	03	Chain	0 x100ms	Slave	☑

Group	ID	Coupling Port	Coupling Ctrl Port	Type	HelloTime	Master-slave	Enable
2	3	01	02	Couple	0 x100ms	Slave	□

Note : Changes will only take effect after system reboot!

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 Management”.

Step 9 In the area of “reboot the device”, click “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.

6.1.4 Creating Spanning Tree

Function Description

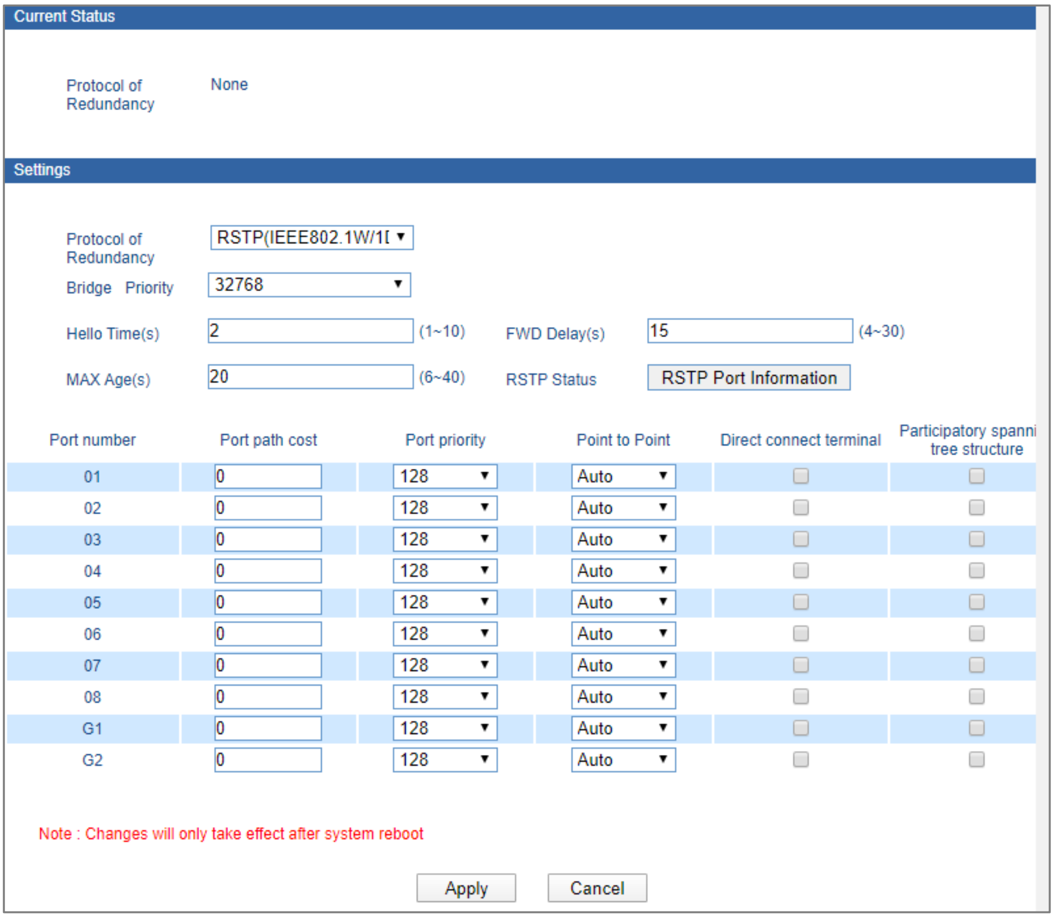
On the "Rapid ring" page, user can choose "RSTP (IEEE 802.1W/1D)" as redundancy protocol to create spanning tree quickly.

Operation Path

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

Interface Description

RSTP interface as follows:



Current Status

Protocol of Redundancy: None

Settings

Protocol of Redundancy: RSTP(IEEE802.1W/1[

Bridge Priority: 32768

Hello Time(s): 2 (1~10)

FWD Delay(s): 15 (4~30)

MAX Age(s): 20 (6~40)

RSTP Status: RSTP Port Information

Port number	Port path cost	Port priority	Point to Point	Direct connect terminal	Participatory spanni tree structure
01	0	128	Auto	□	□
02	0	128	Auto	□	□
03	0	128	Auto	□	□
04	0	128	Auto	□	□
05	0	128	Auto	□	□
06	0	128	Auto	□	□
07	0	128	Auto	□	□
08	0	128	Auto	□	□
G1	0	128	Auto	□	□
G2	0	128	Auto	□	□

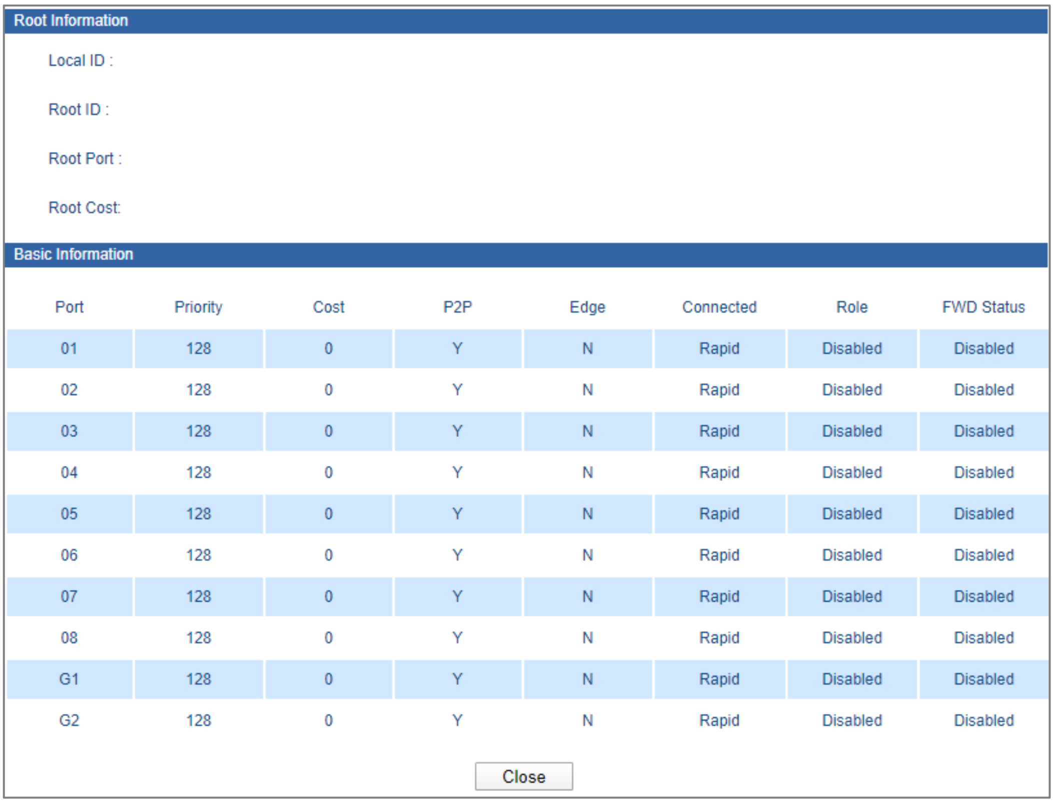
Note : Changes will only take effect after system reboot

The main element configuration description of RSTP interface:

Interface Element	Note
Protocol of Redundancy	Choose the algorithm of redundancy protocol, options are: • None: it means that the ring network function is disabled. • SW-Ring V3: supports single ring, coupling ring, chain and Dual_homing; • 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 (s)	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 (s)	The forward delay time that the port of switch maintains in transition state (listening and learning). Note:

Interface Element	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 (s)	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.
Port path 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.
Participatory spanning tree structure	Checking this checkbox. It represents participating in the operation of spanning tree protocol.

RSTP status interface as follows:



Root Information

Local ID :

Root ID :

Root Port :

Root Cost:

Basic Information

Port	Priority	Cost	P2P	Edge	Connected	Role	FWD Status
01	128	0	Y	N	Rapid	Disabled	Disabled
02	128	0	Y	N	Rapid	Disabled	Disabled
03	128	0	Y	N	Rapid	Disabled	Disabled
04	128	0	Y	N	Rapid	Disabled	Disabled
05	128	0	Y	N	Rapid	Disabled	Disabled
06	128	0	Y	N	Rapid	Disabled	Disabled
07	128	0	Y	N	Rapid	Disabled	Disabled
08	128	0	Y	N	Rapid	Disabled	Disabled
G1	128	0	Y	N	Rapid	Disabled	Disabled
G2	128	0	Y	N	Rapid	Disabled	Disabled

The main element configuration description of RSTP status interface:

Interface Element	Note
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	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.
Cost	The path cost from network bridge to root bridge.
P2P	The directly connected switch port.
Edge	The port that directly connects to terminal instead of other switches.
Connected	It displays the network protocol of devices with connected ports.
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.

6.2 Loop Protection

Function Description

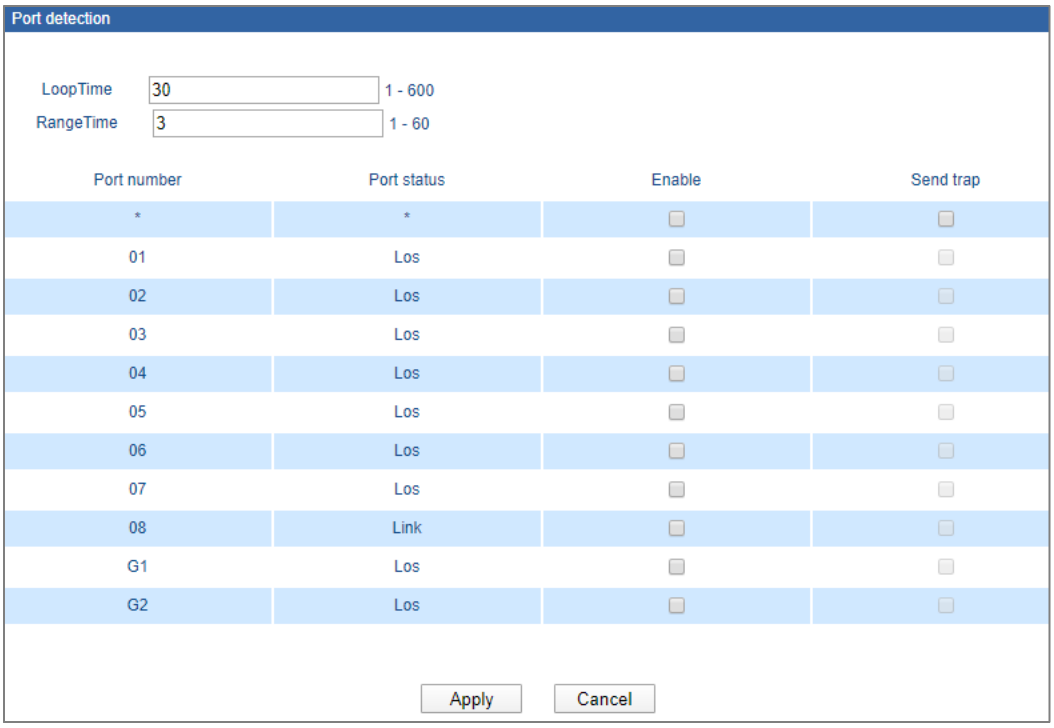
On the "Loop Protection" page, you can configure loop protection to avoid network storms.

Operation Path

Open in order: “Main Menu > Link Backup > Loop Protection”.

Interface Description

Loop Protection Interface Screenshot:



Port detection

LoopTime 30 1 - 600

RangeTime 3 1 - 60

Port number	Port status	Enable	Send trap
*	*	□	□
01	Los	□	□
02	Los	□	□
03	Los	□	□
04	Los	□	□
05	Los	□	□
06	Los	□	□
07	Los	□	□
08	Link	□	□
G1	Los	□	□
G2	Los	□	□

Main elements configuration descriptions of Loop Protection interface:

Interface Element	Note
LoopTime	Time interval for detection after loop formation. Value range is 1-600, default value: 30, unit: seconds.
RangeTime	Time interval before loop formation, ranging from 1--60, default value: 5, unit: second.
Port number	Display the device port number.
Port status	Display port connection status of the device： ● LOS: disconnected ● LINK: connected ● Loop Forward: the forwarding port in the loop ● Loop Block: the blocking port in the loop Note: After the page is refreshed, the Loop Forward state will quickly switch to the Link state.
Enable	If the loop protection function is enabled, when there is a port self-loop or a port loop, the loop can be quickly disconnected, and the port status can be set to blocking or forwarding to avoid network storms.

	Notice: The loop port cannot be set as a loop detection port.
Send trap	Check the box to enable sending trap. When the self-loop and the ring are formed, the TRAP alarm will be sent. Note: Before enabling this function, SNMP configuration function needs to be enabled on the "SNMP configuration" page first, and SNMP Trap address needs to be set.

6.3 Port Trunking

Link aggregation technology can achieve the goal of increasing link bandwidth through binding multiple physical interfaces to one logical interface without upgrading hardware. While increasing the bandwidth, link aggregation adopts the mechanism of backup link, which can effectively improve the reliability of link between devices.

Link aggregation technology has the following three advantages:

- Increase bandwidth
  The maximum bandwidth of link aggregation interface can reach the sum of the bandwidth of each member interface.
- Improve the reliability
  When an active link fails, traffic can be switched to other available member links, thus improving the reliability of link aggregation interface.
- Load sharing
  Within a link aggregation group, load sharing can be achieved on the active links of each member.

Function Description

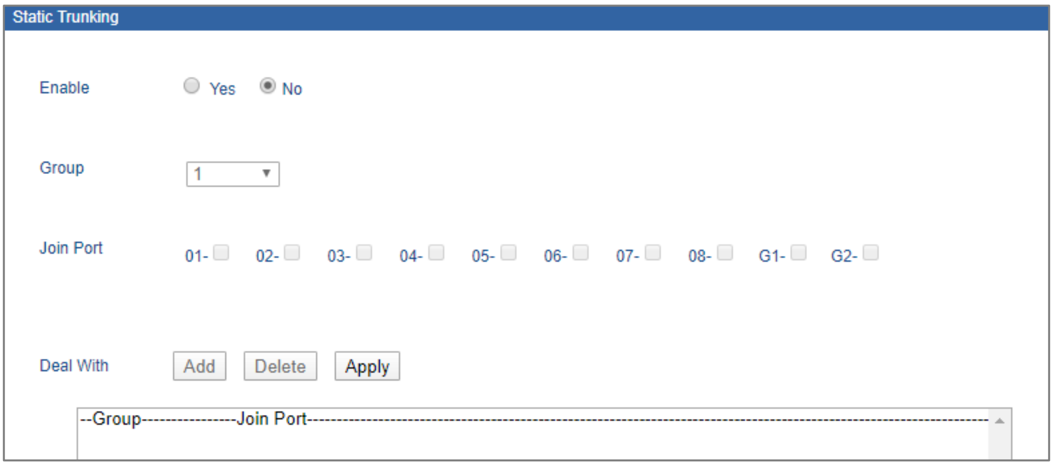
Binding multiple physical ports into one logical channel.

Operation Path

Open in order: “Main Menu > Redundancy > Port Trunking > Static Trunking”.

Interface Description

Static Trunking interface as follows:



Static Trunking

Enable ○ Yes ● No

Group 1

Join Port 01- □ 02- □ 03- □ 04- □ 05- □ 06- □ 07- □ 08- □ G1- □ G2- □

Deal With

--Group---------------Join Port---

The main element configuration description of static trunking interface:

Interface Element	Note
Enable	Enable or disable trunking configuration.
Group	Choose trunking group.
Join Port	Check the box of ports that join the trunking group.
Deal with	Add, edit, delete or apply the configuration of port trunking group.

For instance: port trunking

For example: if the port 1 and port 2 of switch A and switch B share the same rates and duplex modes. To increase bandwidth, Port 1 and Port 2 of Switch A and Switch B are now required to converge into a Trunking group.

Operation steps

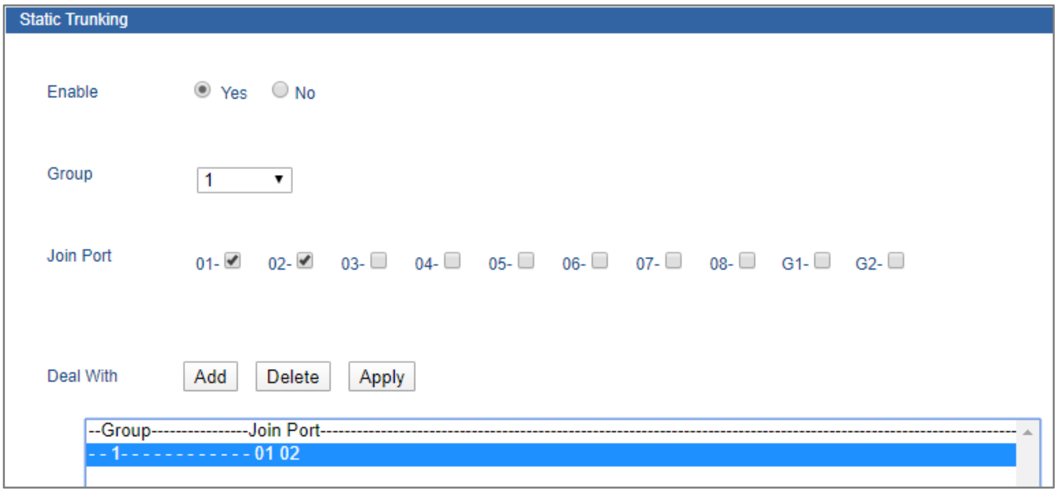
Configure switch A and switch B in the same way respectively.

Step 1 Log into Web configuration interface.

Step 2 Choose “Main Menu > Redundancy > Port Trunking > Static Trunking”.

Step 3 On the page of “Static Trunking”, check the box of “Yes” in the “Enable” bar.

Step 4 Choose “1” in the droplist of “Group”.



Static Trunking

Enable ● Yes ○ No

Group 1

Join Port 01- ☑ 02- ☑ 03- □ 04- □ 05- □ 06- □ 07- □ 08- □ G1- □ G2- □

Deal With

--Group---------------Join Port---

- - 1- - - - - - - - - - - - 01 02

Step 5 Check the box of Port 1 and Port 2 in the “join port” bar.

Step 6 Click “Add/Edit”.

Step 7 Click “Apply”.

Step 8 End.

Note

- All attributes of ports in trunking group should be the same, including rates and duplex modes, etc.
- Setting one port as both ring network port and trunking port is not supported.
- Each trunking group should have 2 ports at least, up to 4.
- One port can only join a trunking group.

7 LLDP

7.1 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 received TTL value in the LLDPDU equals to zero, the neighbor information would be aged immediately.

Function Description

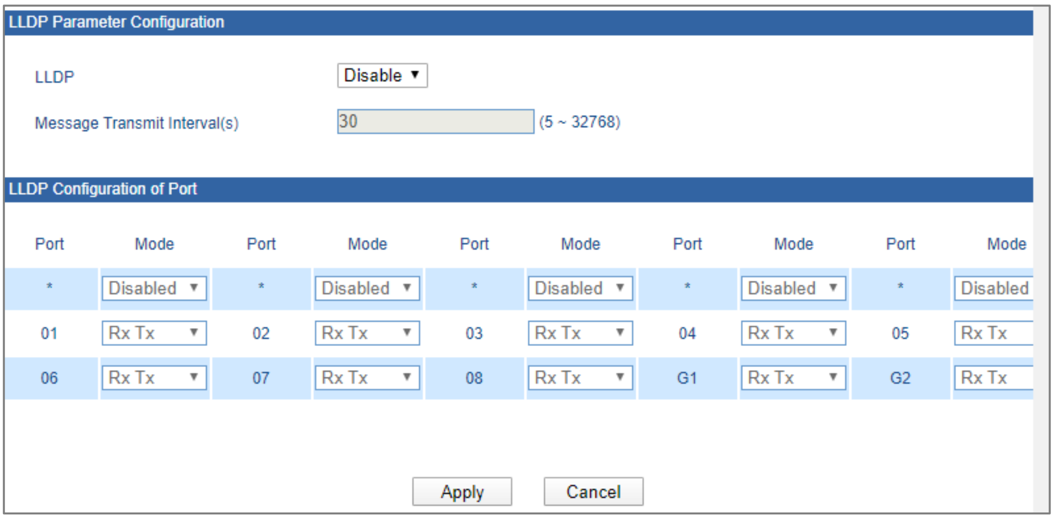
On the page of “Parameters Configuration”, user can configure LLDP function of the port and notify its device identity and performance in the local device.

Operation Path

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

Interface Description

Parameter configuration interface as follows:



LLDP Parameter Configuration

LLDP: Disable

Message Transmit Interval(s): 30 (5 ~ 32768)

LLDP Configuration of Port

Port	Mode	Port	Mode	Port	Mode	Port	Mode	Port	Mode
*	Disabled	*	Disabled	*	Disabled	*	Disabled	*	Disabled
01	Rx Tx	02	Rx Tx	03	Rx Tx	04	Rx Tx	05	Rx Tx
06	Rx Tx	07	Rx Tx	08	Rx Tx	G1	Rx Tx	G2	Rx Tx

Main elements configuration description of parameter configuration interface:

Interface Element	Note
LLDP	Enable/disable LLDP function.
Messages Transmit Interval (s)	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	• Disable: disable LLDP function. • Tx Rx: send and receive LLDP message. • Tx only: periodically send LLDP message to neighbor device.

Interface Element	Note
	- Rx only: check the validity of received LLDP and carried TLV, and configure the ageing time of neighbor device in the local device according to TTL (Time To Live) value in TLV.

7.2 Neighbor Information

Function Description

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

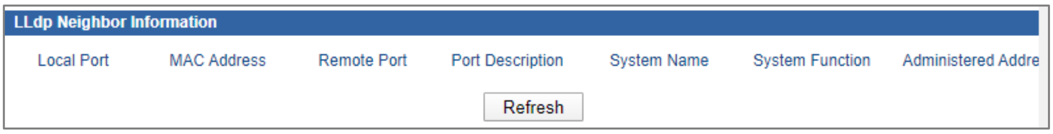
- MAC address;
- Remote port;
- Port description;
- System name;
- System function;
- Management address.

Operation Path

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

Interface Description

Neighbor information interface as follows:



LLdp Neighbor Information

Local Port	MAC Address	Remote Port	Port Description	System Name	System Function	Administered Addre

Main elements configuration description of neighbor information interface:

Interface Element	Note
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	Note
Administered 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.

8 Access Control

8.1 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 view permissions.

Function Description

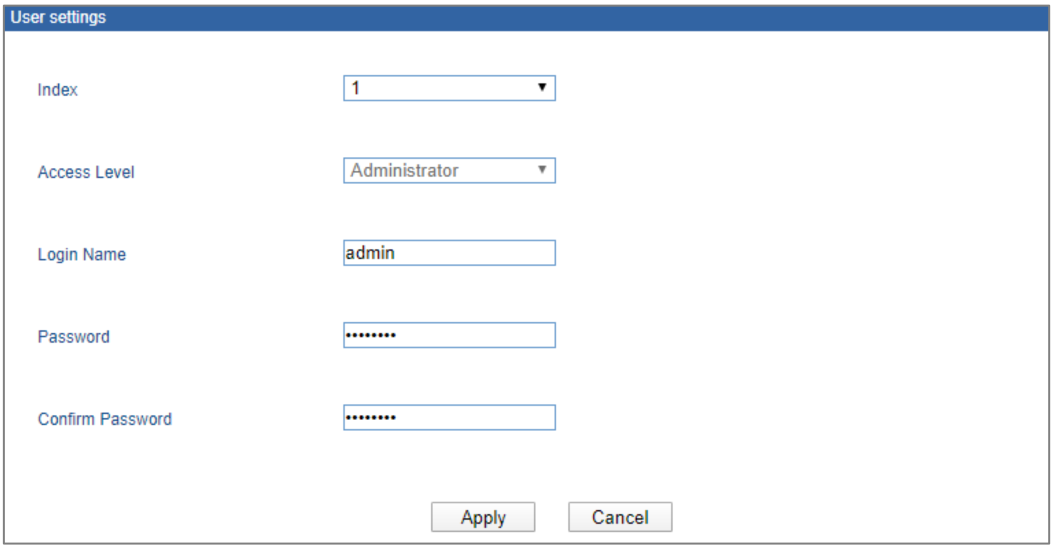
On the page of “Login Settings”, user can configure the login name, password and other parameters information of logging in to WEB configuration page.

Operation Path

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

Interface Description

User password interface as follows:



Index: 1

Access Level: Administrator

Login Name: admin

Password: ••••••••

Confirm Password: ••••••••

The main element configuration description of login settings interface:

Interface Element	Note
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.
Login 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.

8.2 IEE802.1X

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

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

802.1X structure mainly consists of three parts:

- Supplicant: user or client that wants to get the authentication;
- authentication server: typical example is RADIUS server;

- Authentication system Authenticator: access devices, such as wireless access points, switches, etc

8.2.1 IEEE802.1X Attestation

Function Description

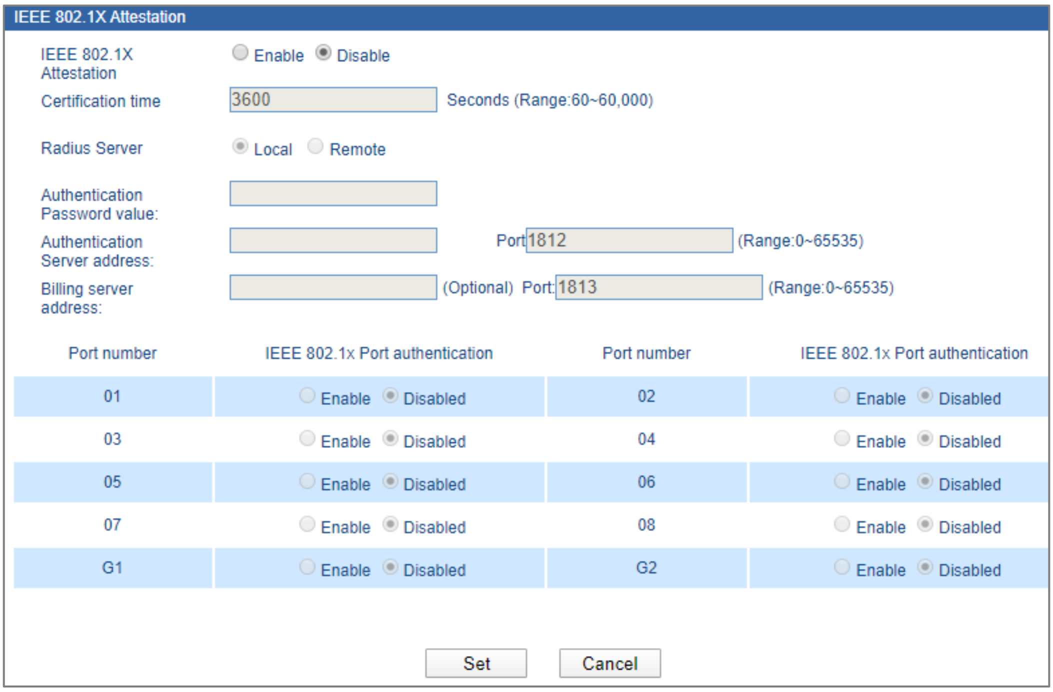
On the "IEEE 802.1X attestation" page, user can configure 802.1x authentication and Radius server parameters.

Operation Path

Open in order: "Main Menu > Access Control > IEEE 802.1X > IEEE 802.1X attestation ".

Interface Description

IEEE 802.1X attestation interface is as follows:



IEEE 802.1X Attestation

IEEE 802.1X Attestation ○ Enable ● Disable

Certification time 3600 Seconds (Range:60~60,000)

Radius Server ● Local ○ Remote

Authentication Password value:

Authentication Server address: Port 1812 (Range:0~65535)

Billing server address: (Optional) Port 1813 (Range:0~65535)

Port number	IEEE 802.1x Port authentication	Port number	IEEE 802.1x Port authentication
01	○ Enable ● Disabled	02	○ Enable ● Disabled
03	○ Enable ● Disabled	04	○ Enable ● Disabled
05	○ Enable ● Disabled	06	○ Enable ● Disabled
07	○ Enable ● Disabled	08	○ Enable ● Disabled
G1	○ Enable ● Disabled	G2	○ Enable ● Disabled

The main element configuration description of port authentication interface.

Interface Element	Discription
IEEE802.1X Attestation	IEEE 802.1X authentication status settings: • Enable; • Disable.
Centification time	The range of authentication upgrade interval is 60~60000,

Interface Element	Discription
	unit: minute. The reauthentication interval of 802.1x used for strengthening the security of authentication.
Radius Server	Local internal Radius server and external Radius server configuration: • Local: built-in Radius server, if choosing internal Radius server, the applicant will only use the username and password of internal Radius database. • Remote: fill in the IP address, port number and shared password for authentication of the authentication server if using external Radius server.
Authentication password value	The shared password character string used for device accessing Radius server.
Authentication Server Address	IP address of Radius server
Port	The port number of the Radius server. The default is 1812, value range is 1-65535.
Billing Server Address	Reserved
(Optional) Port	Reserved
IEEE802.1x port authentication	IEEE802.1X authentication state settings of each port: • Enable; • Disable.

Notes

When the device enable local Radius Server, MD5-challenge network identification method is supported temporarily.

8.2.2 Authentication Database

Function Description

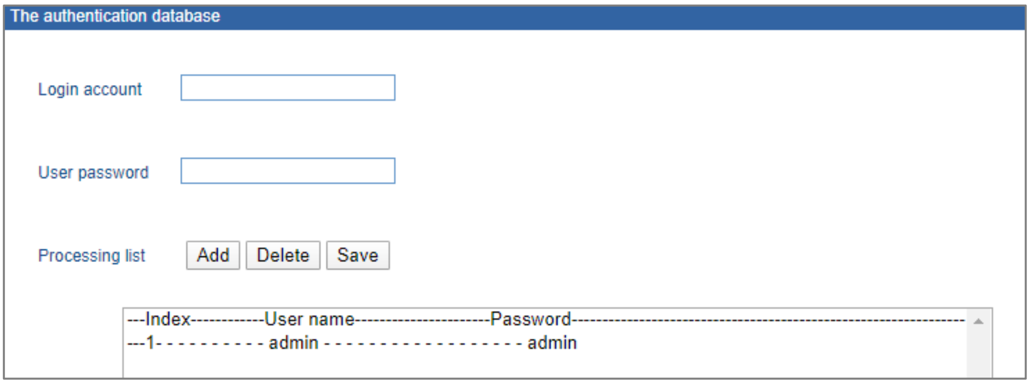
On the "Authentication Database" page, you can set login account and password of users locally authenticated by 802.1X, and you can add, delete and save users.

Operation Path

Open in order: "Main Menu > Access Control > IEEE 802.1X > Authentication Database".

Interface Description

Screenshot of database authentication interface:



The authentication database

Login account

User password

Processing list

```
---Index------------User name---------------------Password--------------------------------------------------------------
---1- - - - - - - - - - admin - - - - - - - - - - - - - - - - - - admin
```

The main element configuration description of database authentication interface:

Interface Element	Note
Login account	Username of logging into local authentication
User Password	Password of logging into local authentication
Processing list	Add, delete or apply the configuration of authentication data.

9 Remote Monitoring

9.1 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 complete information query, information modification and fault troubleshooting on any node on the network by using SNMP platform, 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 managed 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 whole network, NMS manages devices. Each managed device contains Agent processes, MIB, and multiple managed objects residing on 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 value of the next parameter from the Agent in lexicographical order.
Set	The Set operation can set one or more parameter values of the Agent.
Response	Response operation can return one or multiple parameters. 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:

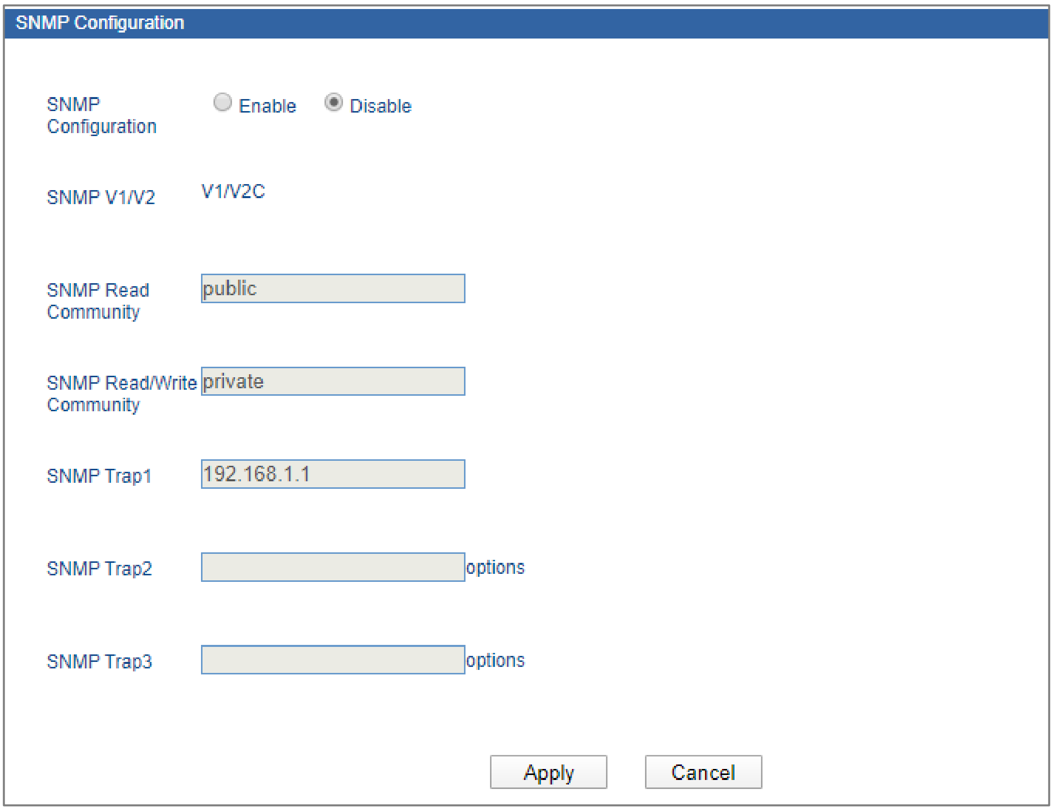
- Enable or disable SNMP configuration functions;
- Configure SNMP V1/V2 read-only community name;
- Configure SNMP V1/V2 read-only community name;
- Configure SNMP gateway.

Operation Path

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

Interface Description

Interface screenshot of SNMP configuration as follows:



SNMP Configuration

SNMP Configuration ○ Enable ● Disable

SNMP V1/V2 V1/V2C

SNMP Read Community: public

SNMP Read/Write Community: private

SNMP Trap1: 192.168.1.1

SNMP Trap2: options

SNMP Trap3: options

Main elements configuration description of SNMP configuration interface:

Interface Element	Discription
SNMP Configuration	SNMP configuration function, options as follows: • Enable; • Disable.
SNMP v1/v2	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.

9.2 Threshold Alarm Settings

Function Description

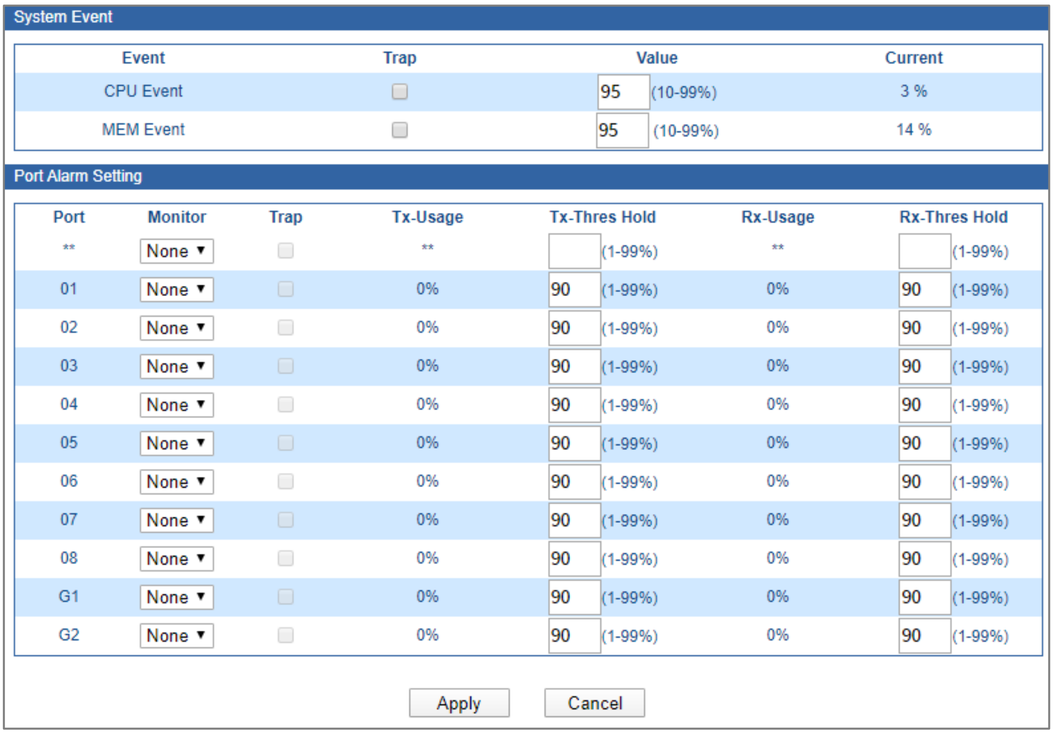
On the “Threshold Alarm Setting” page, you can set alarm events such as CPU utilization, memory utilization, transmission bandwidth utilization and receiving bandwidth utilization. When the alarm event parameter value exceeds the set threshold, the device will continuously send out Trap information to inform relevant personnel. When the alarm event parameter value drops below the set threshold, the device will send out a Trap message to inform the relevant personnel. SNMP Trap information can be used in combination with BlueEyes Pro software, and all Trap information can be displayed directly in the BlueEyes Pro information window. SNMP function must be enabled to use threshold alarm, ; Meanwhile, in order to manage the network topology environment, please enable LLDP function.

Operation Path

Open in order: "Main Menu > Remote Monitoring > Threshold Alarm Settings".

Interface Description

Screenshot of threshold alarm setting interface:



System Event

Event	Trap	Value	Current
CPU Event	□	95 (10-99%)	3 %
MEM Event	□	95 (10-99%)	14 %

Port Alarm Setting

Port	Monitor	Trap	Tx-Usage	Tx-Thres Hold	Rx-Usage	Rx-Thres Hold
**	None ▼	□	**	(1-99%)	**	(1-99%)
01	None ▼	□	0%	90 (1-99%)	0%	90 (1-99%)
02	None ▼	□	0%	90 (1-99%)	0%	90 (1-99%)
03	None ▼	□	0%	90 (1-99%)	0%	90 (1-99%)
04	None ▼	□	0%	90 (1-99%)	0%	90 (1-99%)
05	None ▼	□	0%	90 (1-99%)	0%	90 (1-99%)
06	None ▼	□	0%	90 (1-99%)	0%	90 (1-99%)
07	None ▼	□	0%	90 (1-99%)	0%	90 (1-99%)
08	None ▼	□	0%	90 (1-99%)	0%	90 (1-99%)
G1	None ▼	□	0%	90 (1-99%)	0%	90 (1-99%)
G2	None ▼	□	0%	90 (1-99%)	0%	90 (1-99%)

Main elements configuration description of threshold alarm interface:

Interface Element	Discription
System Event	**System event alert configuration bar**
Event	System alarm events are shown as follows: • CPU alarm: CPU utilization alarm; • MEN alarm: Memory utilization alarm.
Trap	Check the Trap check box to send Trap information when the utilization rate reaches the threshold.

	Note: Before enabling this function, SNMP configuration function needs to be enabled on the "SNMP configuration" page first, and SNMP Trap address needs to be set.
Value	Utilization threshold, when the utilization reaches the threshold, an alarm will be generated. Value range is 10-100, unit: %.
Current	The current utilization value of the system.
Port Alarm Settings	**Port Alarm Settings Configuration Bar**
Port	The Ethernet port number of the device.
Monitor	Port bandwidth monitoring, options are as follows: ● None ● Tx: port transmission bandwidth monitoring. ● Rx: port receiving bandwidth monitoring. ● TxRx: port transmission and receiving bandwidth monitoring. When it is detected that the transmission or reception bandwidth utilization reaches the threshold, an alarm is generated.
Trap	Check the Trap check box to send Trap information when the utilization rate reaches the threshold.
Tx-Usage	Current transmission bandwidth utilization of port.
Tx-Thres Hold	Port bandwidth utilization threshold, the threshold value range is 1-99, the unit is %.
Rx-Usage	Current receiving bandwidth utilization of port.
Rx-Thres hold	Port receiving bandwidth utilization threshold, the threshold value range is 1-99, the unit is %.

9.3 Modbus_TCP

Function Description

On the page of "Modbus_TCP", user can enable Modbus TCP monitoring function. Client can read the switch system, port, ring network, frame statistics and other parameters information via Modbus TCP protocol, which are convenient for various integrated systems to monitor and manage the device.

Note

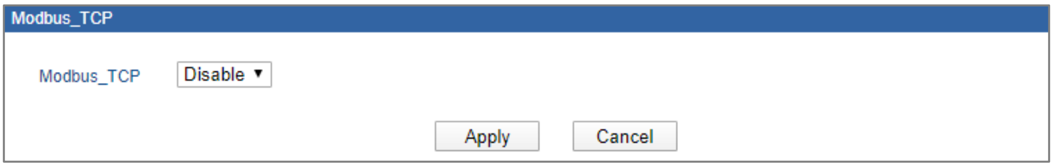
Please see the switch read-only register address information in the "Modbus TCP data sheet" of this section.

Operation Path

Open in order: "Main Menu > Remote Monitoring > Modbus_TCP".

Interface Description

Modbus_TCP screenshot:


Modbus_TCP

Modbus_TCP Disable

The main element configuration description of Modbus_TCP interface:

Interface Element	Note
Modbus_TCP	"Enable" drop-down list of Modbus_TCP monitoring, options as follows: ● Disable: it defaults to disabled; ● Enable: After enabling Modbus_TCP monitoring function, client can read the switch device information via function code 4.

Modbus_TCP Data Sheet

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

Note

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

Information Type	Address (HEX)	Data Type	Description
System Information	0x0000	2 Words	Device ID (reserved)
	0x0002	16 Words	Name (ASCII display)
	0x0012	16 Words	Description (ASCII display)

Information Type	Address (HEX)	Data Type	Description
	0x0022	3 Words	MAC Address (HEX display)
	0x0025	2 Words	IP address
	0x0027	16 Words	Contact Information
	0x0037	16 Words	Firmware Ver (ASCII display)
	0x0047	16 Words	Hardware Ver (ASCII display)
	0x0057	16 Words	Serial No.
	0x0067	1 Word	Power supply 1 status: • 0x0000：OFF • 0x0001：ON
	0x0068	1 Word	Power supply 2 status: • 0x0000：OFF • 0x0001：ON
Port Information	0x1000-0x101B	1 Word	Port connection status: • 0x0000：Link down • 0x0001：Link up • 0x0002：Disable • 0xFFFF：No port
	0x101D-0x1038	1 Word	Port operating mode: • 0x0000：10M-Half • 0x0001：10M-Full • 0x0002：100M-Half • 0x0003：100M-Full • 0x0004：1G-Half • 0x0005：1G-Full • 0xFFFF：No port
	0x1039-0x1054	1 Word	Port flow control status: • 0x0000：OFF • 0x0001：ON • 0xFFFF：No port
	0x1056-0x1071	1 Word	Port interface type: • 0x0000: Copper port • 0x0001: Fiber port • 0x0002: Combo port • 0xFFFF：No port
Frame Statistics	0x2000-0x2037	2 Words	Quantity of sending packets of the port. For example, sending

Information Type	Address (HEX)	Data Type	Description
			packets quantity of port 1 is 0x44332211, namely: Word 1 is 0x4433, Word 2 is 0x2211
	0x2039-0x2070	2 Words	Quantity of receiving packets of the port. For example, receiving packets quantity of port 1 is 0x44332211, namely: Word 1 is 0x4433, Word 2 is 0x2211.
	0x2072-0x20A9	2 Words	Quantity of error packets sending of the port. For example, sending error packets quantity of port 1 is 0x44332211, namely: Word 1 is 0x4433, Word 2 is 0x2211.
	0x20AB-0x20E2	2 Words	Quantity of receiving error packets of the port. For example, receiving error packets quantity of port 1 is 0x44332211, namely: Word 1 is 0x4433, Word 2 is 0x2211.
Ring Information	0x3000	1 Word	Link redundancy algorithm category: ● 0x0000：None ● 0x0001：SW-Ring V1 ● 0x0002：SW-Ring V2 ● 0x0003：SW-Ring V3 ● 0x0004：RSTP
	0x3001	1 Word	Ring type of Ring group 1: ● 0x0000: Single Ring ● 0x0001: Coupling Ring ● 0x0002: Chain ● 0x0003：Dual_homing

Information Type	Address (HEX)	Data Type	Description
	0x3002	1 Word	Ring port 1 of Ring group 1
	0x3003	1 Word	Ring port 2 of Ring group 1
	0x3004	1 Word	Ring ID of Ring group 1
	0x3005	1 Word	HelloTime of Ring group 1
	0x3006	1 Word	Ring group 1 enable: ● 0x0000：Disable ● 0x0001：Enable
	0x3007	1 Word	Master/slave device of Ring group 1 ● 0x0000: master device ● 0x0001: slave device
	0x3008	1 Word	Ring type of Ring group 2: ● 0x0000: Single Ring ● 0x0001: Coupling Ring ● 0x0002: Chain ● 0x0003：Dual_homing
	0x3009	1 Word	Ring port 1 of Ring group 2
	0x300A	1 Word	Ring port 2 of Ring group 2
	0x300B	1 Word	Ring ID of Ring group 2
	0x300C	1 Word	HelloTime of Ring group 2
	0x300D	1 Word	Ring group 2 enable: ● 0x0000：Disable ● 0x0001：Enable
	0x300E	1 Word	Master/slave device of Ring group 2 ● 0x0000: master device ● 0x0001: slave device
	0x300F	1 Word	Ring type of Ring group 3: ● 0x0000: Single Ring ● 0x0001: Coupling Ring ● 0x0002: Chain ● 0x0003：Dual_homing
	0x3010	1 Word	Ring port 1 of Ring group 3
	0x3011	1 Word	Ring port 2 of Ring group 3
	0x3012	1 Word	Ring ID of Ring group 3
	0x3013	1 Word	HelloTime of Ring group 3
	0x3014	1 Word	Ring group 3 enable: ● 0x0000：Disable

Information Type	Address (HEX)	Data Type	Description
			● 0x0001：Enable
	0x3015	1 Word	Master/slave device of Ring group 3 ● 0x0000: master device ● 0x0001: slave device
	0x3016	1 Word	Ring type of Ring group 4: ● 0x0000: Single Ring ● 0x0001: Coupling Ring ● 0x0002: Chain ● 0x0003：Dual_homing
	0x3017	1 Word	Ring port 1 of Ring group 4
	0x3018	1 Word	Ring port 2 of Ring group 4
	0x3019	1 Word	Ring ID of Ring group 4
	0x301A	1 Word	HelloTime of Ring group 4
	0x301B	1 Word	Ring group 4 enable: ● 0x0000：Disable ● 0x0001：Enable
	0x301C	1 Word	Master/slave device of Ring group 4 ● 0x0000: master device ● 0x0001: slave device
SFP DDM Information	0x50E4—0x5100	1 word	Port DDM status: ● 0x0001:DDM SFP module has been connected; ● 0x0000:DDM SFP module has not been connected;
	0x5101—0x5139	1 word	Wavelength of port DDM (nm)
	0x513A—0x5172	1 word	The current voltage of port DDM (V)
	0x5173—0x51AB	1 word	The maximum voltage of port DDM (V)
	0x51AC—0x51E4	1 word	The minimum voltage of port DDM (V)
	0x51E5—	1 word	The current temperature of

Information Type	Address (HEX)	Data Type	Description
	0x521D		port DDM (℃)
	0x521E—0x5256	1 word	The maximum temperature of port DDM (℃)
	0x5257—0x528F	1 word	The minimum temperature of port DDM (℃)
	0x5290—0x52C8	1 word	The current value of DDM TX Power (dBm)
	0x52C9—0x5301	1 word	The maximum value of DDM TX Power (dBm)
	0x5302—0x533A	1 word	The minimum value of DDM TX Power (dBm)
	0x533B—0x5373	1 word	The current value of DDM RX Power (dBm)
	0x5374—0x53AC	1 word	The maximum value of DDM RX Power (dBm)
	0x53AD—0x53E5	1 word	The minimum value of DDM RX Power (dBm)
	0x53E6—0x5424	1 word	The current value of DDM Bias (mA)
	0x5425—0x545D	1 word	The maximum value of DDM Bias (mA)
	0x545E—0x54F4	1 word	The minimum value of DDM Bias (mA)

Example: MODBUS_TCP Configuration

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

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

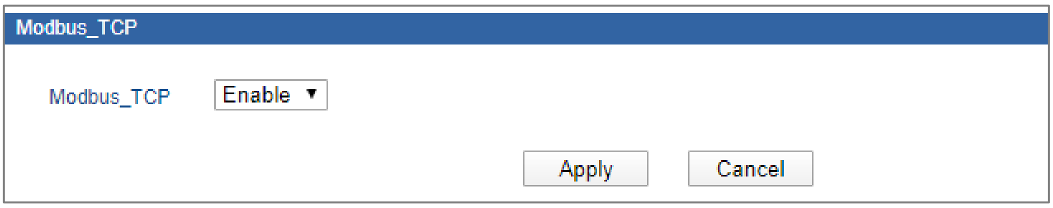
Operation Steps

Configure the switch Modbus_TCP monitoring enable.

Step 1 Log into Web configuration interface.

Step 2 Select "Main Menu > Remote Monitoring > Modbus_TCP".

Step 3 Select "Enable" on the drop-down list of "Modbus_TCP", as the picture below.



Modbus_TCP

Modbus_TCP: Enable

Step 4 Click “Apply”.

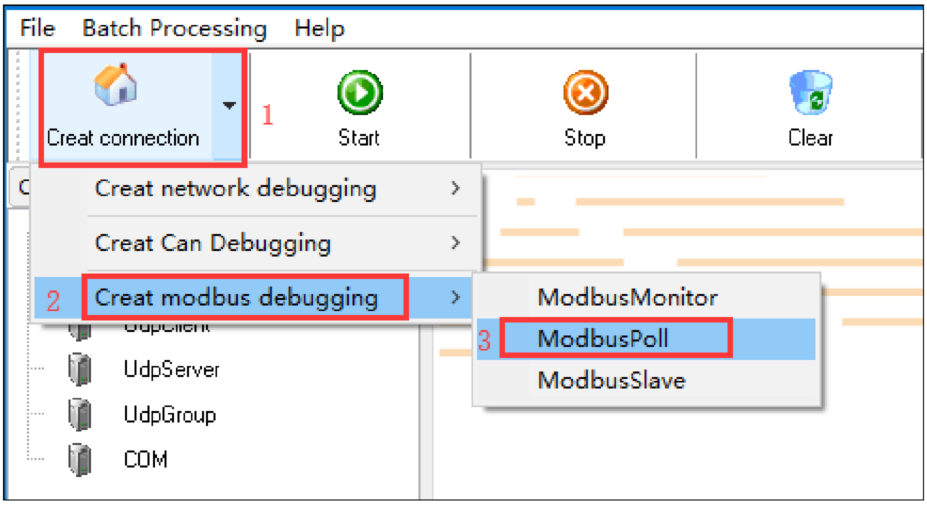
Step 5 End.

Operate the debug tool software to acquire the device parameters.

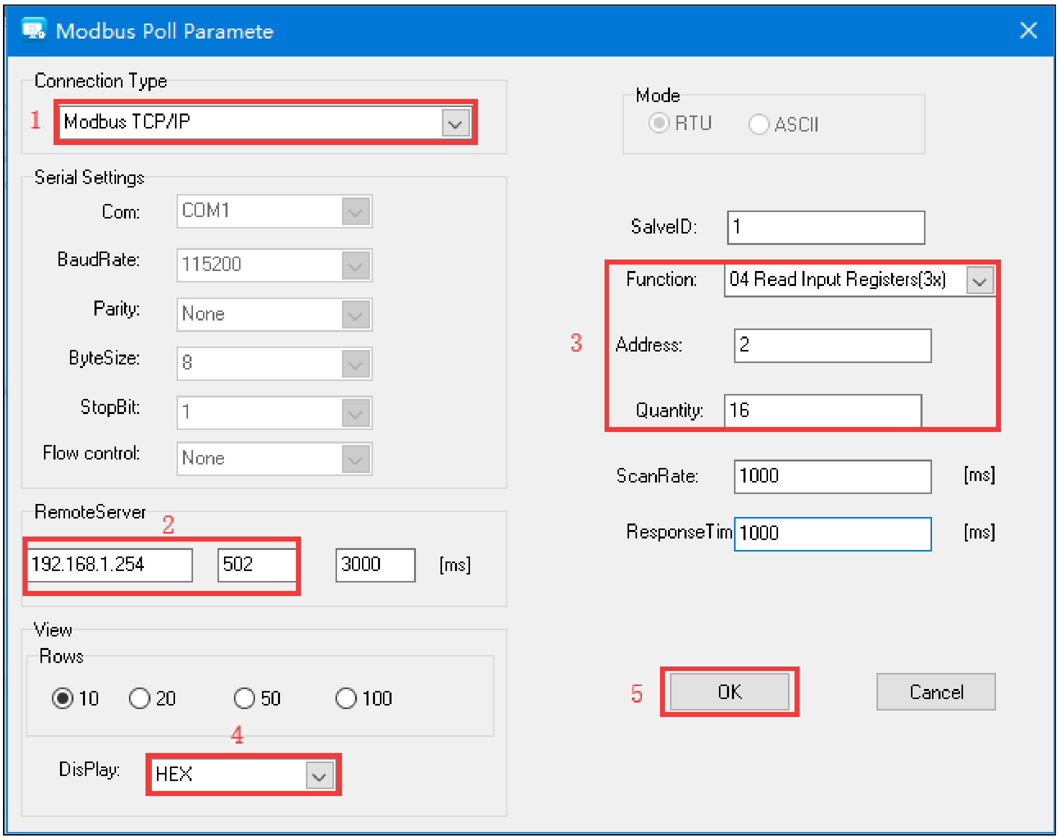
Step 1 Open "Debug Tool".

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

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



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



Modbus Poll Paramete

Connection Type
1 Modbus TCP/IP

Serial Settings
Com: COM1
BaudRate: 115200
Parity: None
ByteSize: 8
StopBit: 1
Flow control: None

RemoteServer
2 192.168.1.254 502 3000 [ms]

View
Rows
● 10 ○ 20 ○ 50 ○ 100
4 DisPlay: HEX

Mode
● RTU ○ ASCII

SalveID: 1
3 Function: 04 Read Input Registers(3x)
Address: 2
Quantity: 16
ScanRate: 1000 [ms]
ResponseTim 1000 [ms]

5 OK Cancel

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

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

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

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

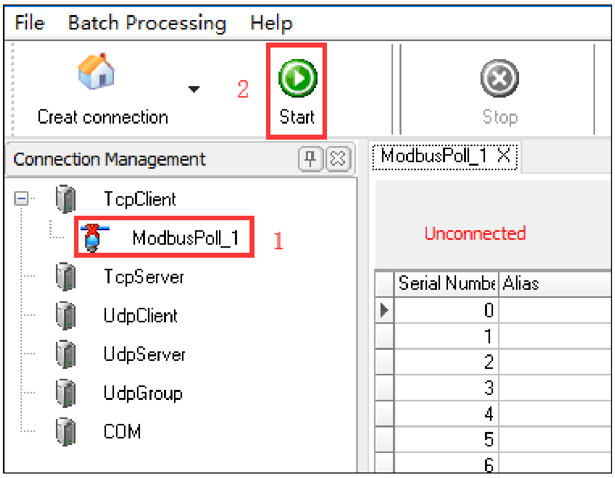
Notice:
Here the start address is decimal format, so hexadecimal register address should be converted into decimal format.

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

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

7 Click "OK".

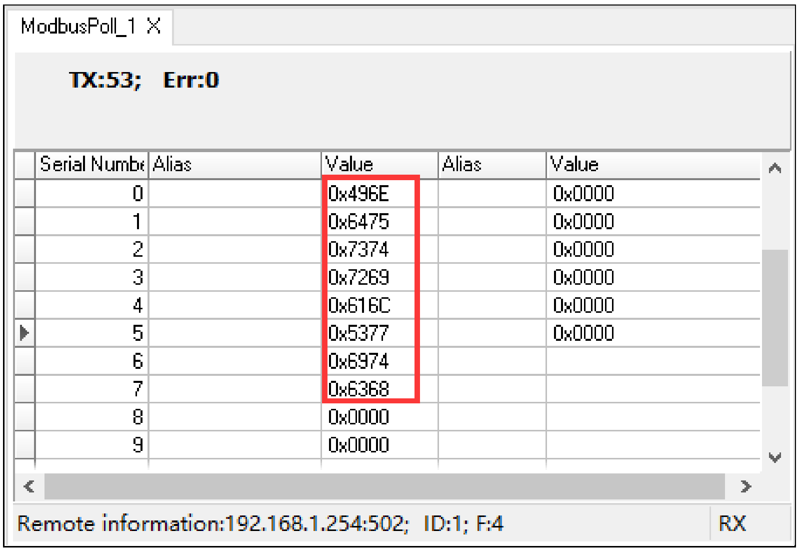
Step 5 On the page of Debug Tool, select created ModbusPoll, and then click "Start";



Unconnected

Serial Numbe	Alias
0	
1	
2	
3	
4	
5	
6	

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



TX:53; Err:0

Serial Numbe	Alias	Value	Alias	Value
0		0x496E		0x0000
1		0x6475		0x0000
2		0x7374		0x0000
3		0x7269		0x0000
4		0x616C		0x0000
5		0x5377		0x0000
6		0x6974		
7		0x6368		
8		0x0000		
9		0x0000		

Remote information:192.168.1.254:502; ID:1; F:4 RX

Step 7 End.

Note

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

9.4 Alarm Settings

Function Description

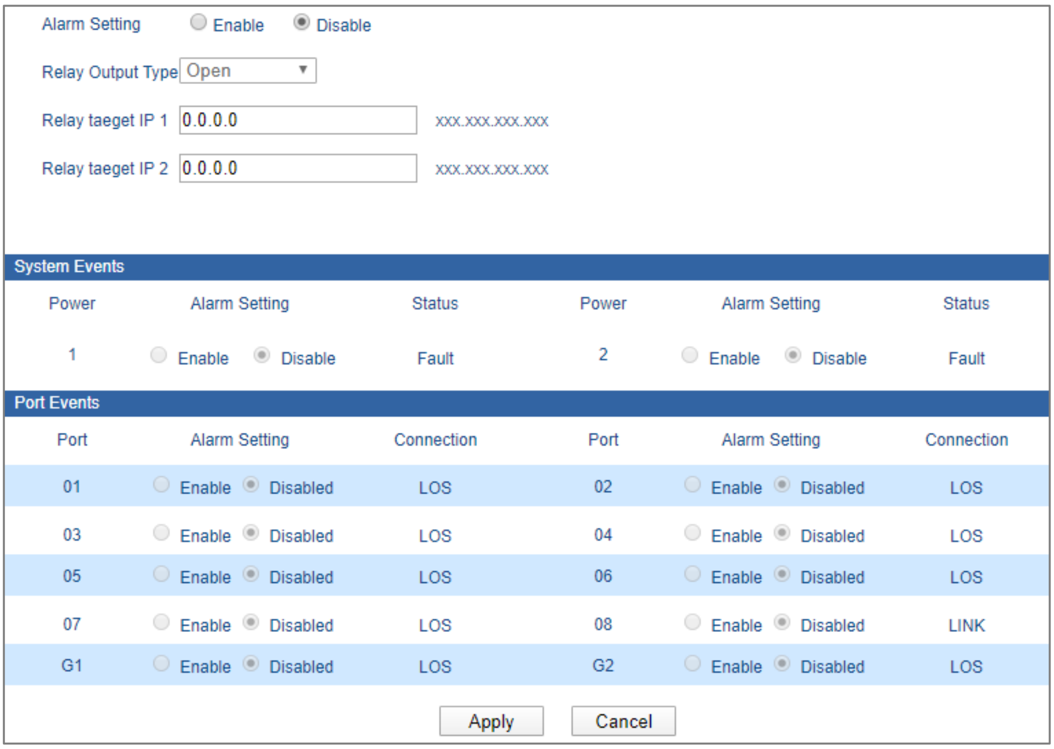
On the page of "Alarm Warning", user can configure power supply alarm and port alarm; when the equipment runs abnormally, it can promptly notify the administrator, and quickly repair the equipment to avoid excessive loss.

Operation Path

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

Interface Description

Alarm warning interface as follows:



Alarm Setting ○ Enable ● Disable

Relay Output Type: Open ▾

Relay taeget IP 1: 0.0.0.0 xxx.xxx.xxx.xxx

Relay taeget IP 2: 0.0.0.0 xxx.xxx.xxx.xxx

System Events

Power	Alarm Setting	Status	Power	Alarm Setting	Status
1	○ Enable ● Disable	Fault	2	○ Enable ● Disable	Fault

Port Events

Port	Alarm Setting	Connection	Port	Alarm Setting	Connection
01	○ Enable ● Disabled	LOS	02	○ Enable ● Disabled	LOS
03	○ Enable ● Disabled	LOS	04	○ Enable ● Disabled	LOS
05	○ Enable ● Disabled	LOS	06	○ Enable ● Disabled	LOS
07	○ Enable ● Disabled	LOS	08	○ Enable ● Disabled	LINK
G1	○ Enable ● Disabled	LOS	G2	○ Enable ● Disabled	LOS

Main elements configuration description of alarm warning interface:

Interface Element	Note
Alarm Settings	Configure alarm settings. Options: ● Enable; ● Disable.
Relay Output Type	Click the drop-down list of "Relay Output Type", options as follows:

Interface Element	Note
	● 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 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	Display the device port number.
Alarm Setting	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	Display port connection status of the device:

Interface Element	Note
	• 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.

10 Port Statistics

10.1 Frame Statistics

Function Description

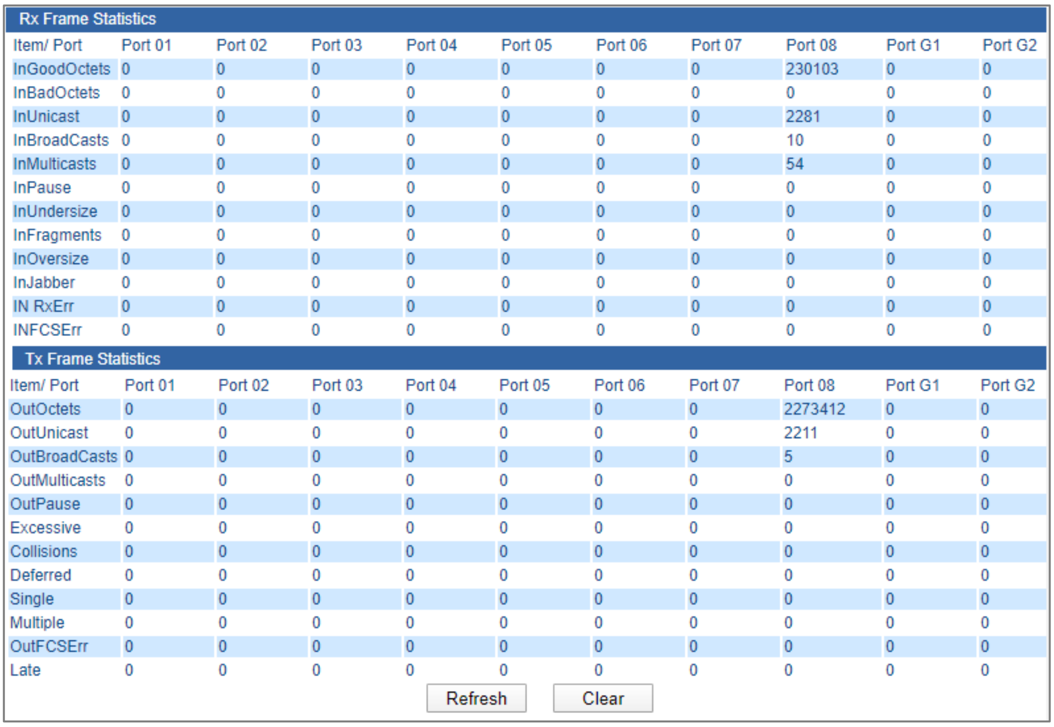
On the page of “Frame Statistics”, user can check frame statistics of sending/receiving data packets transmitted by the port within a period of time.

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	Port 06	Port 07	Port 08	Port G1	Port G2
InGoodOctets	0	0	0	0	0	0	0	230103	0	0
InBadOctets	0	0	0	0	0	0	0	0	0	0
InUnicast	0	0	0	0	0	0	0	2281	0	0
InBroadCasts	0	0	0	0	0	0	0	10	0	0
InMulticasts	0	0	0	0	0	0	0	54	0	0
InPause	0	0	0	0	0	0	0	0	0	0
InUndersize	0	0	0	0	0	0	0	0	0	0
InFragments	0	0	0	0	0	0	0	0	0	0
InOversize	0	0	0	0	0	0	0	0	0	0
InJabber	0	0	0	0	0	0	0	0	0	0
IN RxErr	0	0	0	0	0	0	0	0	0	0
INFCSErr	0	0	0	0	0	0	0	0	0	0

Tx Frame Statistics

Item/ Port	Port 01	Port 02	Port 03	Port 04	Port 05	Port 06	Port 07	Port 08	Port G1	Port G2
OutOctets	0	0	0	0	0	0	0	2273412	0	0
OutUnicast	0	0	0	0	0	0	0	2211	0	0
OutBroadCasts	0	0	0	0	0	0	0	5	0	0
OutMulticasts	0	0	0	0	0	0	0	0	0	0
OutPause	0	0	0	0	0	0	0	0	0	0
Excessive	0	0	0	0	0	0	0	0	0	0
Collisions	0	0	0	0	0	0	0	0	0	0
Deferred	0	0	0	0	0	0	0	0	0	0
Single	0	0	0	0	0	0	0	0	0	0
Multiple	0	0	0	0	0	0	0	0	0	0
OutFCSErr	0	0	0	0	0	0	0	0	0	0
Late	0	0	0	0	0	0	0	0	0	0

Main elements configuration description of received frames statistics interface:

Interface Element	Note
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.
IN RxErr	The number of error frames in the receiving process.
InFCSErr	Number (complete data) of error frames counted by FCS verification.

Main elements configuration description of transmitted frames statistics interface:

Interface Element	Note
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.

Interface Element	Note
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.

11 Network Diagnosis

11.1 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

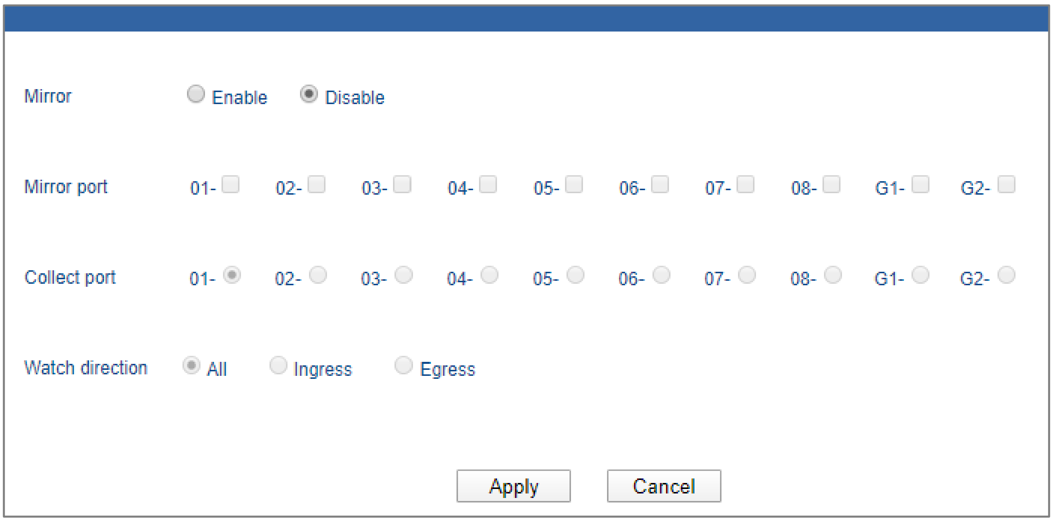
On the “Port Mirror” page, user can enable or configure the correspondence between ingress data mirror and egress data mirror.

Operation Path

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

Interface Description

Port mirror interface as follows:



Mirror ○ Enable ● Disable

Mirror port 01-□ 02-□ 03-□ 04-□ 05-□ 06-□ 07-□ 08-□ G1-□ G2-□

Collect port 01-● 02-○ 03-○ 04-○ 05-○ 06-○ 07-○ 08-○ G1-○ G2-○

Watch direction ● All ○ Ingress ○ Egress

The main element configuration description of port mirror interface:

Interface Element	Note
Mirror	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.
Watch direction	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.

12 System Management

12.1 Log Information

Function Description

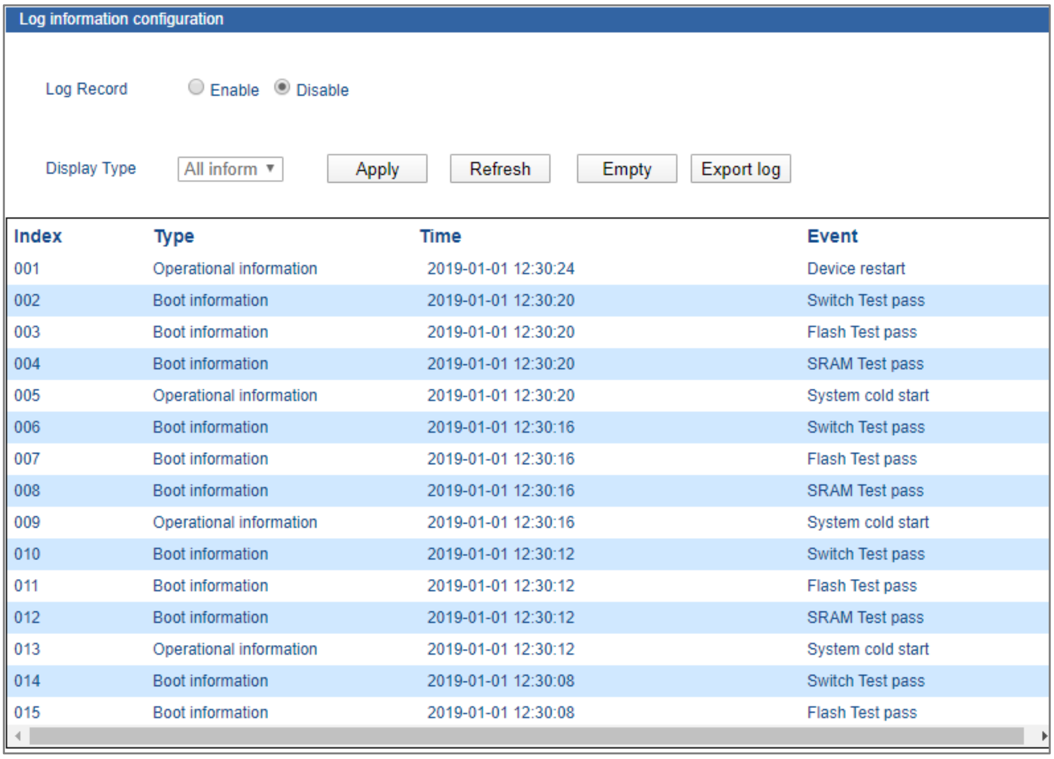
On the page of “Log information”, user can enable “log record” to check the status information of the device.

Operation Path

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

Interface Description

Log information interface as follows:


Log information configuration

Log Record ○ Enable ● Disable

Display Type All inform ▼

Index	Type	Time	Event
001	Operational information	2019-01-01 12:30:24	Device restart
002	Boot information	2019-01-01 12:30:20	Switch Test pass
003	Boot information	2019-01-01 12:30:20	Flash Test pass
004	Boot information	2019-01-01 12:30:20	SRAM Test pass
005	Operational information	2019-01-01 12:30:20	System cold start
006	Boot information	2019-01-01 12:30:16	Switch Test pass
007	Boot information	2019-01-01 12:30:16	Flash Test pass
008	Boot information	2019-01-01 12:30:16	SRAM Test pass
009	Operational information	2019-01-01 12:30:16	System cold start
010	Boot information	2019-01-01 12:30:12	Switch Test pass
011	Boot information	2019-01-01 12:30:12	Flash Test pass
012	Boot information	2019-01-01 12:30:12	SRAM Test pass
013	Operational information	2019-01-01 12:30:12	System cold start
014	Boot information	2019-01-01 12:30:08	Switch Test pass
015	Boot information	2019-01-01 12:30:08	Flash Test pass

Main elements configuration description of log information interface:

Interface Element	Note
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".

12.2 Time Configuration

Function Description

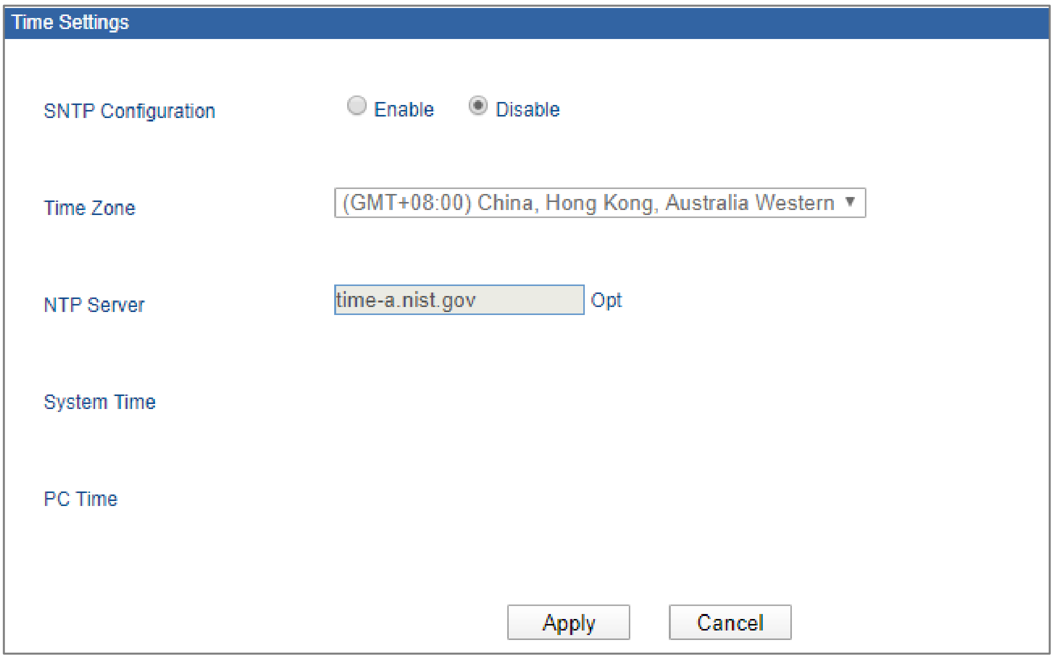
On the page of “Time Configuration”, user can check current PC time or system operation time, and select relative time zone.

Operation Path

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

Interface Description

Time setting interface as follows:



Time Settings

SNTP Configuration ○ Enable ● Disable

Time Zone (GMT+08:00) China, Hong Kong, Australia Western ▾

NTP Server time-a.nist.gov Opt

System Time

PC Time

Main elements configuration description of time configuration interface:

Interface Element	Note
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.

Note

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

12.3 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

Note

- 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 mask corresponding to class A address is 255.0.0.0; The mask of class B address is 255.255.0.0; The mask for class C addresses 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:

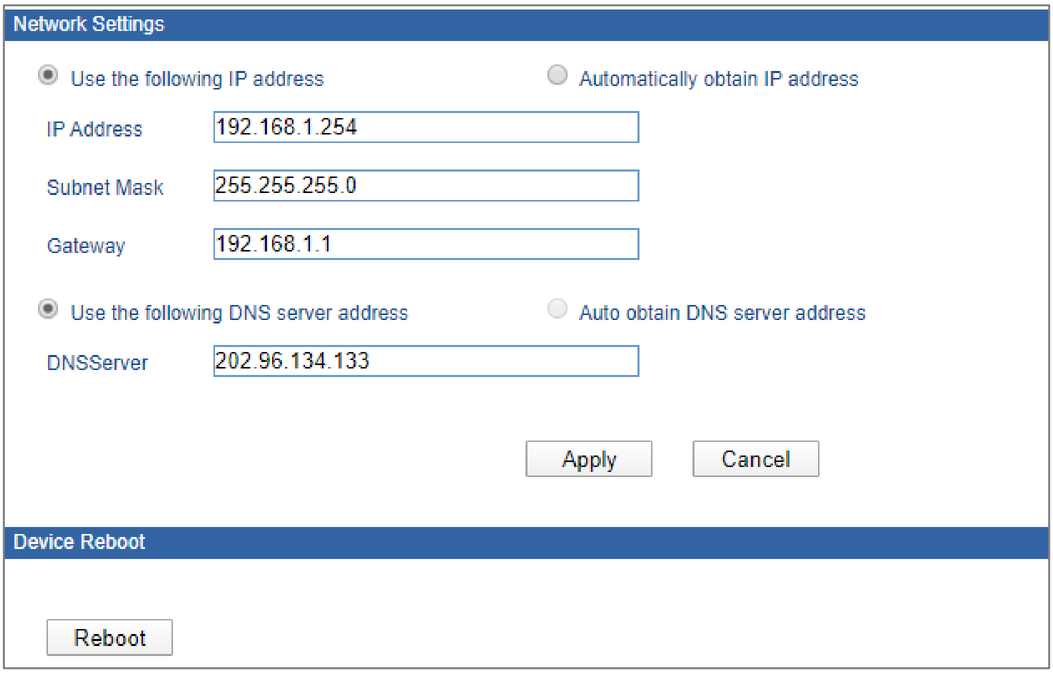
- Configure default IP address of the device;
- Configure netmask;
- Configure gateway address;
- Configure DNS server;
- Reboot the device.

Operation Path

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

Interface Description

The Device management interface is as follows:



Network Settings

● Use the following IP address ○ Automatically obtain IP address

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

● Use the following DNS server address ○ Auto obtain DNS server address

DNSServer: 202.96.134.133

Device Reboot

Main elements configuration description of device address interface:

Interface Element	Note
Network Settings	**Configuration column of the Network Settings**
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 automatically 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.
Auto 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.

Interface Element	Note
DNS Server	Configure DNS server address.
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.
Device Reboot	**Configuration column of the 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.

12.4 System Information

Function Description

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

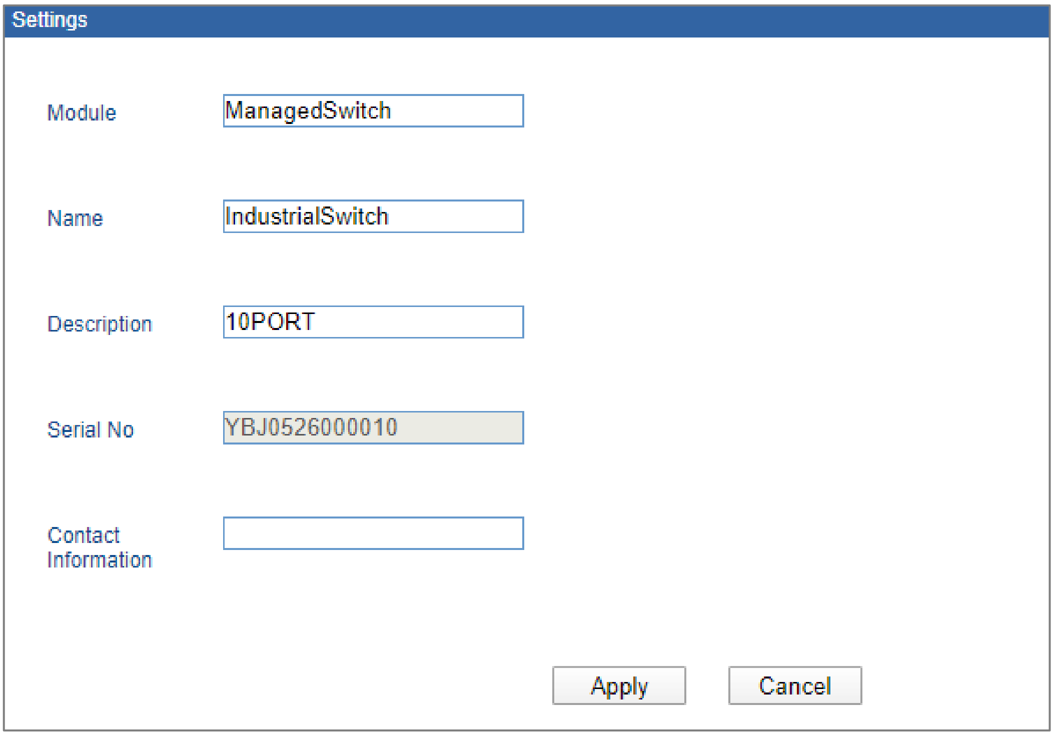
- Device model;
- Device name;
- Device description;
- Contact information.

Operation Path

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

Interface Description

System information interface as follows:



Settings

Module	ManagedSwitch
Name	IndustrialSwitch
Description	10PORT
Serial No	YBJ0526000010
Contact Information	

Main element configuration instructions in System Information interface.

Interface Element	Note
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.

12.5 File Management

Function Description

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

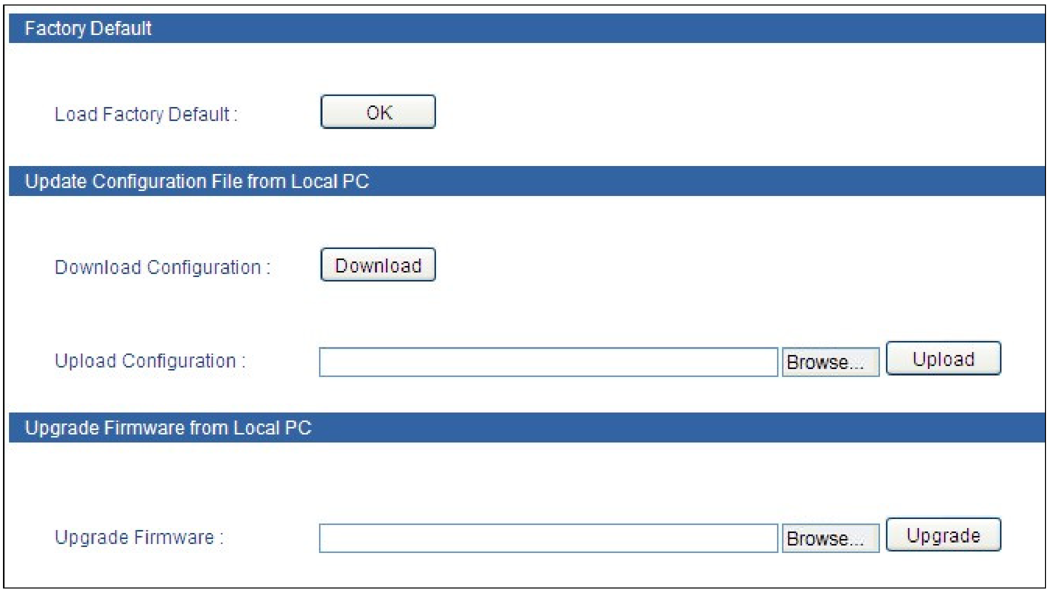
- Restore factory defaults;
- Upload and download configuration files;
- System upgrading.

Operation Path

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

Interface Description

System File interface as follow:



Factory Default

Load Factory Default : OK

Update Configuration File from Local PC

Download Configuration : Download

Upload Configuration : Browse... Upload

Upgrade Firmware from Local PC

Upgrade Firmware : Browse... Upgrade

Main element configuration instructions in System File interface.

Interface Element	Note
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, or 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

Note

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.

12.6 System Logout

Function Description

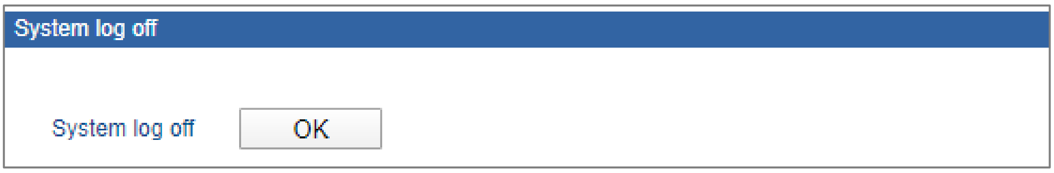
On the page of “System log off”, user can log off the login information of current user.

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	Note
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.

13 FAQ

13.1 Sign in Problems

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

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

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

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

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

   Both configurations are the same, without conflict.

13.2 Configuration Problem

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

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

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

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

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

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

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

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

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

13.3 Indicator Problem

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

   Possible reasons include:

   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Power supply or indicators faults; troubleshooting, change the power supply or device test.

- Power supply voltage can't meet the device requirements; troubleshooting, configure the power supply voltage according to the device manual.

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

   Possible reasons include:

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

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

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

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

   Reasons may include:

   - Surrounding environment disturbs the product; troubleshooting, product grounding adopts shielding line or shields the interference source.
   - Site wiring is not normative; Troubleshooting, optical fiber, network cable, optical cable cannot be arranged with power line and high-voltage line.
   - Network cable is disturbed by static electricity or surge; Troubleshooting, change the shielded cable or install a lightning protector.
   - High and low temperature influence; troubleshooting, check the device temperature usage range.

14 Maintenance and Service

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

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

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

14.1 Internet Service

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

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

14.2 Service Hotline

Users of our company's products could call technical support office for help. Our company has professional technical engineers to answer your questions and help you solve the product or usage problems ASAP. Free service hotline: +86-400-880-4496

14.3 Product Repair or Replacement

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

3onedata Co., Ltd.

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

Technology support: tech-support@3onedata.com

Service hotline: 400-880-4496

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